KPMG Accountants N.V.
Postbus 74500
1070 DB Amsterdam

Laan van Langerhuize 1
1186 DS Amstelveen
Telefoon (020) 656 7890
www.kpmg.nl

NBA
Consultatie-wet-en-regelgeving@nba.nl

Onze ref. TV/DS/RvL/ir

Amstelveen, 3 mei 2021

Betreft: Reactie consultatiedocument 'Vertaling herziene Standaard 315 en wijzigingen in andere Standaarden van de NV COS'

Geachte heer, mevrouw,

Wij maken graag gebruik van de door u geboden gelegenheid om te reageren op het consultatiedocument 'Vertaling herziene Standaard 315 en wijzigingen in andere Standaarden van de NV COS'. Wij hebben de door u geformuleerde consultatievragen als basis voor onze reactie gehanteerd.

Vraag 1. Heeft u specifieke opmerkingen bij de vertaling van de wijzigingen in Standaard 315 en de vertaling van de wijzigingen in andere Standaarden?

Allereerst merken we op dat het niet beschikbaar stellen van een zogenaamde 'side by side' versie in Word waarbij de relevante ISA teksten naast de COS vertaling daarvan worden uiteengezet, een gemis was in deze consultatie. Een dergelijke 'side by side' versie zorgt voor een effectievere en efficiëntere evaluatie van de vertaling wat bijdraagt aan de verhoging van de kwaliteit daarvan. Daarom bevelen wij u aan om in toekomstige consultaties van vertaalde Standaarden wel de gebruikelijke 'side by side' versie ter beschikking te stellen.

Voor een efficiënte en effectieve beoordeling zou het helpen om de vertaalconventie ter beschikking te stellen. Daarmee worden onnodige opmerkingen ten aanzien van de vertaling voorkomen. Sommige vertalingen waarvan wij verwachten dat ze gerelateerd zijn aan de vertaalconventie resulteren in de opbouw van moeilijk leesbare zinnen.

Wij hebben zelf 'side by side' versies van de vertaling opgemaakt op basis van de beschikbaar gestelde pdf-versies. In verband met de grote hoeveelheid opmerkingen hebben wij de focus gelegd op de vereisten van Standaard 315. De toelichtende paragrafen en bijlagen van Standaard 315 alsmede de wijziging in de overige Standaarden hebben we globaal geëvalueerd. Omdat uit onze evaluatie van alleen de vereisten er best wat opmerkingen zijn gebleken vragen wij uw aandacht voor de kwaliteit van de vertaling. In de bijlage bij deze brief treft u onze detailopmerkingen. Ondanks dat het niet om 'fatal flaws' gaat verzoeken wij u om goede kennis van deze opmerkingen te nemen en om met deze opmerkingen in het achterhoofd opnieuw te kijken naar de vertaling van de toelichtende paragrafen en bijlage bij Standaard 315 alsmede de aanpassingen in de andere Standaarden. Desgewenst kunnen wij u in dat kader mede assisteren.

NBA
Betreft: Reactie consultatiedocument 'Vertaling herziene Standaard 315 en wijzigingen in andere Standaarden van de NV COS'
Amstelveen, 3 mei 2021

Vraag 2. Zijn de wijzigingen in deze Standaarden toepasbaar in uw omgeving? Zo niet, wat is daarvoor de reden?

Op dit moment zien wij geen reden om te verwachten dat de wijzigingen in deze Standaarden niet toepasbaar zullen zijn in onze omgeving. Pas bij de feitelijke toepassing daarvan in de praktijk zal dit duidelijk worden. Verder verwijzen we naar de brief van KPMG (International) bij de ISA 315 revised exposure draft welke publiek beschikbaar is.

Vraag 3. Vindt u dat er specifieke guidance nodig is voor het mkb? Zo ja, op welke gebieden en kunt u toelichten waarom dit nodig is?

Onze internationale controleaanpak is gebaseerd op de vereisten in de ISA's. Vanuit dat oogpunt signaleren wij geen noodzaak voor specifieke Nederlandse guidance. Maar als er specifieke guidance wordt ontwikkeld met betrekking tot het toepassen van deze standaard voor het mkb zullen we daar met belangstelling kennis van nemen.

Vraag 4. Kunt u zich vinden in de voorgestelde ingangsdatum?

Wij kunnen ons vinden in de voorgestelde ingangsdatum die gelijk is aan de ingangsdatum van de aanpassingen in de betreffende ISA's.

Met vriendelijke groet,

Tom Volleberg
Partner

Bijlage(n):
Detailopmerkingen vereisten Standaard 315
Detailopmerkingen bijlagen 5 en 6 bij Standaard 315

BIJLAGE 1 - Detailopmerkingen vereisten Standaard 315

Introduction Scope of this ISA 1. This International Standard on Auditing (ISA) deals with the auditor's responsibility to identify and assess the risks of material misstatement in the financial statements. Key Concepts in this ISA 2. ISA 200 deals with the overall objectives of the auditor in conducting an audit of the financial statements,1 including to obtain sufficient appropriate audit evidence to reduce audit risk to an acceptably low level.2 Audit risk is a function of the risks of material misstatement and detection risk.3 ISA 200 explains that the risks of material misstatement may exist at two levels:4 the overall financial statement level; and the assertion level for classes of transactions, account balances and disclosures. 3. ISA 200 requires the auditor to exercise professional judgment in planning and performing an audit, and to plan and perform an audit with professional skepticism recognizing that circumstances may exist that cause the financial statements to be materially misstated.5 4. Risks at the financial statement level relate pervasively to the financial statements as a whole and potentially affect many assertions. Risks of material misstatement at the assertion level consist of two components, inherent and control risk: • Inherent risk is described as the susceptibility of an assertion about a class of transaction, account balance or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls. • Control risk is described as the risk that a misstatement that could occur in an assertion about a class of transaction, account balance or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or detected and corrected, on a timely basis by the entity's system of internal control. 5. ISA 200 explains that risks of material misstatement are assessed at the assertion level in order to determine the nature, timing and extent of further audit procedures necessary to obtain sufficient appropriate audit evidence.6 For the identified risks of material misstatement at the assertion level, a separate assessment of inherent risk and control risk is required by this ISA. As explained in ISA 200, inherent risk is higher for some assertions and related classes of transactions, account balances and disclosures than for others. The degree to which inherent risk varies is referred to in this ISA as the 'spectrum of inherent risk.' 6. Risks of material misstatement identified and assessed by the auditor include both those due to error and those due to fraud. Although both are addressed by this ISA, the significance of fraud is such that further requirements and guidance are included in ISA 2407 in relation to risk assessment procedures and related	Inleiding Toepassingsgebied van deze Standaard 1 Deze Standaard behandelt de verantwoordelijkheid van de accountant om de risico's op een af wijking van materieel belang in de financiële overzichten te identificeren en in te schatten. Belangrijke uitgangspunten in deze Standaard 2 Standaard 200 behandelt de algehele doelstellingen van de accountant bij het uitvoeren van een controle van de financiële overzichten1, inclusief het verkrijgen van voldoende en geschikte con- trole-informatie om het controlerisico terug te brengen tot een aanvaardbaar laag niveau.2 Con- trolerisico is een functie van de risico's op een afwijking van materieel belang en ontdekkingsri- sico.3 Standaard 200 legt uit dat de risico's op een afwijking van materieel belang op twee ni- veaus kunnen bestaan:4 op het niveau van de financiële overzichten als geheel; en op het niveau van beweringen voor transactiestromen, rekeningsaldi en toelichtingen. 3 Standaard 200 vereist dat de accountant professionele oordeelsvorming toepast bij het plannen en uitvoeren van een controle en dat de accountant een controle plant en uitvoert met een pro- fessioneel-kritische instelling waarbij de accountant ~~er~~ rekening ~~mee~~ houdt dat er omstandighe- den kunnen bestaan die ertoe leiden dat de financiële overzichten een afwijking van materieel belang bevatten.5 4 Risico's op het niveau van de financiële overzichten hebben een diepgaande invloed op de finan- ciële overzichten als geheel en kunnen een ~~groot aantal~~ veel beweringen beïnvloeden. Risico's op een afwijking van materieel belang op het niveau van beweringen bestaan uit twee componenten, inherent risico en interne beheersingsrisico[A1]: • Inherent risico ~~wordt~~ is beschreven als de vatbaarheid van een bewering met betrekking tot een transactiestroom, rekeningsaldo of toelichting voor een afwijking die afzonderlijk of gezamen- lijk met andere afwijkingen van materieel belang ~~is~~kan zijn, [A2]voordat er rekening wordt gehouden met de eventuele daarop betrekking hebbende [A3]interne beheersingsmaatregelen; • Interne beheersingsrisico ~~wordt~~ is beschreven als het risico dat een afwijking in een bewering met betrekking tot een transactiestroom, rekeningsaldo of toelichting en die afzonderlijk of gezamenlijk met andere afwijkingen van materieel belang is[A4], niet wordt voorkomen of niet tij- dig door het interne beheersingssysteem van de entiteit wordt gedetecteerd en hersteld.[A5] 5 Standaard 200 legt uit dat risico's op een afwijking van materieel belang worden ingeschat op het niveau van beweringen om de aard, timing en omvang van verdere controlewerkzaamheden te bepalen die nodig zijn om voldoende en geschikte controle-informatie te verkrijgen.6 Voor de ge- identificeerde risico's op een afwijking van materieel belang op het niveau van beweringen, ver- eist deze Standaard een afzonderlijke inschatting van het inherente risico en het interne beheer- singsrisico. Zoals uitgelegd in Standaard 200, is het inherente risico hoger voor sommige bewe- ringen en daarmee verband houdende transactiestromen, rekeningsaldi en toelichtingen dan voor andere. De mate waarin het inherente risico varieert, wordt in deze Standaard aangeduid als het 'spectrum van inherent risico'. 6 Risico's op een afwijking van materieel belang die door de accountant zijn geïdentificeerd en in- geschat, omvatten zowel afwijkingen die het gevolg van zijn fouten of [A6][A7]van fraude. Hoewel beide door deze Standaard worden behandeld, is de significantie van fraude zodanig dat verdere ver-

activities to obtain information that is used to identify, assess and respond to the risks of material misstatement due to fraud.	eisten en leidraden zijn opgenomen in Standaard 2407 met betrekking tot risico-inschattingswerk- zaamheden en daarmee verband houdende werkzaamheden voor het verkrijgen van informatie die wordt gebruikt om de risico's op een afwijking van materieel belang die het gevolg is van fraude te identificeren, in te schatten en daarop in te spelen.
7. The auditor's risk identification and assessment process is iterative and dynamic. The auditor's understanding of the entity and its environment, the applicable financial reporting framework, and the entity's system of internal control are interdependent with concepts within the requirements to identify and assess the risks of material misstatement. In obtaining the understanding required by this ISA, initial expectations of risks may be developed, which may be further refined as the auditor progresses through the risk identification and assessment process. In addition, this ISA and ISA 330 require the auditor to revise the risk assessments, and modify further overall responses and further audit procedures, based on audit evidence obtained from performing further audit procedures in accordance with ISA 330, or if new information is obtained.	7 Het risico-identificatie- en inschattingsproces van de accountant is iteratief en dynamisch. Het in- zicht van de accountant in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het interne beheersingssysteem van de entiteit hangen onderling sa- men met concepten in [A8]de vereisten om de risico's op een afwijking van materieel belang te identi- ficeren en in te schatten. Bij het verwerven van het inzicht vereist door deze Standaard, kunnen initiële verwachtingen van risico's worden ontwikkeld[A9], die verder kunnen worden verfijnd naar- mate de accountant vordert met het risico-identificatie- en inschattingsproces. Bovendien verei- sen deze Standaard en Standaard 330 van de accountant om de risico-inschattingen te herzien en verdere algehele manieren om in te spelen op de risico's en verdere controlewerkzaamheden te wijzigen[A10]. Dit gebeurt op basis van controle-informatie verkregen bij het uitvoeren van verdere controlewerkzaamheden in overeenstemming met Standaard 330 of als nieuwe informatie wordt verkregen.
8. ISA 330 requires the auditor to design and implement overall responses to address the assessed risks of material misstatement at the financial statement level.8 ISA 330 further explains that the auditor's assessment of the risks of material misstatement at the financial statement level, and the auditor's overall responses, is affected by the auditor's understanding of the control environment. ISA 330 also requires the auditor to design and perform further audit procedures whose nature, timing and extent are based on and are responsive to the assessed risks of material misstatement at the assertion level.9	8 Standaard 330 vereist dat de accountant algehele manieren [A11][A12]dient op te zetten en te implementeren om op de ingeschatte risico's op een afwijking van materieel belang op het niveau van de financiële overzichten in te spelen[A13].8 Standaard 330 legt verder uit dat de inschatting van de risico's door de accountant op een afwijking van materieel belang op het niveau van de financiële over- zichten en de algehele manieren van inspelen [A14]door de accountant worden beïnvloed door het in- zicht van de accountant in de interne beheersingsomgeving. Standaard 330 vereist ook dat de accountant verdere controlewerkzaamheden opzet en uitvoert waarvan de aard, timing en om- vang zijn gebaseerd op en die inspelen [A15]op de ingeschatte risico's op een afwijking van materieel belang op het niveau van beweringen.9
Scalability 9. ISA 200 states that some ISAs include scalability considerations which illustrate the application of the requirements to all entities regardless of whether their nature and circumstances are less complex or more complex.10 This ISA is intended for audits of all entities, regardless of size or complexity and the application material therefore incorporates specific considerations specific to both less and more complex entities, where appropriate. While the size of an entity may be an indicator of its complexity, some smaller entities may be complex and some larger entities may be less complex.	Schaalbaarheid 9 Standaard 200 stelt dat sommige Standaarden schaalbaarheidsoverwegingen bevatten die de toepassing van de vereisten voor alle entiteiten illustreren, ongeacht of hun aard en omstandig- heden minder of meer complex zijn.10 Deze Standaard is bedoeld voor controles van alle entitei- ten, ongeacht de omvang of complexiteit en de toepassingsgerichte teksten bevatten daarom specifieke overwegingen voor zowel minder als meer complexe entiteiten, in voorkomend geval. Hoewel de omvang van een entiteit een indicatie kan zijn van de complexiteit ervan, kunnen som- mige kleinere entiteiten complex zijn en sommige grotere entiteiten minder complex zijn.
Effective Date 10. This ISA is effective for audits of financial statements for periods beginning on or after December 15, 2021.	Ingangsdatum 10 Deze Standaard is van toepassing voor controles van financiële overzichten voor verslagperio- den beginnend op of na 15 december 2021.
Objective	Doelstelling
11. The objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement.	11 De doelstelling van de accountant is het identificeren en inschatten van de risico's op een afwij- king van materieel belang als gevolg van fraude of fouten, op het niveau van de financiële over- zichten en op het niveau van beweringen, zodat een basis wordt verkregen voor het opzetten en het implementeren van manieren om in te spelen op de ingeschatte risico's op een afwijking van materieel belang[A16].

Definitions 12. For purposes of the ISAs, the following terms have the meanings attributed below: (a) Assertions – Representations, explicit or otherwise, with respect to the recognition, measurement, presentation and disclosure of information in the financial statements which are inherent in management representing that the financial statements are prepared in accordance with the applicable financial reporting framework. Assertions are used by the auditor to consider the different types of potential misstatements that may occur when identifying, assessing and responding to the risks of material misstatement. (Ref: Para. A1) (b) (c) Business risk – A risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies. (d) (c) Controls – Policies or procedures that an entity establishes to achieve the control objectives of management or those charged with governance. In this context: (Ref: Para. A2–A5) (i) Policies are statements of what should, or should not, be done within the entity to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. (ii) Procedures are actions to implement policies. (d) General information technology (IT) controls – Controls over the entity's IT processes that support the continued proper operation of the IT environment, including the continued effective functioning of information processing controls and the integrity of information (i.e., the completeness, accuracy and validity of information) in the entity's information system. Also see the definition of IT environment. (e) Information processing controls – Controls relating to the processing of information in IT applications or manual information processes in the entity's information system that directly address risks to the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information). (Ref: Para. A6) (f) (f) Inherent risk factors – Characteristics of events or conditions that affect susceptibility to misstatement, whether due to fraud or error, of an assertion about a class of transactions, account balance or disclosure, before consideration of controls. Such factors may be qualitative or quantitative, and include complexity, subjectivity, change, uncertainty or susceptibility to misstatement due to management bias or other fraud risk factors11 insofar as they affect inherent risk. (Ref: Para. A7–A8) (g) IT environment – The IT applications and supporting IT infrastructure, as well as the IT processes and personnel involved in those processes, that an entity uses to support business operations and achieve business strategies. For the purposes of this ISA: (i) An IT application is a program or a set of programs that is used in the initiation, processing, recording and reporting of transactions or information. IT applications include data warehouses and report writers. (ii) The IT infrastructure comprises the network, operating systems, and databases and their related hardware and software. (iii) The IT processes are the entity's processes to manage access to the IT environment, manage program changes or changes to the IT environment and manage IT operations.	Definities 12 Voor de toepassing van de Standaarden hebben de volgende termen de hierna weergegeven be- tekenis: a Beweringen - al dan niet expliciete uitspraken met betrekking tot de opname[A17], waardering, presentatie en toelichting van informatie in de financiële overzichten die inherent zijn aan de bevestiging door het management dat de financiële overzichten in overeenstemming zijn met het van toepassing zijnde stelsel inzake financiële verslaggeving zijn opgesteld. Beweringen wor- den door de accountant gebruikt om de verschillende soorten mogelijke afwijkingen die kun- nen voorkomen te overwegen bij het identificeren, inschatten van en inspelen op de risico's op een afwijking van materieel belang. (Zie Par. A1) b Bedrijfsrisico - een risico dat voortkomt uit significante voorwaarden, gebeurtenissen, om- standigheden, handelingen of het achterwege laten van handelingen die een nadelig effect kunnen hebben op de mogelijkheid van een entiteit om de [A18]doelstellingen te bereiken en de strategieën uit te voeren, of dat voortkomt uit het vaststellen van ongepaste doelstellingen en strategieën. c Interne beheersingsmaatregelen - beleidslijnen of procedures die een entiteit vaststelt om de beheersingsdoelstellingen van management of de met governance belaste personen te be- reiken. In deze context: (Zie Par. A2 – A5) i Beleidslijnen zijn bepalingen [A19]over wat wel of niet binnen de entiteit dient te worden ge- daan om de interne beheersing te bewerkstelligen. Dergelijke uiteenzettingen [A20]kunnen zijn gedocumenteerd, expliciet vermeld in mededelingen[A21], of impliciet door handelingen en be- slissingen; ii Procedures zijn handelingen om beleidslijnen te implementeren. d General IT controls - interne beheersingsmaatregelen met betrekking tot de informatietechno- logie (IT)-processen van de entiteit die de voortdurende goede werking van de IT-omgeving ondersteunen, inclusief de voortdurende effectieve werking van interne beheersingsmaatre- gelen met betrekking tot informatieverwerking en de integriteit van informatie (d.w.z. de volle- digheid, nauwkeurigheid en geldigheid [A22]van informatie) in het informatiesysteem van de enti- teit. Zie ook de definitie van IT-omgeving. e Interne beheersingsmaatregelen met betrekking tot informatieverwerking- Interne beheer- singsmaatregelen in verband met de verwerking van informatie in IT-applicaties of handma- tige informatieprocessen in het informatiesysteem van de entiteit die rechtstreeks inspelen op risico's voor de integriteit van informatie (d.w.z. de volledigheid, nauwkeurigheid en geldig- heid van transacties en andere informatie). (Zie Par. A6) f Inherente risicofactoren - Kenmerken van gebeurtenissen of omstandigheden die de vatbaar- heid voor afwijkingen beïnvloeden, die het gevolg zijn van fraude of fouten, van een bewering met betrekking tot een transactiestroom, rekeningsaldo of toelichting, voordat rekening wordt gehouden met interne beheersingsmaatregelen. Dergelijke factoren kunnen kwalitatief of kwantitatief zijn en omvatten complexiteit, subjectiviteit, wijzigingen, onzekerheid of vatbaar- heid voor afwijkingen als gevolg van tendentie bij het management of andere frauderisicofac- toren11 voor zover ze het inherente risico beïnvloeden. (Zie Par. A7 – A8) g IT-omgeving - De IT-applicaties en ondersteunende IT-infrastructuur, evenals de IT- processen en personeel betrokken bij die processen, die een entiteit gebruikt om bedrijfsacti- viteiten te ondersteunen en bedrijfsstrategieën te bereiken. Voor de toepassing van deze Standaard geldt het volgende: i Een IT-applicatie is een programma of een reeks programma's die worden gebruikt bij het initiëren, verwerken, vastleggen en rapporteren van transacties of informatie. IT- applicaties omvatten ook datawarehouses en rapportgenerators; ii De IT-infrastructuur omvat het netwerk, besturingssystemen en databases en hun gerela- teerde hardware en software;

(h) Relevant assertions – An assertion about a class of transactions, account balance or disclosure is relevant when it has an identified risk of material misstatement. The determination of whether an assertion is a relevant assertion is made before consideration of any related controls (i.e., the inherent risk). (Ref: Para. A9)	iii De IT-processen zijn de processen van de entiteit om de toegang tot de IT-omgeving, programmawijzigingen of wijzigingen in de IT-omgeving en IT-activiteiten te beheren. h Relevante beweringen - Een bewering met betrekking tot een transactiestroom, rekening-saldo of toelichting is relevant wanneer voor die bewering een geïdentificeerd risico op een afwijking van materieel belang bestaat. De bepaling of een bewering een relevante bewering is, wordt gemaakt vóóór dat rekening wordt gehouden met de eventuele daarop betrekking hebbende interne beheersingsmaatregelen (d.w.z. het inherente risico). (Zie Par. A9)
(i) Risks arising from the use of IT – Susceptibility of information processing controls to ineffective design or operation, or risks to the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information) in the entity's information system, due to ineffective design or operation of controls in the entity's IT processes (see IT environment).	i Risico's die voortkomen uit het gebruik van IT- Vatbaarheid van interne beheersingsmaatre-gelen met betrekking tot informatieverwerking voor ineffectieve opzet of werking, of risico's voor de integriteit van informatie (d.w.z. de volledigheid, nauwkeurigheid en geldigheid van transacties en andere informatie) in het informatiesysteem van de entiteit als gevolg van inef- fectieve opzet of werking van interne beheersingsmaatregelen in de IT-processen van de en- titeit (zie IT-omgeving).
(j) Risk assessment procedures – The audit procedures designed and performed to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels.	j Risico-inschattingswerkzaamheden - De controlewerkzaamheden die zijn opgezet en uitge-voerd om de risico's op een afwijking van materieel belang als gevolg van fraude of fouten [A23] te identificeren en in te schatten op het niveau van de financiële overzichten en op het niveau van beweringen.
(k) Significant class of transactions, account balance or disclosure – A class of transactions, account balance or disclosure for which there is one or more relevant assertions. (l) Significant risk – An identified risk of material misstatement: (Ref: Para. A10)	k Significante transactiestroom, rekeningsaldo of toelichting- Een transactiestroom, rekening-saldo of toelichting waarvoor er een of meer relevante beweringen zijn. l Significant risico - Een geïdentificeerd risico op een afwijking van materieel belang: (Zie Par. A10)
(i) For which the assessment of inherent risk is close to the upper end of the spectrum of inherent risk due to the degree to which inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur; or (ii) That is to be treated as a significant risk in accordance with the requirements of other ISAs.12	i Waarvoor de inschatting van het inherente risico dicht bij de bovengrens [A24] van het spec-trum van inherent risico is vanwege de mate waarin inherente risicofactoren de combina- tie van de waarschijnlijkheid dat een afwijking voorkomt en de orde van grootte [A25] van de potentiële afwijking indien die afwijking zich zou voordoen, beïnvloeden; of ii Dat moet worden behandeld als een significant risico in overeenstemming met de vereis- ten van andere Standaarden.12
(m) System of internal control – The system designed, implemented and maintained by those charged with governance, management and other personnel, to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. For the purposes of the ISAs, the system of internal control consists of five inter- related components: (i) Control environment; (ii) The entity's risk assessment process; (iii) The entity's process to monitor the system of internal control; (iv) The information system and communication; and (v) Control activities.	m Systeem van interne beheersing- Het systeem dat is ontworpen, geïmplementeerd en onder-houden door de met governance belaste personen, management en ander personeel om een redelijke mate van zekerheid te verschaffen over het bereiken van de doelstellingen van een entiteit met betrekking tot de betrouwbaarheid van financiële verslaggeving, effectiviteit en efficiëntie van activiteiten en naleving van de van toepassing zijnde wet- en regelgeving. Voor de toepassing van de Standaarden bestaat het interne beheersingssysteem uit vijf onderling verbonden componenten: i Interne beheersingsomgeving; ii Het risico-inschattingsproces van de entiteit; iii Het proces van de entiteit om het interne beheersingssysteem te monitoren; iv Het informatiesysteem en communicatie; en v Interne beheersingsactiviteiten.
Requirements	Vereisten
Risk Assessment Procedures and Related Activities 13. The auditor shall design and perform risk assessment procedures to obtain audit evidence that provides an appropriate basis for: (Ref: Para. A11–A18) (a) The identification and assessment of risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels; and (b) The design of further audit procedures in accordance with ISA 330. The auditor shall design and perform risk assessment procedures in a manner that is not biased towards obtaining audit evidence that may be corroborative or towards excluding audit evidence that may be contradictory. (Ref: Para. A14)	Risico-inschattingswerkzaamheden en daarmee verband houdende werkzaamheden 13 De accountant dient risico-inschattingswerkzaamheden op te zetten en uit te voeren om controle- informatie te verkrijgen die een geschikte basis biedt voor: (Zie Par. A11 – A18) a De identificatie en inschatting van risico's op een afwijking van materieel belang als gevolg van fraude of fouten, op het niveau van de financiële overzichten en beweringen; en b De opzet van verdere controlewerkzaamheden in overeenstemming met Standaard 330. De accountant dient risico-inschattingswerkzaamheden op te zetten en uit te voeren op een ma- nier die niet tendeert naar het verkrijgen van controle-informatie die bevestigend kan zijn of naar het uitsluiten van controle-informatie die tegenstrijdig kan zijn. (Zie Par. A14)

14. The risk assessment procedures shall include the following: (Ref: Para. A19–A21) (a) Inquiries of management and of other appropriate individuals within the entity, including individuals within the internal audit function (if the function exists). (Ref: Para. A22–A26) (b) Analytical procedures. (Ref: Para. A27–A31) (c) Observation and inspection. (Ref: Para. A32–A36) Information from Other Sources 15. In obtaining audit evidence in accordance with paragraph 13, the auditor shall consider information from: (Ref: Para. A37–A38) (a) The auditor's procedures regarding acceptance or continuance of the client relationship or the audit engagement; and (b) When applicable, other engagements performed by the engagement partner for the entity. 16. When the auditor intends to use information obtained from the auditor's previous experience with the entity and from audit procedures performed in previous audits, the auditor shall evaluate whether such information remains relevant and reliable as audit evidence for the current audit. (Ref: Para. A39–A41) Engagement Team Discussion 17. The engagement partner and other key engagement team members shall discuss the application of the applicable financial reporting framework and the susceptibility of the entity's financial statements to material misstatement. (Ref: Para. A42–A47) 18. When there are engagement team members not involved in the engagement team discussion, the engagement partner shall determine which matters are to be communicated to those members. Obtaining an Understanding of the Entity and Its Environment, the Applicable Financial Reporting Framework and the Entity's System of Internal Control (Ref: Para. A48–A49) Understanding the Entity and Its Environment, and the Applicable Financial Reporting Framework (Ref: Para. A50–A55) 19. The auditor shall perform risk assessment procedures to obtain an understanding of: (a) The following aspects of the entity and its environment: (i) The entity's organizational structure, ownership and governance, and its business model, including the extent to which the business model integrates the use of IT; (Ref: Para. A56–A67) (ii) Industry, regulatory and other external factors; (Ref: Para. A68–A73) and (iii) The measures used, internally and externally, to assess the entity's financial performance; (Ref: Para. A74–A81) (b) The applicable financial reporting framework, and the entity's accounting policies and the reasons for any changes thereto; (Ref: Para. A82–A84) and (c) How inherent risk factors affect susceptibility of assertions to misstatement and the degree to which they do so, in the preparation of the financial statements in accordance with the applicable financial reporting framework, based on the understanding obtained in (a) and (b). (Ref: Para. A85–A89)	14 De risico-inschattingswerkzaamheden omvatten het volgende: (Zie Par. A19 - A21) a Verzoeken om inlichtingen bij het management en bij andere geschikte personen binnen de entiteit, inclusief personen binnen de interne auditfunctie (als de functie bestaat); (Zie Par. A22 - A26) b Cijferanalyses; (Zie Par. A27 – A31) c Waarneming en inspectie. (Zie Par. A32 – A36) Informatie uit andere bronnen 15 Bij het verkrijgen van controle-informatie in overeenstemming met paragraaf 13 dient de accoun- tant informatie in overweging te nemen van: (Zie Par. A37 – A38) a De werkzaamheden van de accountant met betrekking tot aanvaarding of continuering van de cliëntrelatie of de controle-opdracht; en b Indien van toepassing, andere opdrachten die door de opdrachtpartner voor de entiteit zijn uitgevoerd. 16 Wanneer de accountant voornemens is informatie te gebruiken die is verkregen uit eerdere erva- ringen van de accountant met de entiteit en uit controlewerkzaamheden die zijn uitgevoerd in eer- dere controles, dient de accountant te evalueren of dergelijke informatie relevant en betrouwbaar blijft als controle-informatie voor de lopende controle. (Zie Par. A39 - A41) Bespreking opdrachtteam 17 De opdrachtpartner en andere kernleden van het opdrachtteam bespreken de toepassing van het van toepassing zijnde stelsel inzake financiële verslaggeving en de vatbaarheid van de financiële overzichten van de entiteit voor een afwijking van materieel belang. (Zie Par. A42 - A47) 18 Wanneer er leden van het opdrachtteam niet betrokken zijn bij de bespreking van het opdracht- team, dient de opdrachtpartner te bepalen welke aangelegenheden aan die leden moeten wor- den meegedeeld. Het verwerven van inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het interne beheersingssysteem van de entiteit (Zie Par. A48 – A49) Inzicht in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslag- geving (Zie Par. A50 - A55) 19 De accountant dient risico-inschattingswerkzaamheden uit te voeren om inzicht te verwerven in: a De volgende aspecten van de entiteit en haar omgeving: i De organisatiestructuur, eigendom en governance van de entiteit en haar bedrijfsmodel, inclusief de mate waarin het bedrijfsmodel het gebruik van IT integreert; (Zie Par. A56 - A67) ii Sector, regelgevende en andere externe factoren; (Zie Par. A68 – A73) en iii De maatregelen [A26]die intern en extern zijn gebruikt om de financiële prestaties van de enti- teit te beoordelen. (Zie Par. A74 – A81) b Het van toepassing zijnde stelsel inzake financiële verslaggeving en de grondslagen voor fi- nanciële verslaggeving van de entiteit en de redenen voor eventuele wijzigingen daarin; (Zie Par. A82 – A84) en c Hoe inherente risicofactoren de vatbaarheid van beweringen voor afwijkingen beïnvloeden en de mate waarin zij dit doen bij het opstellen van de financiële overzichten in overeenstem- ming met het van toepassing zijnde stelsel inzake financiële verslaggeving, op basis van de onder (a) en (b) verworven inzichten. (Zie Par. A85 – A89)

20. The auditor shall evaluate whether the entity's accounting policies are appropriate and consistent with the applicable financial reporting framework.	20 De accountant dient te evalueren of de grondslagen voor financiële verslaggeving van de entiteit passend en consistent zijn met het van toepassing zijnde stelsel inzake financiële verslaggeving.
Understanding the Components of the Entity's System of Internal Control (Ref: Para. A90 – A95) Control Environment, the Entity's Risk Assessment Process and the Entity's Process to Monitor the System of Internal Control (Ref: Para. A96–A98)	Inzicht in de componenten van het interne beheersingssysteem van de entiteit (Zie Par. A90 - A95) Interne beheersingsomgeving, het risico-inschattingsproces van de entiteit en het proces van de enti- teit om het interne beheersingssysteem te monitoren (Zie Par. A96 – A98)
Control environment	Interne beheersingsomgeving
21. The auditor shall obtain an understanding of the control environment relevant to the preparation of the financial statements, through performing risk assessment procedures, by: (Ref: Para. A99–A100) (a) Understanding the set of controls, processes and structures that address: (Ref: Para. A101–A102) (i) How management's oversight responsibilities are carried out, such as the entity's culture and management's commitment to integrity and ethical values; (ii) When those charged with governance are separate from management, the independence of, and oversight over the entity's system of internal control by, those charged with governance; (iii) The entity's assignment of authority and responsibility; (iv) How the entity attracts, develops, and retains competent individuals; and (v) How the entity holds individuals accountable for their responsibilities in the pursuit of the objectives of the system of internal control; (b) Evaluating whether: (Ref: Para. A103–A108) (i) Management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior; (ii) The control environment provides an appropriate foundation for the other components of the entity's system of internal control considering the nature and complexity of the entity; and (iii) Control deficiencies identified in the control environment undermine the other components of the entity's system of internal control.	21 De accountant dient door het uitvoeren van risico-inschattingswerkzaamheden inzicht te verwer- ven in de interne beheersingsomgeving die relevant is voor het opstellen van de financiële over- zichten, door: (Zie Par. A99 – A100) a Inzicht te verwerven in de interne beheersingsmaatregelen, processen en structuren die be- trekking hebben op: (Zie Par. A101 – A102) i Hoe de verantwoordelijkheden van het management om toezicht uit te oefenen worden uitgevoerd, zoals de cultuur van de entiteit en de toewijding van het management aan in- tegriteit en ethische waarden; ii Wanneer de met governance belaste personen gescheiden zijn [A27]van het management, de onafhankelijkheid van en toezicht op het interne beheersingssysteem van de entiteit door de met governance belaste personen; iii De toewijzing door de entiteit van bevoegdheden en verantwoordelijkheid[A28]; iv Hoe de entiteit competente personen aantrekt, ontwikkelt [A29]en behoudt; en v Hoe de entiteit personen verantwoording laat afleggen over hun verantwoordelijkheden bij het nastreven van de doelstellingen van het interne beheersingssysteem; en b Te evalueren of: (Zie Par. A103 - A108) i Management, met het toezicht van de met governance belaste personen, een cultuur van eerlijkheid en ethisch gedrag heeft gecreëerd en gehandhaafd; ii De interne beheersingsomgeving een geschikte basis verschaft voor de andere compo- nenten van het interne beheersingssysteem van de entiteit gezien de aard en complexi- teit van de entiteit; en iii Tekortkomingen in de interne beheersing geïdentificeerd in de interne beheersingsomge- ving de andere componenten van het interne beheersingssysteem van de entiteit onder- mijnen.
The entity's risk assessment process	Het risico-inschattingsproces van de entiteit
22. The auditor shall obtain an understanding of the entity's risk assessment process relevant to the preparation of the financial statements, through performing risk assessment procedures, by: (a) Understanding the entity's process for: (Ref: Para. A109–A110) (i) Identifying business risks relevant to financial reporting objectives; (Ref: Para. A62) (ii) Assessing the significance of those risks, including the likelihood of their occurrence; and (iii) Addressing those risks; and (b) Evaluating whether the entity's risk assessment process is appropriate to the entity's circumstances considering the nature and complexity of the entity. (Ref: Para. A111–A113)	22 De accountant dient door het uitvoeren van risico-inschattingswerkzaamheden inzicht te verwer- ven in het risico-inschattingsproces van de entiteit dat relevant is voor het opstellen van de finan- ciële overzichten, door: a Inzicht te verwerven in het proces van de entiteit voor: (Zie Par. A109 - A110) i Het identificeren van bedrijfsrisico's die relevant zijn voor de doelstellingen van de financi- ele verslaggeving; (Zie Par. A62) ii Het inschatten van de significantie van die risico's, inclusief de waarschijnlijkheid dat deze voorkomen; en iii Het inspelen op die risico's; en b Te evalueren of het risico-inschattingsproces van de entiteit geschikt is voor de omstandighe- den van de entiteit gezien de aard en complexiteit van de entiteit. (Zie Par. A111 – A113)
23. If the auditor identifies risks of material misstatement that management failed to identify, the auditor shall:	23 Als de accountant risico's op een afwijking van materieel belang identificeert die het management niet heeft geïdentificeerd, dient de accountant: a Te bepalen of dergelijke risico's van een soort zijn waarvan de accountant verwacht had dat deze geïdentificeerd zouden worden door het risico-inschattingsproces van de entiteit en, zo ja, inzicht

(a) Determine whether any such risks are of a kind that the auditor expects would have been identified by the entity's risk assessment process and, if so, obtain an understanding of why the entity's risk assessment process failed to identify such risks of material misstatement; and (b) Consider the implications for the auditor's evaluation in paragraph 22(b). The entity's process to monitor the system of internal control 24 .The auditor shall obtain an understanding of the entity's process for monitoring the system of internal control relevant to the preparation of the financial statements, through performing risk assessment procedures, by: (Ref: Para. A114–A115) (a) Understanding those aspects of the entity's process that address: (i) Ongoing and separate evaluations for monitoring the effectiveness of controls, and the identification and remediation of control deficiencies identified; (Ref: Para. A116–A117) and (ii) The entity's internal audit function, if any, including its nature, responsibilities and activities; (Ref: Para. A118) (b) Understanding the sources of the information used in the entity's process to monitor the system of internal control, and the basis upon which management considers the information to be sufficiently reliable for the purpose; (Ref: Para. A119–A120) and (c) Evaluating whether the entity's process for monitoring the system of internal control is appropriate to the entity's circumstances considering the nature and complexity of the entity. (Ref: Para. A121–A122) Information System and Communication, and Control Activities (Ref: Para. A123–A130) The information system and communication 25. The auditor shall obtain an understanding of the entity's information system and communication relevant to the preparation of the financial statements, through performing risk assessment procedures, by: (Ref: Para. A131) (a) Understanding the entity's information processing activities, including its data and information, the resources to be used in such activities and the policies that define, for significant classes of transactions, account balances and disclosures: (Ref: Para. A132–A143) (i) How information flows through the entity's information system, including how: a. Transactions are initiated, and how information about them is recorded, processed, corrected as necessary, incorporated in the general ledger and reported in the financial statements; and b. Information about events and conditions, other than transactions, is captured, processed and disclosed in the financial statements; (ii) The accounting records, specific accounts in the financial statements and other supporting records relating to the flows of information in the information system; (iii) The financial reporting process used to prepare the entity's financial statements, including disclosures; and (iv) The entity's resources, including the IT environment, relevant to (a)(i) to (a)(iii) above; (b) Understanding how the entity communicates significant matters that support the preparation of the financial statements and related reporting responsibilities in the information system and other components of the system of internal control: (Ref: Para. A144–A145) (i) Between people within the entity, including how financial reporting roles and responsibilities are communicated; (ii) Between management and those charged with governance; and (iii) With external parties, such as those with regulatory authorities;	te verwerven in de reden dat het risico-inschattingsproces van de entiteit dergelijke risico's op een afwijking van materieel belang niet heeft geïdentificeerd; en b De implicaties voor de evaluatie van de accountant in paragraaf 22(b) te overwegen. Het proces van de entiteit om het interne beheersingssysteem te monitoren 24 De accountant dient door het uitvoeren van risico-inschattingswerkzaamheden inzicht te verwer- ven in het proces van de entiteit voor het monitoren van het interne beheersingssysteem dat rele- vant is voor het opstellen van de financiële overzichten, door: (Zie Par. A114 – A115) a Inzicht te verwerven in die aspecten van het proces van de entiteit die betrekking hebben op: i Voortdurende[A30] en afzonderlijke evaluaties voor het monitoren van de effectiviteit van in- terne beheersingsmaatregelen en de identificatie en het herstel van geïdentificeerde te- kortkomingen in de interne beheersing; (Zie Par. A116 – A117) en ii De interne auditfunctie van de entiteit, indien aanwezig, inclusief de aard, verantwoorde- lijkheden en activiteiten; (Zie Par. A118) b Inzicht te verwerven in de bronnen van de informatie die gebruikt wordt in het proces van de entiteit om het interne beheersingssysteem te monitoren en de basis waarop management de informatie als voldoende betrouwbaar voor het doel overweegt; (Zie Par. A119 – A120) en c Te evalueren of het proces voor het monitoren van het interne beheersingssysteem van de entiteit geschikt is voor de omstandigheden van de entiteit gezien de aard en complexiteit van de entiteit. (Zie Par. A121 – A122) Informatiesysteem en communicatie, en interne beheersingsactiviteiten (Zie Par. A123 – A130) Het informatiesysteem en communicatie 25 De accountant dient door middel van risico-inschattingswerkzaamheden inzicht te verwerven in het informatiesysteem en de communicatie van de entiteit die relevant is voor het opstellen van de financiële overzichten, door: (Zie Par. A131) a Inzicht te verwerven in de informatieverwerkingsactiviteiten van de entiteit, inclusief gegevens en informatie, de benodigde middelen voor dergelijke activiteiten en de beleidslijnen die voor significante transactiestromen, rekeningsaldi en toelichtingen definiëren[A31]: (Zie Par. A132 – A143) i Hoe informatie stroomt door het informatiesysteem van de entiteit, inclusief hoe: • transacties worden geïnitieerd, en hoe informatie daarover wordt vastgelegd, ver- werkt, gecorrigeerd indien nodig[A32], opgenomen [A33]in het grootboek en gerapporteerd in de financiële overzichten; en • informatie over gebeurtenissen en omstandigheden, anders dan transacties, wordt vastgelegd, verwerkt en toegelicht in de financiële overzichten. ii De administratieve vastleggingen, specifieke rekeningen in de financiële overzichten en andere ondersteunende vastleggingen met betrekking tot de informatiestromen in het in- formatiesysteem; iii Het proces van financiële verslaggeving dat is gebruikt om de financiële overzichten van de entiteit, inclusief toelichtingen, op te stellen; en iv De middelen van de entiteit, inclusief de IT-omgeving, relevant voor (a) (i) tot (a) (iii) hier- boven; b Inzicht te verwerven in hoe de entiteit significante aangelegenheden communiceert die het opstellen van de financiële overzichten en gerelateerde rapporteringsverantwoordelijkheden in het informatiesysteem en andere componenten van het interne beheersingssysteem on- dersteunen: (Zie Par. A144 – A145) i Tussen mensen binnen de entiteit, inclusief hoe financiële verslaggevingstaken en ver- antwoordelijkheden worden gecommuniceerd; ii Tussen management en de met governance belaste personen; en iii Met externe partijen, zoals die met regelgevende of toezichthoudende instanties; en

(c) Evaluating whether the entity's information system and communication appropriately support the preparation of the entity's financial statements in accordance with the applicable financial reporting framework. (Ref: Para. A146)	c Te evalueren of het informatiesysteem van de entiteit en de communicatie op gepaste wijze het opstellen van de financiële overzichten van de entiteit in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving ondersteunen. (Zie Par. A146)
Control activities	Interne beheersingsactiviteiten
26. The auditor shall obtain an understanding of the control activities component, through performing risk assessment procedures, by: (Ref: Para. A147–A157) (a) Identifying controls that address risks of material misstatement at the assertion level in the control activities component as follows: (i) Controls that address a risk that is determined to be a significant risk; (Ref: Para. A158–A159) (ii) Controls over journal entries, including non- standard journal entries used to record non- recurring, unusual transactions or adjustments; (Ref: Para. A160–A161) (iii) Controls for which the auditor plans to test operating effectiveness in determining the nature, timing and extent of substantive testing, which shall include controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence; and (Ref: Para. A162– A164) (iv) Other controls that the auditor considers are appropriate to enable the auditor to meet the objectives of paragraph 13 with respect to risks at the assertion level, based on the auditor's professional judgment; (Ref: Para. A165)	26 De accountant dient inzicht te verwerven in de component 'interne beheersingsactiviteiten' door middel van uitvoering van risico-inschattingswerkzaamheden, door: (Zie Par. A147 – A157) a Het identificeren van interne beheersingsmaatregelen die inspelen op risico's op een afwij- king van materieel belang op het niveau van beweringen in de component 'interne beheer- singsactiviteiten' als volgt: i Interne beheersingsmaatregelen die inspelen op een risico dat is bepaald als een signifi- cant risico; (Zie Par. A158 – A159) ii Interne beheersingsmaatregelen met betrekking tot journaalboekingen, inclusief niet-standaard journaalboekingen die worden gebruikt om niet-terugkerende, ongebruikelijke transacties of aanpassingen vast te leggen; (Zie Par. A160 – A161) iii Interne beheersingsmaatregelen waarvoor de accountant van plan is de effectieve wer- king te toetsen bij het bepalen van de aard, timing en omvang van gegevensgerichte werkzaamheden, waaronder interne beheersingsmaatregelen die inspelen op risico's waarvoor gegevensgerichte werkzaamheden alleen geen voldoende en geschikte con- trole-informatie bieden[A34]; en (Zie Par. A162 – A164) iv Andere interne beheersingsmaatregelen waarvan de accountant overweegt dat deze ge- schikt zijn om de accountant in staat te stellen de doelstellingen van paragraaf 13 te be- reiken met betrekking tot risico's op het niveau van beweringen, op basis van de professi- onele oordeelsvorming van de accountant. (Zie Par. A165)
(b) Based on controls identified in (a), identifying the IT applications and the other aspects of the entity's IT environment that are subject to risks arising from the use of IT; (Ref: Para. A166–A172) (c) For such IT applications and other aspects of the IT environment identified in (b), identifying: (Ref: Para. A173–A174) (i) The related risks arising from the use of IT; and (ii) The entity's general IT controls that address such risks; and	b Gebaseerd op de onder (a) geïdentificeerde interne beheersingsmaatregelen, het identifice- ren van de IT-applicaties en de andere aspecten van de IT-omgeving van de entiteit die on- derhevig zijn aan risico's die voortkomen uit het gebruik van IT; (Zie Par. A166 – A172) c Voor dergelijke IT-applicaties en andere aspecten van de IT-omgeving geïdentificeerd in (b), het identificeren van: (Zie Par. A173 - A174) i De bijbehorende risico's die voortkomen uit het gebruik van IT; en ii De general IT-controls van de entiteit die inspelen op dergelijke risico's; en
(d) For each control identified in (a) or (c)(ii): (Ref: Para. A175–A181) (i) Evaluating whether the control is designed effectively to address the risk of material misstatement at the assertion level, or effectively designed to support the operation of other controls; and (ii) Determining whether the control has been implemented by performing procedures in addition to inquiry of the entity's personnel.	d Voor elke interne beheersingsmaatregel onder (a) of (c) (ii): (Zie Par. A175 – A181) i Te evalueren of de interne beheersingsmaatregel effectief is opgezet om in te spelen op het risico op een afwijking van materieel belang op het niveau van beweringen, of effec- tief is opgezet om de werking van andere interne beheersingsmaatregelen te ondersteu- nen; en ii Te bepalen of de interne beheersingsmaatregel is geïmplementeerd door het uitvoeren van werkzaamheden in aanvulling op verzoeken om inlichtingen bij het personeel van de entiteit.
Control Deficiencies Within the Entity's System of Internal Control 27. Based on the auditor's evaluation of each of the components of the entity's system of internal control, the auditor shall determine whether one or more control deficiencies have been identified. (Ref: Para. A182–A183)	Tekortkomingen binnen het interne beheersingssysteem van de entiteit 27 Gebaseerd op de [A35]evaluatie door de accountant van elk van de componenten van het interne be- heersingssysteem van de entiteit, dient de accountant te bepalen of een of meer tekortkomingen in de interne beheersing zijn geïdentificeerd. (Zie Par. A182 - A183)
Identifying and Assessing the Risks of Material Misstatement (Ref: Para. A184–A185)	Het identificeren en inschatten van de risico's op een afwijking van materieel belang (Zie Par. A184 – A185)
Identifying Risks of Material Misstatement 28. The auditor shall identify the risks of material misstatement and determine whether they exist at: (Ref: Para. A186–A192) (a) The financial statement level; (Ref: Para. A193–A200) or	Identificeren van risico's op een afwijking van materieel belang 28 De accountant dient de risico's op een afwijking van materieel belang te identificeren en te bepa- len of deze bestaan op: (Zie Par. A186 - A192) a Het niveau van de financiële overzichten; (Zie Par. A193 – A200) of

(b) The assertion level for classes of transactions, account balances and disclosures. (Ref: Para. A201)	b Het niveau van beweringen voor transactiestromen, rekeningsaldi en toelichtingen. (Zie Par. A201)
29. The auditor shall determine the relevant assertions and the related significant classes of transactions, account balances and disclosures. (Ref: Para. A202–A204)	29 De accountant dient de relevante beweringen en de bijbehorende significante transactiestromen, rekeningsaldi en toelichtingen te bepalen. (Zie Par. A202 – A204)
Assessing Risks of Material Misstatement at the Financial Statement Level	Het inschatten van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten
30. For identified risks of material misstatement at the financial statement level, the auditor shall assess the risks and: (Ref: Para. A193–A200) (a) Determine whether such risks affect the assessment of risks at the assertion level; and (b) Evaluate the nature and extent of their pervasive effect on the financial statements.	30 Voor geïdentificeerde risico's op een afwijking van materieel belang op het niveau van de financi- ele overzichten, dient de accountant de risico's in te schatten en: (Zie Par. A193 – A200) a Te bepalen of dergelijke risico's de inschatting van risico's op het niveau van beweringen be-invloeden; en b De aard en omvang van hun diepgaande invloed op de financiële overzichten te evalueren.
Assessing Risks of Material Misstatement at the Assertion Level Assessing Inherent Risk (Ref: Para. A205–A217)	Inschatting van risico's op een afwijking van materieel belang op het niveau van beweringen Inschatting van het inherente risico (Zie Par. A205 – A217)
31. For identified risks of material misstatement at the assertion level, the auditor shall assess inherent risk by assessing the likelihood and magnitude of misstatement. In doing so, the auditor shall take into account how, and the degree to which: (a) Inherent risk factors affect the susceptibility of relevant assertions to misstatement; and (b) The risks of material misstatement at the financial statement level affect the assessment of inherent risk for risks of material misstatement at the assertion level. (Ref: Para. A215–A216)	31 Voor geïdentificeerde risico's op een afwijking van materieel belang op het niveau van bewerin- gen, dient de accountant het inherente risico in te schatten door de waarschijnlijkheid en de orde van grootte [A36]van een afwijking in te schatten. Daarbij dient de accountant rekening te houden met hoe en in welke mate: a Inherente risicofactoren de vatbaarheid van relevante beweringen voor afwijkingen beïnvloe-den; en b De risico's op een afwijking van materieel belang op het niveau van de financiële overzichten de inschatting van inherent risico voor risico's op een afwijking van materieel belang op het niveau van beweringen beïnvloeden. (Zie Par. A215 – A216)
32. The auditor shall determine whether any of the assessed risks of material misstatement are significant risks. (Ref: Para. A218–A221)	32 De accountant dient te bepalen of een of meer [A37]van de ingeschatte risico's op een afwijking van materieel belang een significant risico is. (Zie Par. A218 – A221)
33. The auditor shall determine whether substantive procedures alone cannot provide sufficient appropriate audit evidence for any of the risks of material misstatement at the assertion level. (Ref: Para. A222–A225)	33 De accountant dient te bepalen of gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie kunnen verschaffen voor de risico's op een afwijking van materieel belang op het niveau van beweringen. (Zie Par. A222 - A225)
Assessing Control Risk	Inschatting van het interne beheersingsrisico
34. If the auditor plans to test the operating effectiveness of controls, the auditor shall assess control risk. If the auditor does not plan to test the operating effectiveness of controls, the auditor's assessment of control risk shall be such that the assessment of the risk of material misstatement is the same as the assessment of inherent risk. (Ref: Para. A226–A229)	34 Als de accountant van plan is de effectieve werking van interne beheersingsmaatregelen te toet- sen, dient de accountant het interne beheersingsrisico in te schatten. Als de accountant niet van plan is om de effectieve werking van interne beheersingsmaatregelen te toetsen, dient zijn in-schatting van het interne beheersingsrisico zodanig te zijn dat de inschatting van het risico op een afwijking van materieel belang hetzelfde is als de inschatting van inherent risico. (Zie Par. A226 – A229)
Evaluating the Audit Evidence Obtained from the Risk Assessment Procedures 35. The auditor shall evaluate whether the audit evidence obtained from the risk assessment procedures provides an appropriate basis for the identification and assessment of the risks of material misstatement. If not, the auditor shall perform additional risk assessment procedures until audit evidence has been obtained to provide such a basis. In identifying and assessing the risks of material misstatement, the auditor shall take into account all audit evidence obtained from the risk assessment procedures, whether corroborative or contradictory to assertions made by management. (Ref: Para. A230–A232)	Evalueren van de controle-informatie verkregen uit de risico-inschattingswerkzaamheden 35 De accountant dient te evalueren of de controle-informatie verkregen uit de risico-inschattings- werkzaamheden een geschikte basis verschaft voor de identificatie en inschatting van de risico's op een afwijking van materieel belang. Zo niet, dan dient de accountant aanvullende risico-in-schattingswerkzaamheden uit te voeren totdat controle-informatie is verkregen om een dergelijke basis te verschaffen. Bij het identificeren en inschatten van de risico's op een afwijking van mate- rieel belang, dient de accountant rekening te houden met alle controle-informatie verkregen uit de risico-inschattingswerkzaamheden, hetzij bevestigend of tegenstrijdig met beweringen van het management. (Zie Par. A230 - A232)

Classes of Transactions, Account Balances and Disclosures that Are Not Significant, but Which Are Material 36. For material classes of transactions, account balances or disclosures that have not been determined to be significant classes of transactions, account balances or disclosures, the auditor shall evaluate whether the auditor's determination remains appropriate. (Ref: Para. A233–A235) Revision of Risk Assessment 37. If the auditor obtains new information which is inconsistent with the audit evidence on which the auditor originally based the identification or assessments of the risks of material misstatement, the auditor shall revise the identification or assessment. (Ref: Para. A236) Documentation 38. The auditor shall include in the audit documentation:13 (Ref: Para. A237–A241) (a) The discussion among the engagement team and the significant decisions reached; (b) Key elements of the auditor's understanding in accordance with paragraphs 19, 21, 22, 24 and 25; the sources of information from which the auditor's understanding was obtained; and the risk assessment procedures performed; (c) The evaluation of the design of identified controls, and determination whether such controls have been implemented, in accordance with the requirements in paragraph 26; and (d) The identified and assessed risks of material misstatement at the financial statement level and at the assertion level, including significant risks and risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence, and the rationale for the significant judgments made.	Transactiestromen, rekeningsaldi en toelichtingen die niet significant zijn, maar die wel van materieel belang zijn 36 Voor van materieel belang zijnde transactiestromen, rekeningsaldi of toelichtingen die niet als significante transactiestromen, rekeningsaldi of toelichtingen zijn vastgesteld[A38], dient de accountant te evalueren of deze vaststelling [A39]geschikt blijft. (Zie Par. A233 – A235) Herziening van de risico-inschatting 37 Als de accountant nieuwe informatie verkrijgt die niet consistent is met de controle-informatie waarop de accountant oorspronkelijk de identificatie of inschattingen van de risico's op een afwij- king van materieel belang baseerde, dient de accountant de identificatie of inschatting te herzien. (Zie Par. A236) Documentatie 38 De accountant dient in de controledocumentatie op te nemen:13 (Zie Par. A237 – A241) a De bespreking tussen het opdrachtteam en de significante beslissingen die zijn genomen; b De belangrijke elementen van het verworven inzicht van de accountant in overeenstemming met paragrafen 19, 21, 22, 24 en 25; de informatiebronnen waaruit het inzicht van de accoun- tant is verkregen; en de uitgevoerde risico-inschattingswerkzaamheden; c De evaluatie van de opzet van geïdentificeerde interne beheersingsmaatregelen, en de bepa- ling of dergelijke interne beheersingsmaatregelen geïmplementeerd zijn in overeenstemming met de vereisten in paragraaf 26; en d De geïdentificeerde en ingeschatte risico's op een afwijking van materieel belang op het ni- veau van de financiële overzichten en op het niveau van beweringen, inclusief significante risico's en risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en ge- schikte controle-informatie kunnen verschaffen, en de beweegreden [A40]voor de significante oor- deelsvormingen die gemaakt zijn.

Application and Other Explanatory Material Definitions (Ref: Para. 12) Assertions (Ref: Para. 12(a)) A1. Categories of assertions are used by auditors to consider the different types of potential misstatements that may occur when identifying, assessing and responding to the risks of material misstatement. Examples of these categories of assertions are described in paragraph A190. The assertions differ from the written representations required by ISA 580,14 to confirm certain matters or support other audit evidence. Controls (Ref: Para. 12(c)) A2. Controls are embedded within the components of the entity's system of internal control. A3. Policies are implemented through the actions of personnel within the entity, or through the restraint of personnel from taking actions that would conflict with such policies. A4. Procedures may be mandated, through formal documentation or other communication by management or those charged with governance, or may result from behaviors that are not mandated but are rather conditioned by the entity's culture. Procedures may be enforced through the actions permitted by the IT applications used by the entity or other aspects of the entity's IT environment. A5. Controls may be direct or indirect. Direct controls are controls that are precise enough to address risks of material misstatement at the assertion level. Indirect controls are controls that support direct controls. Information Processing Controls (Ref: Para. 12(e)) A6. Risks to the integrity of information arise from susceptibility to ineffective implementation of the entity's information policies, which are policies that define the information flows, records and reporting processes in the entity's information system. Information processing controls are procedures that support effective implementation of the entity's information policies. Information processing controls 14 ISA 580, Written Representations may be automated (i.e., embedded in IT applications) or manual (e.g., input or output controls) and may rely on other controls, including other information processing controls or general IT controls. Inherent Risk Factors (Ref: Para. 12(f)) A7. Inherent risk factors may be qualitative or quantitative and affect the susceptibility of assertions to misstatement. Qualitative inherent risk factors relating to the preparation of information required by the applicable financial reporting framework include: • Complexity; • Subjectivity; • Change; • Uncertainty; or • Susceptibility to misstatement due to management bias or other fraud risk factors insofar as they affect inherent risk.	Toepassingsgerichte en overige verklarende teksten Definities (Zie Par. 12) Beweringen (Zie Par. 12(a)) A1 Categorieën van beweringen worden bij het identificeren, inschatten en inspelen op de risico's op een afwijking van materieel belang door accountants gebruikt om de verschillende soorten potentiële afwijkingen van materieel belang die kunnen voorkomen te overwegen. Voorbeelden van deze categorieën beweringen worden beschreven in paragraaf A190. De beweringen ver- schillen van de schriftelijke bevestigingen vereist door Standaard 58014 om bepaalde aangele- genheden te bevestigen of andere controle-informatie te ondersteunen. Interne beheersingsmaatregelen (Zie Par. 12(c)) A2 Interne beheersingsmaatregelen zijn ingebed in de componenten van het interne beheersings-systeem van de entiteit. A3 Beleidslijnen worden geïmplementeerd door de handelingen van het personeel binnen de enti- teit, of door de terughoudendheid van het personeel om handelingen te ondernemen die in strijd zouden zijn met dergelijke beleidslijnen. A4 Procedures kunnen verplicht worden gesteld door formele documentatie of andere communica- tie door het management of de met governance belaste personen, of kunnen het gevolg zijn van gedragingen die niet verplicht zijn maar eerder bepaald worden door de cultuur van de en- titeit. Procedures kunnen worden afgedwongen door de acties die worden toegestaan door de door de entiteit gebruikte IT-applicaties of andere aspecten van de IT-omgeving van de entiteit. A5 Interne beheersingsmaatregelen kunnen direct of indirect zijn. Directe interne beheersings-maatregelen zijn interne beheersingsmaatregelen die nauwkeurig genoeg zijn om in te spelen 13 Standaard 230, Controledocumentatie, paragrafen 8-11 en A6–A7. 14 Standaard 580, Schriftelijke bevestigingen. op risico's op een afwijking van materieel belang op het niveau van beweringen. Indirecte in- terne beheersingsmaatregelen zijn interne beheersingsmaatregelen die directe interne beheer-singsmaatregelen ondersteunen. Interne beheersingsmaatregelen met betrekking tot informatieverwerking (Zie Par. 12(e)) A6 Risico's voor de integriteit van informatie komen voort uit vatbaarheid voor een ineffectieve im- plementatie van de informatiebeleidslijnen van de entiteit; dit zijn beleidslijnen die de informa-tiestromen, vastleggingen en processen inzake financiële verslaggeving in het informatiesys- teem van de entiteit definiëren. Interne beheersingsmaatregelen met betrekking tot informatie- verwerking zijn procedures die effectieve implementatie van de informatiebeleidslijnen van de entiteit ondersteunen. Interne beheersingsmaatregelen met betrekking tot informatieverwerking kunnen geautomatiseerd zijn (d.w.z. ingebed in IT-applicaties) of handmatig (bijvoorbeeld in- terne beheersingsmaatregelen met betrekking tot in- of uitvoer) en kunnen steunen op andere interne beheersingsmaatregelen, waaronder die met betrekking tot informatieverwerking of ge- neral IT controls. Inherente risicofactoren (Zie Par. 12(f)) A7 Inherente risicofactoren kunnen kwalitatief of kwantitatief zijn en de vatbaarheid van bewerin-gen voor afwijkingen beïnvloeden. Kwalitatieve inherente risicofactoren met betrekking tot het

	opstellen van informatie, vereist door het van toepassing zijnde stelsel inzake financiële verslaggeving, omvatten: • complexiteit; • subjectiviteit; • wijzigingen; • onzekerheid; of • vatbaarheid voor afwijkingen als gevolg van tendentie bij het management of andere fraude-risicofactoren voor zover ze het inherente risico beïnvloeden.
A8. Other inherent risk factors, that affect susceptibility to misstatement of an assertion about a class of transactions, account balance or disclosure may include: • The quantitative or qualitative significance of the class of transactions, account balance or disclosure; or • The volume or a lack of uniformity in the composition of the items to be processed through the class of transactions or account balance, or to be reflected in the disclosure.	A8 Andere inherente risicofactoren, die van invloed zijn op de vatbaarheid van een bewering met betrekking tot een transactiestroom, rekeningsaldo of toelichting voor een afwijking kunnen omvatten: • de kwantitatieve of kwalitatieve significantie van de transactiestroom, rekeningsaldo of toelichting; of • de hoeveelheid of een gebrek aan uniformiteit in de samenstelling van de elementen die moeten worden verwerkt via de transactiestroom of het rekeningsaldo, of weergegeven in de toelichting.
Relevant Assertions (Ref: Para. 12(h)) A9. A risk of material misstatement may relate to more than one assertion, in which case all the assertions to which such a risk relates are relevant assertions. If an assertion does not have an identified risk of material misstatement, then it is not a relevant assertion.	Relevante beweringen (Zie Par. 12(h)) A9 Een risico op een afwijking van materieel belang kan betrekking hebben op meer dan één bewering, in welk geval alle beweringen waarop een dergelijk risico betrekking heeft, relevante beweringen zijn. Als een bewering geen geïdentificeerd risico heeft op een afwijking van mate- rieel belang, dan is het geen relevante bewering.
Significant Risk (Ref: Para. 12(l)) A10. Significance can be described as the relative importance of a matter, and is judged by the auditor in the context in which the matter is being considered. For inherent risk, significance may be considered in the context of how, and the degree to which, inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur.	Significant risico (Zie Par. 12(l)) A10 Significantie kan worden omschreven als het relatieve belang van een aangelegenheid en wordt ingeschat door de accountant in de context waarin de aangelegenheid wordt overwogen. Significantie kan worden overwogen door na te gaan in hoeverre inherente risicofactoren van invloed zijn op de waarschijnlijkheid dat een afwijking voorkomt en de orde van grootte van de potentiële afwijking indien die afwijking zou voorkomen.
Risk Assessment Procedures and Related Activities (Ref: Para. 13–18) A11. The risks of material misstatement to be identified and assessed include both those due to fraud and those due to error, and both are covered by this ISA. However, the significance of fraud is such that further requirements and guidance are included in ISA 240 in relation to risk assessment procedures and related activities to obtain information that is used to identify and assess the risks of material misstatement due to fraud.15 In addition, the following ISAs provide further requirements and guidance on identifying and assessing risks of material misstatement regarding specific matters or circumstances: • ISA 540 (Revised)16 in regard to accounting estimates; • ISA 55022 in regard to related party relationships and transactions; • ISA 570 (Revised)17 in regard to going concern; and • ISA 60018 in regard to group financial statements.	Risico-inschattingswerkzaamheden en daarmee verband houdende werkzaamheden (Zie Par. 13–18) A11 De risico’s op een afwijking van materieel belang die moeten worden geïdentificeerd en ingeschat, omvatten zowel die het gevolg zijn van fraude als die welke het gevolg zijn van fouten en beide worden in deze Standaard behandeld. De significantie van fraude is echter zodanig dat verdere vereisten en leidraden zijn opgenomen in Standaard 240 met betrekking tot risico-inschattingswerkzaamheden en daarmee verband houdende werkzaamheden om informatie te verkrijgen die wordt gebruikt om de risico’s op een afwijking van materieel belang als gevolg van fraude te identificeren en in te schatten.15 Bovendien bieden de volgende Standaarden na- dere vereisten en leidraden voor het identificeren en inschatten van risico's op een afwijking van materieel belang met betrekking tot specifieke aangelegenheden of omstandigheden: • Standaard 54016 met betrekking tot schattingen; • Standaard 55022 met betrekking tot relaties en transacties met verbonden partijen; • Standaard 57017 met betrekking tot continuïteit; en • Standaard 60018 met betrekking tot financiële overzichten van de groep.
A12. Professional skepticism is necessary for the critical assessment of audit evidence gathered when performing the risk assessment procedures, and assists the auditor in remaining alert to audit evidence that is not biased towards corroborating the existence of risks or that may be contradictory to the existence of risks. Professional	A12 Een professioneel-kritische instelling is noodzakelijk voor de kritische evaluatie van verzamelde controle-informatie bij het uitvoeren van de risico-inschattingswerkzaamheden. Deze instelling helpt

skepticism is an attitude that is applied by the auditor when making professional judgments that then provides the basis for the auditor's actions. The auditor applies professional judgment in determining when the auditor has audit evidence that provides an appropriate basis for risk assessment.
A13. The application of professional skepticism by the auditor may include:
- Questioning contradictory information and the reliability of documents;
- Considering responses to inquiries and other information obtained from management and those charged with governance;
- Being alert to conditions that may indicate possible misstatement due to fraud or error; and
- Considering whether audit evidence obtained supports the auditor's identification and assessment of the risks of material misstatement in light of the entity's nature and circumstances.

Why Obtaining Audit Evidence in an Unbiased Manner Is Important (Ref: Para. 13)
A14. Designing and performing risk assessment procedures to obtain audit evidence to support the identification and assessment of the risks of material misstatement in an unbiased manner may assist the auditor in identifying potentially contradictory information, which may assist the auditor in exercising professional skepticism in identifying and assessing the risks of material misstatement.

15 ISA 240, paragraphs 12–27
16 ISA 540 (Revised), Auditing Accounting Estimates and Related Disclosures
17 ISA 570 (Revised), Going Concern
18 ISA 600, Special Considerations—Audits of Group Financial Statements (Including the Work of Component Auditors)

Sources of Audit Evidence (Ref: Para. 13)
A15. Designing and performing risk assessment procedures to obtain audit evidence in an unbiased manner may involve obtaining evidence from multiple sources within and outside the entity. However, the auditor is not required to perform an exhaustive search to identify all possible sources of audit evidence. In addition to information from other sources19, sources of information for risk assessment procedures may include:
- Interactions with management, those charged with governance, and other key entity personnel, such as internal auditors.
- Certain external parties such as regulators, whether obtained directly or indirectly.
- Publicly available information about the entity, for example entity-issued press releases, materials for analysts or investor group meetings, analysts' reports or information about trading activity.

Regardless of the source of information, the auditor considers the relevance and reliability of the information to be used as audit evidence in accordance with ISA 500.20

de accountant alert te blijven voor controle informatie die niet tendeert naar het bevesti- gen van het bestaan van risico's of die tegenstrijdig kan zijn met het bestaan van risico's. Een professioneel-kritische instelling is een houding die door de accountant wordt toegepast wan- neer professionele oordeelsvormingen worden gemaakt die vervolgens de basis vormen voor de handelingen van de accountant. De accountant past professionele oordeelsvorming toe bij het bepalen wanneer de accountant controle-informatie heeft die een geschikte basis verschaft voor risico-inschatting.

A13 De toepassing van een professioneel-kritische instelling door de accountant kan omvatten:
- tegenstrijdige informatie en de betrouwbaarheid van documenten ter discussie stellen;
- overwegen van reacties op verzoeken om inlichtingen en andere informatie verkregen van het management en de met governance belaste personen;
- alert zijn op omstandigheden die kunnen wijzen op mogelijke afwijking als gevolg van fraude of fouten; en
- overwegen of de verkregen controle-informatie de identificatie en inschatting van de risico's op een afwijking van materieel belang van de accountant ondersteunt in het licht van de aard en omstandigheden van de entiteit.

Waarom het verkrijgen van controle-informatie op een niet-tendentieuze manier belangrijk is (Zie Par. 13)
A14 Het opzetten en uitvoeren van risico-inschattingswerkzaamheden om controle-informatie te verkrijgen ter ondersteuning van de identificatie en inschatting van de risico's op een afwijking van materieel belang op een niet-tendentieuze manier kan de accountant helpen bij het identifi- ceren van mogelijk tegenstrijdige informatie. Die informatie kan de accountant helpen bij het uitoefenen van een professioneel-kritische instelling bij het identificeren en inschatten van de risico's op een afwijking van materieel belang.

Bronnen van controle-informatie (Zie Par. 13)
A15 Risico-inschattingswerkzaamheden opzetten en uitvoeren om op een niet tendentieuze manier controle-informatie te verkrijgen kan bestaan uit het verkrijgen van informatie uit meerdere bronnen binnen en buiten de entiteit. De accountant hoeft echter niet een volledige zoekop- dracht uit te voeren om alle mogelijke bronnen van controle-informatie te identificeren. Naast informatie uit andere bronnen19, kunnen informatiebronnen voor risico-inschattingswerkzaam- heden omvatten:
- interacties met het management, de met governance belaste personen en ander personeel van de entiteit op sleutelposities, zoals interne auditors;
- bepaalde externe partijen zoals regelgevers of toezichthouders, ongeacht of deze direct of indirect zijn verkregen;
- openbaar beschikbare informatie over de entiteit, bijvoorbeeld door de entiteit uitgegeven persberichten, materialen voor analisten of vergaderingen van investeerdersgroepen, ana- listenrapporten of informatie over handelsactiviteit.

15 Standaard 240, paragrafen 12–27.
16 Standaard 540, De controle van schattingen en toelichtingen daarop.
17 Standaard 570, Continuïteit.
18 Standaard 600, Speciale overwegingen — Controles van financiële overzichten van de groep (inclusief het werk van groeps- accountants).
19 Zie de paragrafen A37 en A38.

Ongeacht de informatiebron houdt de accountant rekening met de relevantie en betrouwbaarheid van de informatie die moet worden gebruikt als controle-informatie in overeenstemming met Standaard 500.20

Scalability (Ref: Para. 13) A16. The nature and extent of risk assessment procedures will vary based on the nature and circumstances of the entity (e.g., the formality of the entity's policies and procedures, and processes and systems). The auditor uses professional judgment to determine the nature and extent of the risk assessment procedures to be performed to meet the requirements of this ISA. A17. Although the extent to which an entity's policies and procedures, and processes and systems are formalized may vary, the auditor is still required to obtain the understanding in accordance with paragraphs 19, 21, 22, 24, 25 and 26. 19 See paragraphs A37 and A38. 20 ISA 500, Audit Evidence, paragraph 7 A18. The nature and extent of risk assessment procedures to be performed the first time an engagement is undertaken may be more extensive than procedures for a recurring engagement. In subsequent periods, the auditor may focus on changes that have occurred since the preceding period. Types of Risk Assessment Procedures (Ref: Para. 14) A19. ISA 50021 explains the types of audit procedures that may be performed in obtaining audit evidence from risk assessment procedures and further audit procedures. The nature, timing and extent of the audit procedures may be affected by the fact that some of the accounting data and other evidence may only be available in electronic form or only at certain points in time.22 The auditor may perform substantive procedures or tests of controls, in accordance with ISA 330, concurrently with risk assessment procedures, when it is efficient to do so. Audit evidence obtained that supports the identification and assessment of risks of material misstatement may also support the detection of misstatements at the assertion level or the evaluation of the operating effectiveness of controls. A20. Although the auditor is required to perform all the risk assessment procedures described in paragraph 14 in the course of obtaining the required understanding of the entity and its environment, the applicable financial reporting framework, and the entity's system of internal control (see paragraphs 19–26), the auditor is not required to perform all of them for each aspect of that understanding. Other procedures may be performed when the information to be obtained may be helpful in identifying risks of material misstatement. Examples of such procedures may include making inquiries of the entity's external legal counsel or external supervisors, or of valuation experts that the entity has used. Automated Tools and Techniques (Ref: Para. 14) A21.Using automated tools and techniques, the auditor may perform risk assessment procedures on large volumes of data (from the general ledger, sub-ledgers or other operational data) including for analysis, recalculations, reperformance or reconciliations. Inquiries of Management and Others within the Entity (Ref: Para. 14(a)) Why Inquiries Are Made of Management and Others Within the Entity	Schaalbaarheid (Zie Par. 13) A16 De aard en omvang van risico-inschattingswerkzaamheden zullen variëren op basis van de aard en omstandigheden van de entiteit (bijvoorbeeld mate waarin de beleidslijnen, procedu- res, processen en systemen van de entiteit geformaliseerd zijn). De accountant past professio- nele oordeelsvorming toe om de aard en omvang van de risico-inschattingswerkzaamheden die moeten worden uitgevoerd om aan de vereisten van deze Standaard te voldoen, te bepa- len. A17 Hoewel de mate waarin de beleidslijnen, procedures, processen en systemen van een entiteit zijn geformaliseerd kan variëren, wordt van de accountant nog steeds vereist om het inzicht te verwerven in overeenstemming met paragrafen 19, 21, 22, 24, 25 en 26. A18 De aard en omvang van risico-inschattingswerkzaamheden die moeten worden uitgevoerd bij de eerste keer dat een opdracht wordt uitgevoerd, kunnen uitgebreider zijn dan werkzaamhe- den voor een doorlopende opdracht. In opvolgende verslagperiodes kan de accountant zich richten op veranderingen die zich sinds de voorgaande verslagperiode hebben voorgedaan. Soorten risico-inschattingswerkzaamheden (Zie Par. 14) A19 Standaard 50021 legt de soorten controlewerkzaamheden uit die kunnen worden uitgevoerd bij het verkrijgen van controle-informatie van risico-inschattingswerkzaamheden en verdere con- trolewerkzaamheden. De aard, timing en omvang van de controlewerkzaamheden kunnen wor- den beïnvloed door het feit dat sommige van de administratieve gegevens en andere informa- tie mogelijk alleen beschikbaar zijn in elektronische vorm of alleen op bepaalde tijdstippen.22 De accountant kan gegevensgerichte controles of toetsingen van interne beheersingsmaatre- gelen uitvoeren, in overeenstemming met Standaard 330, gelijktijdig met risico inschattings- werkzaamheden wanneer dit efficiënt is om te doen. Verkregen controle-informatie die de iden- tificatie en inschatting van risico's op een afwijking van materieel belang ondersteunt kan ook de detectie van afwijkingen op het niveau van beweringen of de evaluatie van de effectieve werking van interne beheersingsmaatregelen ondersteunen. A20 Hoewel van de accountant vereist wordt om alle in paragraaf 14 beschreven risico-inschat- tingswerkzaamheden uit te voeren bij het verwerven van het vereiste inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het interne beheersingssysteem van de entiteit (zie paragrafen 19–26), wordt van de accountant niet ver- eist om ze allemaal uit te voeren voor elk aspect van dat inzicht. Andere werkzaamheden kun- nen worden uitgevoerd wanneer de te verkrijgen informatie nuttig kan zijn bij het identificeren van risico's op afwijkingen van materieel belang. Voorbeelden van dergelijke werkzaamheden kunnen het verzoeken om inlichtingen zijn bij de externe juridisch adviseur of externe toezicht- houders van de entiteit, of van waarderingsdeskundigen die de entiteit heeft gebruikt. Geautomatiseerde hulpmiddelen en technieken (Zie Par. 14) 20 Standaard 500, Controle-informatie, paragraaf 7. 21 Standaard 500, paragrafen A14–A17 en A21–A25. 22 Standaard 500, paragraaf A12. A21 Gebruikmakend van geautomatiseerde hulpmiddelen en technieken, kan de accountant alge- mene risico-inschattingswerkzaamheden uitvoeren op grote aantallen gegevens (van het groot- boek, subgrootboeken of andere operationele gegevens) alsmede voor analyse, herberekenin- gen, opnieuw uitvoeren of aansluitingen.

A22. Information obtained by the auditor to support an appropriate basis for the identification and assessment of risks, and the design of further audit procedures, may be obtained through inquiries of management and those responsible for financial reporting.
A23. Inquiries of management and those responsible for financial reporting and of other appropriate individuals within the entity and other employees with different levels of authority may offer the auditor varying perspectives when identifying and assessing risks of material misstatement.

Examples:
- Inquiries directed towards those charged with governance may help the auditor understand the extent of oversight by those charged with governance over the preparation of the financial statements by management. ISA 260 (Revised)23 identifies the importance of effective two-way communication in assisting the auditor to obtain information from those charged with governance in this regard.
- Inquiries of employees responsible for initiating, processing or recording complex or unusual transactions may help the auditor to evaluate the appropriateness of the selection and application of certain accounting policies.
- Inquiries directed towards in-house legal counsel may provide information about such matters as litigation, compliance with laws and regulations, knowledge of fraud or suspected fraud affecting the entity, warranties, post-sales obligations, arrangements (such as joint ventures) with business partners, and the meaning of contractual terms.
- Inquiries directed towards marketing or sales personnel may provide information about changes in the entity's marketing strategies, sales trends, or contractual arrangements with its customers.
- Inquiries directed towards the risk management function (or inquiries of those performing such roles) may provide information about operational and regulatory risks that may affect financial reporting.
- Inquiries directed towards IT personnel may provide information about system changes, system or control failures, or other IT-related risks.

Considerations Specific to Public Sector Entities
A24. When making inquiries of those who may have information that is likely to assist in identifying risks of material misstatement, auditors of public sector entities may obtain information from additional sources such as from the auditors that are involved in performance or other audits related to the entity.

Verzoeken om inlichtingen bij het management en anderen binnen de entiteit (Zie Par. 14(a))
Waarom verzoeken om inlichtingen worden gedaan bij het management en anderen binnen de entiteit

A22 Informatie verkregen door de accountant ter ondersteuning van een geschikte basis voor de identificatie en inschatting van risico's en het opzetten van verdere controlewerkzaamheden, kan worden verkregen door middel van verzoeken om inlichtingen bij het management en de- genen die verantwoordelijk zijn voor financiële verslaggeving.

A23 Verzoeken om inlichtingen bij het management, degenen die verantwoordelijk zijn voor de financiële verslaggeving, andere geschikte personen binnen de entiteit en andere werknemers met verschillende beslissingsbevoegdheden kunnen de accountant verschillende perspectie- ven bieden bij het identificeren en inschatten van risico's op een afwijking van materieel be- lang.
Voorbeelden
• Verzoeken om inlichtingen gericht aan de met governance belaste personen kunnen de accountant helpen inzicht te verwerven in de mate van toezicht door de met governance belaste personen op het opstellen van de financiële overzichten door het management. Standaard 260 23 onderkent het belang van effectieve wederzijdse communicatie om de accountant te helpen in dit verband informatie te verkrijgen van de met
governance belaste personen.
• Verzoeken om inlichtingen bij werknemers die verantwoordelijk zijn voor het initiëren, verwerken of vastleggen van complexe of ongebruikelijke transacties kunnen de accountant helpen bij het evalueren in welke mate de keuze en toepassing van bepaalde grondslagen voor financiële verslaggeving passend zijn.
• Verzoeken om inlichtingen bij de interne juridische adviseur kunnen informatie verstrekken over aangelegenheden als rechtszaken, de naleving van wet- en regelgeving, kennis van fraude of vermoede fraude die de entiteit beïnvloedt, garanties, verplichtingen
na verkoop, overeenkomsten (zoals joint ventures) met zakenpartners en de betekenis van contractuele bepalingen.
• Verzoeken om inlichtingen bij marketing- of verkooppersoneel kunnen informatie verschaffen over wijzigingen in de marketingstrategieën van de entiteit, verkooptrends of contractuele overeenkomsten met de klanten.
• Verzoeken om inlichtingen gericht op de risicomanagementfunctie (of verzoeken om inlichtingen aan personen die dergelijke rollen uitvoeren) kunnen informatie verschaffen over operationele en wettelijke risico's die van invloed kunnen zijn op de financiële verslaggeving.
• Verzoeken om inlichtingen gericht aan IT-personeel kunnen informatie verschaffen
over systeemwijzigingen, falen van systeem- of interne beheersing, of andere ITgerelateerde risico's.

Overwegingen specifiek voor entiteiten in de publieke sector

A24 Bij verzoeken om inlichtingen bij personen die informatie kunnen hebben die waarschijnlijk zal helpen bij het identificeren van risico's op een afwijking van materieel belang, kunnen accoun- tants van entiteiten in de publieke sector informatie verkrijgen van aanvullende informatiebron- nen zoals van de accountants die betrokken zijn bij doelmatigheids- of andere controles met betrekking tot de entiteit.

23 Standaard 260, Communicatie met de met governance belaste personen, paragraaf 4(b).

Inquiries of the Internal Audit Function Why inquiries are made of the internal audit function (if the function exists) A25. If an entity has an internal audit function, inquiries of the appropriate individuals within the function may assist the auditor in understanding the entity and its environment, and the entity's system of internal control, in the identification and assessment of risks. 23 ISA 260 (Revised), Communication with Those Charged with Governance, paragraph 4(b) Considerations specific to public sector entities A26. Auditors of public sector entities often have additional responsibilities with regard to internal control and compliance with applicable laws and regulations. Inquiries of appropriate individuals in the internal audit function may assist the auditors in identifying the risk of material non-compliance with applicable laws and regulations, and the risk of control deficiencies related to financial reporting. Analytical Procedures (Ref: Para. 14(b)) Why Analytical Procedures Are Performed as a Risk Assessment Procedure A27. Analytical procedures help identify inconsistencies, unusual transactions or events, and amounts, ratios, and trends that indicate matters that may have audit implications. Unusual or unexpected relationships that are identified may assist the auditor in identifying risks of material misstatement, especially risks of material misstatement due to fraud. A28. Analytical procedures performed as risk assessment procedures may therefore assist in identifying and assessing the risks of material misstatement by identifying aspects of the entity of which the auditor was unaware or understanding how inherent risk factors, such as change, affect susceptibility of assertions to misstatement. Types of Analytical Procedures A29. Analytical procedures performed as risk assessment procedures may: • Include both financial and non-financial information, for example, the relationship between sales and square footage of selling space or volume of goods sold (non-financial). • Use data aggregated at a high level. Accordingly, the results of those analytical procedures may provide a broad initial indication about the likelihood of a material misstatement. A30. This ISA deals with the auditor's use of analytical procedures as risk assessment procedures. ISA 52024 deals with the auditor's use of analytical procedures as substantive procedures ("substantive analytical procedures") and the auditor's responsibility to perform analytical procedures near the end of the audit. Accordingly, analytical procedures performed as risk assessment procedures are not required to be performed in accordance with the requirements of ISA 520. However, the requirements and application material in ISA 520 may provide useful guidance to the auditor when performing analytical procedures as part of the risk assessment procedures. 24 ISA 520, Analytical Procedures	Verzoeken om inlichtingen bij de interne auditfunctie Waarom verzoeken om inlichtingen worden gesteld bij de interne auditfunctie (als de functie bestaat) A25 Als een entiteit een interne auditfunctie heeft, kunnen verzoeken om inlichtingen bij de juiste personen binnen de functie de accountant helpen bij het verwerven van inzicht in de entiteit en haar omgeving en het systeem van interne beheersing van de entiteit bij het identificeren en inschatten van risico's. Overwegingen specifiek voor entiteiten in de publieke sector A26 Accountants van entiteiten in de publieke sector hebben vaak extra verantwoordelijkheden met betrekking tot interne beheersing en naleving van de van toepassing zijnde wet- en regelge- ving. Verzoeken om inlichtingen bij de juiste personen in de interne auditfunctie kunnen de ac- countants helpen bij het identificeren van het risico op niet-naleving van de van toepassing zijnde wet- en regelgeving van materieel belang en het risico op tekortkomingen in de interne beheersing met betrekking tot financiële verslaggeving. Cijferanalyses (Zie Par. 14(b)) Waarom cijferanalyses worden uitgevoerd als een van de risico-inschattingswerkzaamheden A27 Cijferanalyses helpen bij het identificeren van inconsistenties, ongebruikelijke transacties of ge- beurtenissen, bedragen, ratio's en trends die wijzen op aangelegenheden die implicaties voor de controle kunnen hebben. Ongebruikelijke of onverwachte relaties die geïdentificeerd zijn, kunnen de accountant helpen bij het identificeren van risico's op een afwijking van materieel belang; met name risico's op een afwijking van materieel belang als gevolg van fraude. A28 Cijferanalyses die worden uitgevoerd als risico-inschattingswerkzaamheden kunnen daarom helpen bij het identificeren en het inschatten van de risico's op een afwijking van materieel be- lang door aspecten van de entiteit te identificeren waarvan de accountant zich niet bewust van was of niet begreep hoe inherente risicofactoren, zoals wijzigingen, de vatbaarheid van bewe- ringen voor afwijkingen beïnvloeden. Soorten cijferanalyses A29 Cijferanalyses uitgevoerd als risico-inschattingswerkzaamheden kunnen: • zowel financiële als niet-financiële informatie omvatten, bijvoorbeeld de relatie tussen ver- koop en vierkante meters van verkooppruimte of hoeveelheid verkochte goederen (niet-fi- nancieel); • gegevens gebruiken die op een hoog niveau zijn samengevoegd. Dienovereenkomstig kunnen de resultaten van die cijferanalyses een eerste globale indicatie geven van de waarschijnlijkheid van een afwijking van materieel belang. A30 Deze Standaard behandelt het gebruik door de accountant van cijferanalyses als risico-in- schattingswerkzaamheden. Standaard 52024 behandelt het gebruik door de accountant van cij- feranalyses als gegevensgerichte werkzaamheden ('gegevensgerichte' cijferanalyses ') en de verantwoordelijkheid van de accountant om cijferanalyses nabij het einde van de controle uit te voeren. Dienovereenkomstig is het niet vereist om cijferanalyses die worden uitgevoerd als ri- sico-inschattingswerkzaamheden uit te voeren in overeenstemming met de vereisten van Stan- daard 520. Echter, de vereisten en toepassingsgerichte teksten in Standaard 520 kunnen

	24 Standaard 520, Cijferanalyses. bruikbare leidraden bieden aan de accountant bij het uitvoeren cijferanalyses als onderdeel van de risico-inschattingswerkzaamheden.
Automated tools and techniques A31. Analytical procedures can be performed using a number of tools or techniques, which may be automated. Applying automated analytical procedures to the data may be referred to as data analytics.	Geautomatiseerde hulpmiddelen en technieken A31 Cijferanalyses kunnen worden uitgevoerd met behulp van een aantal hulpmiddelen of tech- nieken, die geautomatiseerd kunnen zijn. Het toepassen van geautomatiseerde cijferanalyses op de gegevens kan worden aangeduid als data analyse.
Observation and Inspection (Ref: Para. 14(c)) Why Observation and Inspection Are Performed as Risk Assessment Procedures A32. Observation and inspection may support, corroborate or contradict inquiries of management and others, and may also provide information about the entity and its environment.	Waarneming en inspectie (Zie Par. 14(c)) Waarom waarneming en inspectie worden uitgevoerd als risico-inschattingswerkzaamheden A32 Waarneming en inspectie kunnen verzoeken om inlichtingen bij het management en anderen ondersteunen, bevestigen of tegenspreken en kunnen ook informatie verschaffen over de enti- teit en haar omgeving.
Scalability A33. Where policies or procedures are not documented, or the entity has less formalized controls, the auditor may still be able to obtain some audit evidence to support the identification and assessment of the risks of material misstatement through observation or inspection of the performance of the control.	Schaalbaarheid A33 Wanneer beleidslijnen of procedures niet zijn gedocumenteerd of de entiteit minder geformali- seerde interne beheersingsmaatregelen heeft, kan de accountant nog steeds enige controle- informatie verkrijgen om de identificatie en inschatting van de risico's op een afwijking van ma- terieel belang te ondersteunen door waarneming of inspectie van de uitvoering van de interne beheersingsmaatregel.
Observation and Inspection as Risk Assessment Procedures A34. Risk assessment procedures may include observation or inspection of the following: • The entity's operations. • Internal documents (such as business plans and strategies), records, and internal control manuals. • Reports prepared by management (such as quarterly management reports and interim financial statements) and those charged with governance (such as minutes of board of directors' meetings). • The entity's premises and plant facilities. • Information obtained from external sources such as trade and economic journals; reports by analysts, banks, or rating agencies; regulatory or financial publications; or other external documents about the entity's financial performance (such as those referred to in paragraph A79). • The behaviors and actions of management or those charged with governance (such as the observation of an audit committee meeting).	Waarneming en inspectie als risico-inschattingswerkzaamheden A34 Risico-inschattingswerkzaamheden kunnen waarneming of inspectie van het volgende omvat- ten: • de activiteiten van de entiteit; • interne documenten (zoals ondernemingsplannen en strategieën), vastleggingen en hand- boeken over de interne beheersing; • verslagen opgesteld door het management (zoals kwartaalverslagen van het management en tussentijdse financiële overzichten) en de met governance belaste personen (zoals no- tulen van de vergaderingen van de raad van bestuur); • de panden en fabrieksinstallaties van de entiteit; • informatie verkregen uit externe bronnen zoals handels- en economische tijdschriften; rap- porten door analisten, banken of kredietbeoordelaars; publicaties van regelgevende of toe- zichthoudende instanties of financiële publicaties; of andere externe documenten over de financiële prestaties van de entiteit (zoals die waarnaar in paragraaf A79 wordt verwezen); • de gedragingen en de handelingen van het management of de met governance belaste personen (zoals de waarneming van een vergadering van het auditcomité).
Automated tools and techniques A35. Automated tools or techniques may also be used to observe or inspect, in particular assets, for example through the use of remote observation tools (e.g., a drone).	Geautomatiseerde hulpmiddelen en technieken A35 Geautomatiseerde hulpmiddelen of technieken kunnen ook worden gebruikt om waar te nemen of te inspecteren, in het bijzonder activa, bijvoorbeeld door het gebruik van externe waarne- mingshulpmiddelen (bijv. een drone).

Considerations Specific to Public Sector Entities
A36. Risk assessment procedures performed by auditors of public sector entities may also include observation and inspection of documents prepared by management for the legislature, for example documents related to mandatory performance reporting.

Information from Other Sources (Ref: Para. 15)
Why the Auditor Considers Information from Other Sources
A37. Information obtained from other sources may be relevant to the identification and assessment of the risks of material misstatement by providing information and insights about:
- The nature of the entity and its business risks, and what may have changed from previous periods.
- The integrity and ethical values of management and those charged with governance, which may also be relevant to the auditor's understanding of the control environment.
- The applicable financial reporting framework and its application to the nature and circumstances of the entity.

Other Relevant Sources
A38. Other relevant sources of information include:
- The auditor's procedures regarding acceptance or continuance of the client relationship or the audit engagement in accordance with ISA 220, including the conclusions reached thereon.25
- Other engagements performed for the entity by the engagement partner. The engagement partner may have obtained knowledge relevant to the audit, including about the entity and its environment, when performing other engagements for the entity. Such engagements may include agreed-upon procedures engagements or other audit or assurance engagements, including engagements to address incremental reporting requirements in the jurisdiction.

25 ISA 220, Quality Control for an Audit of Financial Statements, paragraph 12

Information from the Auditor's Previous Experience with the Entity and Previous Audits (Ref: Para. 16) Why information from previous audits is important to the current audit
A39. The auditor's previous experience with the entity and from audit procedures performed in previous audits may provide the auditor with information that is relevant to the auditor's determination of the nature and extent of risk assessment procedures, and the identification and assessment of risks of material misstatement.

Nature of the Information from Previous Audits
A40. The auditor's previous experience with the entity and audit procedures performed in previous audits may provide the auditor with information about such matters as:
- Past misstatements and whether they were corrected on a timely basis.
- The nature of the entity and its environment, and the entity's system of internal control (including control deficiencies).
- Significant changes that the entity or its operations may have undergone since the prior financial period.

Overwegingen specifiek voor entiteiten in de publieke sector

A36 Risico-inschattingswerkzaamheden die worden uitgevoerd door accountants van entiteiten in de publieke sector kunnen ook waarneming en inspectie van documenten opgesteld door het management voor de wetgever omvatten, bijvoorbeeld documenten met betrekking tot ver- plichte prestatierapportage.

Informatie uit andere bronnen (Zie Par. 15)
Waarom de accountant informatie uit andere bronnen overweegt

A37 Informatie verkregen uit andere bronnen kan relevant zijn voor de identificatie en inschatting van de risico's op een afwijking van materieel belang door het verstrekken van informatie en inzichten over:
- de aard van de entiteit en de bedrijfsrisico's en wat gewijzigd kan zijn ten opzichte van de vorige verslagperiodes;
- de integriteit en ethische waarden van het management en de met governance belaste per- sonen, die ook relevant kunnen zijn voor het inzicht van de accountant in de interne be- heersingsomgeving;
- het van toepassing zijnde stelsel inzake financiële verslaggeving en de toepassing ervan op de aard en omstandigheden van de entiteit.

Andere relevante bronnen

A38 Andere relevante informatiebronnen omvatten:
- de werkzaamheden van de accountant met betrekking tot aanvaarding of continuering van de cliëntrelatie of de controleopdracht in overeenstemming met Standaard 220, inclusief de conclusies die hierover zijn getrokken;25
- andere opdrachten voor de entiteit die door de opdrachtpartner zijn uitgevoerd. De op- drachtpartner kan kennis hebben verkregen die relevant is voor de controle, inclusief ken- nis over de entiteit en haar omgeving bij het uitvoeren van andere opdrachten voor de enti- teit. Dergelijke opdrachten kunnen opdrachten tot het uitvoeren van overeengekomen spe- cifieke werkzaamheden of andere controle- of assurance-opdrachten omvatten, inclusief opdrachten om te voldoen aan incrementele verslaggevingsvereisten in het rechtsgebied.

Informatie uit eerdere ervaringen van de accountant met de entiteit en eerdere controles (Zie Par. 16)
Waarom informatie uit eerdere controles belangrijk is voor de lopende controle
A39 De eerdere ervaring van de accountant met de entiteit en uit controlewerkzaamheden die zijn uitgevoerd in eerdere controles kunnen de accountant informatie verschaffen die relevant is voor de bepaling door de accountant van de aard en omvang van risico-inschattingswerkzaam- heden en de identificatie en inschatting van risico's op afwijkingen van materieel belang.

Aard van de informatie uit eerdere controles

A40 De eerdere ervaring van de accountant met de entiteit en controlewerkzaamheden die zijn uit- gevoerd bij eerdere controles kan de accountant informatie verstrekken over aangelegenheden als:
- afwijkingen uit het verleden en of deze tijdig zijn gecorrigeerd;
- de aard van de entiteit en haar omgeving en het systeem van interne beheersing van de entiteit (inclusief tekortkomingen in de interne beheersing);
- significante wijzigingen die de entiteit of de activiteiten sinds de vorige financiële verslagpe- riode hebben ondergaan;

• Those particular types of transactions and other events or account balances (and related disclosures) where the auditor experienced difficulty in performing the necessary audit procedures, for example, due to their complexity. A1. The auditor is required to determine whether information obtained from the auditor's previous experience with the entity and from audit procedures performed in previous audits remains relevant and reliable, if the auditor intends to use that information for the purposes of the current audit. If the nature or circumstances of the entity have changed, or new information has been obtained, the information from prior periods may no longer be relevant or reliable for the current audit. To determine whether changes have occurred that may affect the relevance or reliability of such information, the auditor may make inquiries and perform other appropriate audit procedures, such as walk-throughs of relevant systems. If the information is not reliable, the auditor may consider performing additional procedures that are appropriate in the circumstances. Engagement Team Discussion (Ref: Para. 17–18) Why the Engagement Team Is Required to Discuss the Application of the Applicable Financial Reporting Framework and the Susceptibility of the Entity's Financial Statements to Material Misstatement A42. The discussion among the engagement team about the application of the applicable financial reporting framework and the susceptibility of the entity's financial statements to material misstatement: • Provides an opportunity for more experienced engagement team members, including the engagement partner, to share their insights based on their knowledge of the entity. Sharing information contributes to an enhanced understanding by all engagement team members. • Allows the engagement team members to exchange information about the business risks to which the entity is subject, how inherent risk factors may affect the susceptibility to misstatement of classes of transactions, account balances and disclosures, and about how and where the financial statements might be susceptible to material misstatement due to fraud or error. • Assists the engagement team members to gain a better understanding of the potential for material misstatement of the financial statements in the specific areas assigned to them, and to understand how the results of the audit procedures that they perform may affect other aspects of the audit, including the decisions about the nature, timing and extent of further audit procedures. In particular, the discussion assists engagement team members in further considering contradictory information based on each member's own understanding of the nature and circumstances of the entity. • Provides a basis upon which engagement team members communicate and share new information obtained throughout the audit that may affect the assessment of risks of material misstatement or the audit procedures performed to address these risks. ISA 240 requires the engagement team discussion to place particular emphasis on how and where the entity's financial statements may be susceptible to material misstatement due to fraud, including how fraud may occur.26 A43. Professional skepticism is necessary for the critical assessment of audit evidence, and a robust and open engagement team discussion, including for recurring audits, may lead to improved identification and assessment of the risks of material misstatement. Another outcome from the discussion may be that the auditor identifies	• die bijzondere soorten transacties en andere gebeurtenissen of rekeningsaldi (en daarmee samenhangende toelichtingen) waar de accountant moeilijkheden ondervond bij met het uitvoeren van de noodzakelijke controlewerkzaamheden, bijvoorbeeld vanwege hun com- plexiteit. A41 Van de accountant wordt vereist om te bepalen of informatie verkregen uit de vorige ervaring van de accountant met de entiteit en van controlewerkzaamheden die bij eerdere controles zijn uitgevoerd, relevant en betrouwbaar blijft, als de accountant voornemens is die informatie te gebruiken voor de doeleinden van de lopende controle. Als de aard of omstandigheden van de entiteit zijn gewijzigd of nieuwe informatie is verkregen, is de informatie uit voorgaande verslag- perioden mogelijk niet langer relevant of betrouwbaar voor de lopende controle. Om te bepalen of er wijzigingen zijn voorgekomen die de relevantie of betrouwbaarheid van dergelijke informa- tie kunnen beïnvloeden, kan de accountant verzoeken om inlichtingen en andere geschikte controlewerkzaamheden uitvoeren, zoals lijncontroles van relevante systemen. Als de informa- tie niet betrouwbaar is, kan de accountant overwegen extra werkzaamheden uit te voeren die passend zijn in de omstandigheden. Bespreking opdrachtteam (Zie Par. 17 – 18) Waarom het opdrachtteam de toepassing van het van toepassing zijnde stelsel inzake financiële ver- slaggeving en de vatbaarheid van de financiële overzichten van de entiteit voor afwijkingen van mate- rieel belang moet bespreken A42 De bespreking binnen het opdrachtteam over de toepassing van het van toepassing zijnde stel- sel inzake financiële verslaggeving en de vatbaarheid van de financiële overzichten van de en- titeit voor afwijkingen van materieel belang: • Biedt een kans voor meer ervaren leden van het opdrachtteam, waaronder de opdracht- partner, om de op hun kennis van de entiteit gebaseerde inzichten te delen. Het delen van informatie draagt bij aan een verbeterd inzicht door alle leden van het opdrachtteam; • Staat de opdrachtteamleden toe om informatie uit te wisselen over de bedrijfsrisico's waar- aan de entiteit is blootgesteld, hoe inherente risicofactoren de vatbaarheid voor afwijkingen van transactiestromen, rekeningsaldi en toelichtingen kunnen beïnvloeden en over hoe en waar de financiële overzichten vatbaar kunnen zijn voor een afwijking van materieel belang als gevolg van fraude of fouten; • Helpt de betrokken teamleden om een beter inzicht te krijgen in de mogelijkheid voor een afwijking van materieel belang in de financiële overzichten in de specifieke gebieden die aan hen zijn toegewezen en om inzicht te verwerven in hoe de resultaten van de door hen uitgevoerde controlewerkzaamheden van invloed kunnen zijn op andere aspecten van de controle, inclusief de beslissingen over de aard, timing en omvang van verdere controle- werkzaamheden. De bespreking helpt het opdrachtteam in het bijzonder tegenstrijdige in- formatie verder te overwegen op basis van het eigen inzicht van elk lid in de aard en om- standigheden van de entiteit; • Biedt een basis waarop leden van het opdrachtteam nieuwe informatie verkregen tijdens de controle en die van invloed kan zijn op de inschatting van risico's op een afwijking van materieel belang of op de uitgevoerde controlewerkzaamheden om in te spelen op deze risico's communiceren en delen. Standaard 240 vereist dat de opdrachtteam bespreking bijzondere nadruk legt op hoe en waar de financiële overzichten van de entiteit mogelijk vatbaar zijn voor afwijkingen van materieel belang als gevolg van fraude, waaronder hoe fraude kan voorkomen.26 A43 Een professioneel-kritische instelling is noodzakelijk voor de kritische inschatting van controle- informatie en een robuuste en open opdrachtteam bespreking, ook voor doorlopende contro- les, kan leiden tot verbeterde identificatie en inschatting van de risico's op een afwijking van materieel belang.

specific areas of the audit for which exercising professional skepticism may be particularly important, and may lead to the involvement of more experienced members of the engagement team who are appropriately skilled to be involved in the performance of audit procedures related to those areas.

Scalability

A44. When the engagement is carried out by a single individual, such as a sole practitioner (i.e., where an engagement team discussion would not be possible), consideration of the matters referred to in paragraphs A42 and A46 nonetheless may assist the auditor in identifying where there may be risks of material misstatement.

A45. When an engagement is carried out by a large engagement team, such as for an audit of group financial statements, it is not always necessary or practical for the discussion to include all members in a single discussion (for example, in a multi-location audit), nor is it necessary for all the members of the engagement team to be informed of all the decisions reached in the discussion. The engagement partner may discuss matters with key members of the engagement team including, if considered appropriate, those with specific skills or knowledge, and those responsible for the audits of components, while delegating discussion with others, taking into account the extent of communication considered necessary throughout the engagement team. A communications plan, agreed by the engagement partner, may be useful.

26 ISA 240, paragraph 16

Discussion of Disclosures in the Applicable Financial Reporting Framework

A46. As part of the discussion among the engagement team, consideration of the disclosure requirements of the applicable financial reporting framework assists in identifying early in the audit where there may be risks of material misstatement in relation to disclosures, even in circumstances where the applicable financial reporting framework only requires simplified disclosures. Matters the engagement team may discuss include:

- Changes in financial reporting requirements that may result in significant new or revised disclosures;
- Changes in the entity's environment, financial condition or activities that may result in significant new or revised disclosures, for example, a significant business combination in the period under audit;
- Disclosures for which obtaining sufficient appropriate audit evidence may have been difficult in the past; and
- Disclosures about complex matters, including those involving significant management judgment as to what information to disclose.

Considerations Specific to Public Sector Entities

A47. As part of the discussion among the engagement team by auditors of public sector entities, consideration may also be given to any additional broader objectives, and related risks, arising from the audit mandate or obligations for public sector entities.

Een ander resultaat van de bespreking kan zijn dat de accountant specifieke gebieden van de controle identificeert waarvoor het uitoefenen van een professioneel-kritische instelling bijzonder belangrijk is en wat kan leiden tot de betrokkenheid van meer ervaren leden van het opdrachtteam die voldoende bekwaam zijn om betrokken te zijn bij de uitvoering van controlewerkzaamheden met betrekking tot deze gebieden.

Schaalbaarheid

26 Standaard 240, paragraaf 16.

A44 Wanneer de opdracht wordt uitgevoerd door een enkele persoon, zoals een zelfstandige accountant (d.w.z. waar een opdrachtteam bespreking niet mogelijk is), kan overweging van de in de paragrafen A42 en A46 genoemde aangelegenheden de accountant niettemin helpen om te identificeren waar er risico's kunnen zijn op afwijkingen van materieel belang.

A45 Wanneer een opdracht wordt uitgevoerd door een groot opdrachtteam, zoals voor een controle van financiële overzichten van de groep, is het niet altijd noodzakelijk of praktisch uitvoerbaar dat de bespreking alle leden in een enkele bespreking omvat (bijvoorbeeld in een controle die meerdere locaties betreft), noch is het nodig dat alle leden van het opdrachtteam op de hoogte worden gehouden van alle beslissingen die in de bespreking zijn genomen. De opdrachtpartner kan aangelegenheden bespreken met kernleden van het opdrachtteam, met inbegrip van, in- dien nodig geacht, degenen met specifieke vaardigheden of kennis en degenen die verant- woordelijk zijn voor de controles van groepsonderdelen, terwijl bespreking met anderen wordt gedelegeerd, rekening houdend met de omvang van communicatie die door het hele opdracht- team noodzakelijk wordt geacht. Een door de opdrachtpartner goedgekeurd communicatieplan kan nuttig zijn.

Bespreking van toelichtingen in het van toepassing zijnde stelsel inzake financiële verslaggeving A46

Als onderdeel van de bespreking binnen het opdrachtteam, helpt rekening houden met de toelichtingsvereisten van het van toepassing zijnde stelsel inzake financiële verslaggeving in het begin van de controle bij het identificeren van mogelijke risico's op een afwijking van materieel belang met betrekking tot toelichtingen, zelfs in omstandigheden waarin het van toepassing zijnde stelsel inzake financiële verslaggeving alleen vereenvoudigde toelichtingen vereist. Aan- gelegenheden die het opdrachtteam kan bespreken omvatten:

- veranderingen in financiële verslaggevingsvereisten die kunnen leiden tot significante nieuwe of herziene toelichtingen;
- veranderingen in haar omgeving, financiële toestand of activiteiten van de entiteit die kunnen leiden tot significante nieuwe of herziene toelichtingen, bijvoorbeeld een significante fusie of overname in de gecontroleerde verslagperiode;
- toelichtingen waarvoor het verkrijgen van voldoende en geschikte controle-informatie moeilijk kan zijn geweest in het verleden; en
- toelichtingen over complexe aangelegenheden, waaronder die waarbij significante oordeelsvorming van het management betrokken is over welke informatie moet worden toege- licht.

Overwegingen specifiek voor entiteiten in de publieke sector

A47 Als onderdeel van de bespreking binnen het opdrachtteam door accountants van entiteiten in de publieke sector, kan er ook rekening worden gehouden met eventuele aanvullende bredere doelstellingen en bijbehorende risico's die voortkomen uit het controlemandaat of verplichtin- gen voor entiteiten in de publieke sector.

Obtaining an Understanding of the Entity and Its Environment, the Applicable Financial Reporting Framework and the Entity's System of Internal Control (Ref: Para. 19–27) Obtaining the Required Understanding (Ref: Para. 19–27) A48. Obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control is a dynamic and iterative process of gathering, updating and analyzing information and continues throughout the audit. Therefore, the auditor's expectations may change as new information is obtained. A49. The auditor's understanding of the entity and its environment and the applicable financial reporting framework may also assist the auditor in developing initial expectations about the classes of transactions, account balances and disclosures that may be significant classes of transactions, account balances and disclosures. These expected significant classes of transactions, account balances and disclosures form the basis for the scope of the auditor's understanding of the entity's information system. Why an Understanding of the Entity and Its Environment, and the Applicable Financial Reporting Framework Is Required (Ref: Para. 19–20) A50. The auditor's understanding of the entity and its environment, and the applicable financial reporting framework, assists the auditor in understanding the events and conditions that are relevant to the entity, and in identifying how inherent risk factors affect the susceptibility of assertions to misstatement in the preparation of the financial statements, in accordance with the applicable financial reporting framework, and the degree to which they do so. Such information establishes a frame of reference within which the auditor identifies and assesses risks of material misstatement. This frame of reference also assists the auditor in planning the audit and exercising professional judgment and professional skepticism throughout the audit, for example, when: • Identifying and assessing risks of material misstatement of the financial statements in accordance with ISA 315 (Revised 2019) or other relevant standards (e.g., relating to risks of fraud in accordance with ISA 240 or when identifying or assessing risks related to accounting estimates in accordance with ISA 540 (Revised)); • Performing procedures to help identify instances of non-compliance with laws and regulations that may have a material effect on the financial statements in accordance with ISA 250;27 • Evaluating whether the financial statements provide adequate disclosures in accordance with ISA 700 (Revised);28 • Determining materiality or performance materiality in accordance with ISA 320;29 or • Considering the appropriateness of the selection and application of accounting policies, and the adequacy of financial statement disclosures. A51. The auditor's understanding of the entity and its environment, and the applicable financial reporting framework, also informs how the auditor plans and performs further audit procedures, for example, when: • Developing expectations for use when performing analytical procedures in accordance with ISA 520;30 • Designing and performing further audit procedures to obtain sufficient appropriate audit evidence in accordance with ISA 330; and • Evaluating the sufficiency and appropriateness of audit evidence obtained (e.g., relating to assumptions or management's oral and written representations). 27 ISA 250 (Revised), Consideration of Laws and Regulations in an Audit of Financial Statements, paragraph 14 28 ISA 700 (Revised), Forming an Opinion and Reporting on Financial Statements, paragraph 13(e)	Het verwerven van inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het systeem van interne beheersing van de entiteit (Zie Par. 19 – 27) Het verwerven van het vereiste inzicht (Zie Par. 19 – 27) A48 Het verwerven van inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel in- zake financiële verslaggeving en het interne beheersingssysteem van de entiteit is een dyna- misch en iteratief proces van verzamelen, bijwerken en analyseren van informatie en dit gaat door tijdens de controle. Daarom kunnen de verwachtingen van de accountant veranderen als nieuwe informatie wordt verkregen. A49 Het inzicht van de accountant in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving kan de accountant ook helpen bij het ontwikkelen van initiële verwachtingen over de transactiestromen, rekeningsaldi en toelichtingen die significante transactiestroom, rekeningsaldi en toelichtingen kunnen zijn. Deze verwachte significante transactiestromen, rekeningsaldi en toelichtingen vormen de basis voor de reikwijdte van het inzicht van de accountant in het informatiesysteem van de entiteit. Waarom inzicht in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving wordt vereist (Zie Par. 19 – 20) A50 Het inzicht van de accountant in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving, helpt de accountant bij het verwerven van inzicht in de gebeurtenissen en omstandigheden die relevant zijn voor de entiteit en bij het identificeren hoe inherente risicofactoren de vatbaarheid van beweringen voor afwijkingen bij het opstellen van de financiële overzichten beïnvloeden, in overeenstemming met het van toepassing zijnde stel- sel inzake financiële verslaggeving en de mate waarin zij dit doen. Dergelijke informatie vormt een referentiekader waarbinnen de accountant risico's op een afwijking van materieel belang identificeert en inschat. Dit referentiekader helpt de accountant ook bij het plannen van de con- trole en het uitoefenen van professionele oordeelsvorming en een professioneel-kritische in- stelling gedurende de gehele controle, bijvoorbeeld bij: • het identificeren en inschatten van risico's op een afwijking van materieel belang in de fi- nanciële overzichten in overeenstemming met Standaard 315 of andere relevante Stan- daarden (bijv. met betrekking tot risico's op fraude in overeenstemming met Standaard 240 of bij het identificeren of inschatten van risico's met betrekking tot schattingen in overeen- stemming met Standaard 540); • het uitvoeren van werkzaamheden om bij te dragen tot het identificeren van gevallen van niet- naleving van wet- en regelgeving die een invloed van materieel belang kunnen hebben op de financiële overzichten in overeenstemming met Standaard 250;27 • het evalueren of de financiële overzichten voldoende toelichtingen verschaffen in overeen- stemming met Standaard 700;28 • het bepalen van materialiteit of uitvoeringsmaterialiteit in overeenstemming met Standaard 320;29 of • het overwegen van de geschiktheid van de keuze en toepassing van grondslagen voor fi- nanciële verslaggeving en de toereikendheid van de toelichtingen bij de financiële over- zichten. A51 Het inzicht van de accountant in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving, is ook de basis voor de manier waarop de accountant verdere controlewerkzaamheden plant en uitvoert, bijvoorbeeld bij: • het ontwikkelen van verwachtingen voor gebruik bij het uitvoeren van cijferanalyses in overeenstemming met Standaard 520;30

29 ISA 320, Materiality in Planning and Performing an Audit, paragraphs 10–11
30 ISA 520, paragraph 5

Scalability
A52. The nature and extent of the required understanding is a matter of the auditor's professional judgment and varies from entity to entity based on the nature and circumstances of the entity, including:
- The size and complexity of the entity, including its IT environment;
- The auditor's previous experience with the entity;
- The nature of the entity's systems and processes, including whether they are formalized or not; and
- The nature and form of the entity's documentation.

A53. The auditor's risk assessment procedures to obtain the required understanding may be less extensive in audits of less complex entities and more extensive for entities that are more complex. The depth of the understanding that is required by the auditor is expected to be less than that possessed by management in managing the entity.
A54. Some financial reporting frameworks allow smaller entities to provide simpler and less detailed disclosures in the financial statements. However, this does not relieve the auditor of the responsibility to obtain an understanding of the entity and its environment and the applicable financial reporting framework as it applies to the entity.
A55. The entity's use of IT and the nature and extent of changes in the IT environment may also affect the specialized skills that are needed to assist with obtaining the required understanding.

The Entity and Its Environment (Ref: Para. 19(a))
The Entity's Organizational Structure, Ownership and Governance, and Business Model (Ref: Para. 19(a)(i))
The entity's organizational structure and ownership
A56. An understanding of the entity's organizational structure and ownership may enable the auditor to understand such matters as:
- The complexity of the entity's structure.
- The ownership, and relationships between owners and other people or entities, including related parties. This understanding may assist in determining whether related party

transactions have been appropriately identified, accounted for, and adequately disclosed in the financial statements.31
- The distinction between the owners, those charged with governance and management.
- The structure and complexity of the entity's IT environment.

- het opzetten en uitvoeren van verdere controlewerkzaamheden om voldoende en ge- schikte controle te verkrijgen in overeenstemming met Standaard 330; en
- het evalueren van de toereikendheid en geschiktheid van verkregen controle-informatie (bijv. met betrekking tot veronderstellingen of mondelinge en schriftelijke bevestigingen van het management).

Schaalbaarheid

A52 De aard en omvang van het vereiste inzicht is een aangelegenheid van professionele oordeels- vorming door de accountant en varieert van entiteit tot entiteit gebaseerd op de aard en om- standigheden van de entiteit, waaronder:
- de omvang en complexiteit van de entiteit, inclusief de IT-omgeving;
- de eerdere ervaring van de accountant met de entiteit;
- de aard van de systemen en processen van de entiteit, inclusief of deze al dan niet gefor- maliseerd zijn; en
- de aard en vorm van de documentatie van de entiteit.

A53 De risico-inschattingswerkzaamheden van de accountant om het vereiste inzicht te verwerven, kunnen minder uitgebreid zijn in controles van minder complexe entiteiten en uitgebreider voor complexere entiteiten. De diepte van het inzicht dat door de accountant wordt vereist, zal naar verwachting minder zijn dan het inzicht dat het management bezit bij het leiden van de entiteit.

A54 Sommige stelsels inzake financiële verslaggeving staan kleinere entiteiten toe om eenvoudi- gere en minder gedetailleerde toelichtingen te verschaffen in de financiële overzichten. Dit ont- slaat de accountant echter niet van zijn verantwoordelijkheid om inzicht te verwerven in de enti- teit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving zo- als het van toepassing is op de entiteit.

A55 Het gebruik van IT door de entiteit en de aard en omvang van veranderingen in de IT-omgeving kunnen ook van invloed zijn op de specialistische vaardigheden die nodig zijn om het vereiste inzicht te verwerven.

De entiteit en haar omgeving (Zie Par. 19(a))
De organisatiestructuur, het eigendom en de governance van de entiteit en haar bedrijfsmodel (Zie Par. 19(a)(i))

De organisatiestructuur en eigendom van de entiteit

A56 Inzicht in de organisatiestructuur en eigendom van de entiteit kan de accountant in staat stellen inzicht te verwerven in aangelegenheden als:
- de complexiteit van de structuur van de entiteit;

- het eigendom en relaties tussen eigenaren en andere mensen of entiteiten, inclusief ver- bonden partijen. Dit inzicht kan helpen om te bepalen of transacties met verbonden partijen op passende wijze zijn geïdentificeerd, verantwoord en voldoende toegelicht in de financi- ele overzichten;31
- het onderscheid tussen de eigenaars, de met governance belaste personen en manage- ment;

- de structuur en complexiteit van de IT-omgeving van de entiteit;

Automated tools and techniques A57. The auditor may use automated tools and techniques to understand flows of transactions and processing as part of the auditor's procedures to understand the information system. An outcome of these procedures may be that the auditor obtains information about the entity's organizational structure or those with whom the entity conducts business (e.g., vendors, customers, related parties). Considerations specific to public sector entities A58. Ownership of a public sector entity may not have the same relevance as in the private sector because decisions related to the entity may be made outside of the entity as a result of political processes. Therefore, management may not have control over certain decisions that are made. Matters that may be relevant include understanding the ability of the entity to make unilateral decisions, and the ability of other public sector entities to control or influence the entity's mandate and strategic direction. 31 ISA 550 establishes requirements and provide guidance on the auditor's considerations relevant to related parties. 32 ISA 260 (Revised), paragraphs A1 and A2, provide guidance on the identification of those charged with governance and explains that in some cases, some or all of those charged with governance may be involved in managing the entity.	Geautomatiseerde hulpmiddelen en technieken A57 De accountant kan geautomatiseerde hulpmiddelen en technieken gebruiken om inzicht te ver- werven in transactiestromen en verwerking als onderdeel van de werkzaamheden van de ac- countant om inzicht te verwerven in het informatiesysteem. Een uitkomst van deze werkzaam- heden kan zijn dat de accountant informatie verkrijgt over de organisatiestructuur van de enti- teit of degenen waarmee de entiteit zaken doet (bijvoorbeeld leveranciers, klanten, verbonden partijen). Overwegingen specifiek voor entiteiten in de publieke sector A58 Het eigendom van een entiteit in de publieke sector heeft mogelijk niet dezelfde relevantie als in de particuliere sector omdat als gevolg van politieke processen beslissingen met betrekking tot de entiteit buiten de entiteit kunnen worden genomen. Daarom heeft het management mo- gelijk geen zeggenschap over bepaalde beslissingen die worden genomen. Aangelegenheden die relevant kunnen zijn omvatten onder meer inzicht in de mogelijkheid van de entiteit om een- zijdige beslissingen te nemen en de mogelijkheid van andere entiteiten in de publieke sector om het mandaat en de strategische richting van de entiteit te beheersen of te beïnvloeden.
Governance Why the auditor obtains an understanding of governance A59. Understanding the entity's governance may assist the auditor with understanding the entity's ability to provide appropriate oversight of its system of internal control. However, this understanding may also provide evidence of deficiencies, which may indicate an increase in the susceptibility of the entity's financial statements to risks of material misstatement. Understanding the entity's governance A60. Matters that may be relevant for the auditor to consider in obtaining an understanding of the governance of the entity include: • Whether any or all of those charged with governance are involved in managing the entity. • The existence (and separation) of a non-executive Board, if any, from executive management. • Whether those charged with governance hold positions that are an integral part of the entity's legal structure, for example as directors. • The existence of sub-groups of those charged with governance, such as an audit committee, and the responsibilities of such a group. • The responsibilities of those charged with governance for oversight of financial reporting, including approval of the financial statements.	Governance Waarom de accountant inzicht in de governance verkrijgt A59 Inzicht in de governance van de entiteit kan de accountant helpen bij het verwerven van inzicht in de mogelijkheid van de entiteit om passend toezicht te houden op het interne beheersings- systeem. Dit inzicht kan echter ook informatie verschaffen inzake tekortkomingen, wat kan wij- zen op een toename van de vatbaarheid van de financiële overzichten van de entiteit voor risi- co's op afwijkingen van materieel belang. Inzicht in de governance van de entiteit A60 Aangelegenheden die relevant kunnen zijn voor de accountant om te overwegen bij het ver- werven van inzicht in de governance van de entiteit omvatten: • of een of meer van de met governance belaste personen betrokken zijn bij het leiden van de entiteit; • het bestaan (en de scheiding) van een niet-dagelijks bestuur, indien aanwezig, van een da- gelijks bestuur; • of de met governance belaste personen posities bekleden die een integraal onderdeel zijn van de juridische structuur van de entiteit, bijvoorbeeld als directeur; • het bestaan van subgroepen van de met governance belaste personen, zoals een auditco- mité, en de verantwoordelijkheden van een dergelijke groep; • de verantwoordelijkheden van de met governance belaste personen voor het toezicht op de financiële verslaggeving, inclusief goedkeuring van de financiële overzichten.
The Entity's Business Model Why the auditor obtains an understanding of the entity's business model A61. Understanding the entity's objectives, strategy and business model helps the auditor to understand the entity at a strategic level, and to understand the business risks the entity takes and faces. An understanding of the	Het bedrijfsmodel van de entiteit Waarom de accountant inzicht krijgt in het bedrijfsmodel van de entiteit A61 Inzicht in de doelstellingen, strategie en bedrijfsmodel van de entiteit helpt de accountant om inzicht te verwerven in de entiteit op strategisch niveau en om de bedrijfsrisico's te begrijpen die de

business risks that have an effect on the financial statements assists the auditor in identifying risks of material misstatement, since most business risks will eventually have financial consequences and, therefore, an effect on the financial statements.	entiteit neemt en loopt. Een inzicht in de bedrijfsrisico's die van invloed zijn op de finan- ciële overzichten helpt de accountant bij het identificeren van risico's op een afwijking van ma- terieel belang, aangezien de meeste bedrijfsrisico's uiteindelijk financiële consequenties heb- ben en derhalve een effect op de financiële overzichten.
Understanding the entity's business model A62. Not all aspects of the business model are relevant to the auditor's understanding. Business risks are broader than the risks of material misstatement of the financial statements, although business risks include the latter. The auditor does not have a responsibility to understand or identify all business risks because not all business risks give rise to risks of material misstatement. A63. Business risks increasing the susceptibility to risks of material misstatement may arise from: • Inappropriate objectives or strategies, ineffective execution of strategies, or change or complexity. • A failure to recognize the need for change may also give rise to business risk, for example, from: o The development of new products or services that may fail; o A market which, even if successfully developed, is inadequate to support a product or service; or o Flaws in a product or service that may result in legal liability and reputational risk. • Incentives and pressures on management, which may result in intentional or unintentional management bias, and therefore affect the reasonableness of significant assumptions and the expectations of management or those charged with governance. A64. Examples of matters that the auditor may consider when obtaining an understanding of the entity's business model, objectives, strategies and related business risks that may result in a risk of material misstatement of the financial statements include: • Industry developments, such as the lack of personnel or expertise to deal with the changes in the industry; • New products and services that may lead to increased product liability; • Expansion of the entity's business, and demand has not been accurately estimated; • New accounting requirements where there has been incomplete or improper implementation; • Regulatory requirements resulting in increased legal exposure; • Current and prospective financing requirements, such as loss of financing due to the entity's inability to meet requirements; • Use of IT, such as the implementation of a new IT system that will affect both operations and financial reporting; or • The effects of implementing a strategy, particularly any effects that will lead to new accounting requirements. A65. Ordinarily, management identifies business risks and develops approaches to address them. Such a risk assessment process is part of the entity's system of internal control and is discussed in paragraph 22, and paragraphs A109–A113.	Inzicht in het bedrijfsmodel van de entiteit A62 Niet alle aspecten van het bedrijfsmodel zijn relevant voor het inzicht van de accountant. Be- drijfsrisico's zijn breder dan de risico's op een afwijking van materieel belang in de financiële overzichten, hoewel bedrijfsrisico's de laatste omvatten. De accountant heeft geen verantwoor- delijkheid om inzicht te verwerven in alle bedrijfsrisico's of ze te identificeren omdat niet alle bedrijfsrisico's aanleiding geven tot risico's op een afwijking van materieel belang. A63 Bedrijfsrisico's die de vatbaarheid voor risico's op een afwijking van materieel belang vergro- ten, kunnen voortkomen uit: • ongeschikte doelstellingen of strategieën, ineffectieve uitvoering van strategieën, of wijzi- gingen of complexiteit; • het niet onderkennen van de noodzaak voor wijzigingen, wat ook aanleiding kan geven tot bedrijfsrisico's bijvoorbeeld van: o de ontwikkeling van nieuwe producten of diensten die mogelijk geen succes zijn; o een markt die, zelfs als deze met goed gevolg is ontwikkeld, een product of dienst niet op adequate wijze ondersteunt; of o gebreken in een product of dienst die tot wettelijke aansprakelijkheid en reputatierisico kunnen leiden. • stimulansen en druk op het management, die kunnen resulteren in opzettelijke of onopzet- telijke tendenties bij het management en die daarom de redelijkheid van significante veron- derstellingen en de verwachtingen van het management of de met governance belaste per- sonen beïnvloeden. A64 Voorbeelden van aangelegenheden die de accountant kan overwegen bij het verkrijgen van inzicht in het bedrijfsmodel, doelstellingen, strategieën en gerelateerde bedrijfsrisico's van de entiteit die kunnen leiden tot een risico van materieel belang op afwijkingen van de financiële overzichten omvatten: • ontwikkelingen in de sector, zoals het gebrek aan personeel of expertise om de veranderin- gen in de sector aan te pakken; • nieuwe producten en diensten die kunnen leiden tot hogere productaansprakelijkheid; • uitbreiding van de activiteiten van de entiteit, terwijl de vraag niet nauwkeurig is geschat; • nieuwe voorschriften inzake administratieve verwerking bij onvolledige of onjuiste imple- mentatie; • vereisten op grond van regelgeving resulterend in een hogere juridische blootstelling; • huidige en toekomstige financieringsbehoeften, zoals verlies van financiering doordat de entiteit niet in staat is de verplichtingen na te komen; • gebruik van IT, zoals de implementatie van een nieuw IT-systeem dat gevolgen heeft voor zowel de bedrijfsvoering als financiële verslaggeving; of • de effecten van het implementeren van een strategie, met name effecten die tot nieuwe voorschriften inzake administratieve verwerking zullen leiden. A65 Gewoonlijk identificeert het management bedrijfsrisico's en ontwikkelt het benaderingen om hier op in te spelen. Een dergelijk risico-inschattingsproces maakt deel uit van het interne be- heersingssysteem van de entiteit en wordt in paragraaf 22 en de paragrafen A109 – A113 be- sproken.

Considerations specific to public sector entities

A66. Entities operating in the public sector may create and deliver value in different ways to those creating wealth for owners but will still have a ‘business model’ with a specific objective. Matters public sector auditors may obtain an understanding of that are relevant to the business model of the entity, include:

- Knowledge of relevant government activities, including related programs.
- Program objectives and strategies, including public policy elements.

A67. For the audits of public sector entities, “management objectives” may be influenced by requirements to demonstrate public accountability and may include objectives which have their source in law, regulation or other authority.

Industry, Regulatory and Other External Factors (Ref: Para. 19(a)(ii)) Industry factors

A68. Relevant industry factors include industry conditions such as the competitive environment, supplier and customer relationships, and technological developments. Matters the auditor may consider include:

- The market and competition, including demand, capacity, and price competition.
- Cyclical or seasonal activity.
- Product technology relating to the entity’s products.
- Energy supply and cost.

A69. The industry in which the entity operates may give rise to specific risks of material misstatement arising from the nature of the business or the degree of regulation.

Regulatory factors

A70. Relevant regulatory factors include the regulatory environment. The regulatory environment encompasses, among other matters, the applicable financial reporting framework and the legal and political environment and any changes thereto. Matters the auditor may consider include:

- Regulatory framework for a regulated industry, for example, prudential requirements, including related disclosures.
- Legislation and regulation that significantly affect the entity’s operations, for example, labor laws and regulations.
- Taxation legislation and regulations.
- Government policies currently affecting the conduct of the entity’s business, such as monetary, including foreign exchange controls, fiscal, financial incentives (for example, government aid programs), and tariffs or trade restriction policies.
- Environmental requirements affecting the industry and the entity’s business.

A71. ISA 250 (Revised) includes some specific requirements related to the legal and regulatory framework applicable to the entity and the industry or sector in which the entity operates.34

Considerations specific to public sector entities

Overwegingen specifiek voor entiteiten in de publieke sector

A66 Entiteiten die actief zijn in de publieke sector, kunnen op verschillende manieren waarde creëren en leveren ten opzichte van degenen die rijkdom creëren voor eigenaren, maar zullen nog steeds een 'bedrijfsmodel' hebben met een specifieke doelstelling. Aangelegenheden waarin accountants in de publieke sector inzicht kunnen verwerven die relevant zijn voor het bedrijfs- model van de entiteit, omvatten:

- kennis van relevante overheidsactiviteiten, inclusief gerelateerde programma's;
- programmadoelstellingen en -strategieën, inclusief elementen van overheidsbeleidslijnen.

A67 Voor de controles van entiteiten in de publieke sector kunnen ‘managementdoelstellingen’ wor- den beïnvloed door vereisten om publieke verantwoording aan te tonen en kunnen zij doelstellingen omvatten die hun oorsprong hebben in wet- en regelgeving of andere van kracht zijnde voorschriften.

Sectorgebonden factoren, regelgevingsfactoren en andere externe factoren (Zie Par. 19(a)(ii))
Sectorgebonden factoren

A68 Relevante sectorgebonden factoren zijn omstandigheden in de sector zoals de concurrentieomgeving, de relaties met leverancier en cliënten en technologische ontwikkelingen. Aangelegenheden die de accountant kan overwegen omvatten:

- de markt en concurrentie, inclusief vraag, capaciteit en prijsconcurrentie;
- cyclische of seizoensgebonden activiteit;
- technologie met betrekking tot de producten van de entiteit;
- de energievoorziening en kosten.

A69 De sector waarin de entiteit actief is, kan aanleiding geven tot specifieke risico’s op een afwijking van materieel belang die voortkomt uit de aard van de activiteit of de mate van regulering.

Regelgevingsfactoren

A70 Het regelgevingskader behoort tot de relevante regelgevingsfactoren. Het regelgevingskader omvat onder meer het van toepassing zijnde stelsel inzake financiële verslaggeving en de juri- dische en politieke omgeving en eventuele wijzigingen daarvan. Aangelegenheden die de ac- countant kan overwegen, omvatten:

- het regelgevingskader voor een gereguleerde sector, bijvoorbeeld prudentiële vereisten, inclusief vereisten voor toelichtingen;
- wet- en regelgeving die de activiteiten van de entiteit significant beïnvloedt, bijvoorbeeld op het gebied van arbeid;
- fiscale wet- en regelgeving;
- overheidsbeleidslijnen die op dat moment van invloed zijn op de uitvoering van de activiteiten van de entiteit, zoals het monetaire beleid, het begrotingsbeleid, financiële stimuleringsmaatregelen (bijvoorbeeld programma’s voor overheidssteun) en beleidslijnen inzake dou- anerechten of handelsbelemmeringen;
- milieueisen die van invloed zijn op de activiteiten van de sector en de entiteit.

A71 Standaard 250 bevat enkele specifieke vereisten met betrekking tot het wet- en regelgevingskader dat van toepassing is op de entiteit en de branche of sector waarin de entiteit actief is.35

Overwegingen specifiek voor entiteiten in de publieke sector

A72. For the audits of public sector entities, there may be particular laws or regulations that affect the entity's operations. Such elements may be an essential consideration when obtaining an understanding of the entity and its environment.

Other external factors
A73. Other external factors affecting the entity that the auditor may consider include the general economic conditions, interest rates and availability of financing, and inflation or currency revaluation.

Measures Used by Management to Assess the Entity's Financial Performance (Ref: Para. 19(a)(iii)) Why the auditor understands measures used by management
A74. An understanding of the entity's measures assists the auditor in considering whether such measures, whether used externally or internally, create pressures on the entity to achieve performance targets. These pressures may motivate management to take actions that increase the susceptibility to

33 ISA 220, paragraph 14
34 ISA 250 (Revised), paragraph 13

misstatement due to management bias or fraud (e.g., to improve the business performance or to intentionally misstate the financial statements) (see ISA 240 for requirements and guidance in relation to the risks of fraud).
A75. Measures may also indicate to the auditor the likelihood of risks of material misstatement of related financial statement information. For example, performance measures may indicate that the entity has unusually rapid growth or profitability when compared to that of other entities in the same industry.

Measures used by management
A76. Management and others ordinarily measure and review those matters they regard as important. Inquiries of management may reveal that it relies on certain key indicators, whether publicly available or not, for evaluating financial performance and taking action. In such cases, the auditor may identify relevant performance measures, whether internal or external, by considering the information that the entity uses to manage its business. If such inquiry indicates an absence of performance measurement or review, there may be an increased risk of misstatements not being detected and corrected.
A77. Key indicators used for evaluating financial performance may include:
- Key performance indicators (financial and non-financial) and key ratios, trends and operating statistics.
- Period-on-period financial performance analyses.
- Budgets, forecasts, variance analyses, segment information and divisional, departmental or other level performance reports.
- Employee performance measures and incentive compensation policies.
- Comparisons of an entity's performance with that of competitors.

Scalability (Ref: Para. 19(a)(iii))

A72 Voor de controles van entiteiten in de publieke sector kan er bepaalde wet-of regelgeving zijn die van invloed is op de activiteiten van de entiteit. Dergelijke elementen kunnen een essenti- ele overweging zijn bij het verwerven van inzicht de entiteit en haar omgeving.

Andere externe factoren

A73 Andere externe factoren die van invloed zijn op de entiteit en die de accountant kan overwe- gen, omvatten onder meer de algemene economische omstandigheden, de rentevoeten, de beschikbaarheid van financiering, de inflatie of de revaluatie van een munteenheid.

Door het management gebruikte maatstaven om de financiële prestaties van de entiteit in te schatten (Zie Par. 19(a)(iii))

Waarom de accountant inzicht verwerft in de door het management gebruikte maatstaven

A74 Inzicht in de maatstaven van de entiteit helpt de accountant bij het overwegen of dergelijke maatstaven, extern of intern gebruikt, druk leggen op de entiteit om prestatiedoelen te berei- ken. Deze druk kan het management motiveren om acties te ondernemen die de vatbaarheid voor afwijkingen als gevolg van tendentie bij het management of fraude vergroten (b.v. om de bedrijfsprestaties te verbeteren of de financiële overzichten opzettelijk verkeerd weer te geven) (zie Standaard 240 voor vereisten en leidraden met betrekking tot de risico's op fraude).

A75 Maatstaven kunnen de accountant ook wijzen op de waarschijnlijkheid van risico's op een af- wijking van materieel belang van daarmee verband houdende informatie in de financiële over- zichten. Prestatiemaatstaven kunnen bijvoorbeeld aangeven dat de entiteit een ongewoon snelle groei of winstgevendheid heeft in vergelijking met andere entiteiten in dezelfde sector.

Maatstaven die door het management worden gebruikt

A76 Het management en anderen meten en beoordelen gewoonlijk de aangelegenheden die zij be- langrijk achten. Uit verzoeken om inlichtingen bij het management kan blijken dat het manage- ment zich baseert op bepaalde belangrijke indicatoren, openbaar beschikbaar of niet, voor het evalueren van financiële prestaties en het nemen van actie. In dergelijke gevallen kan de ac- countant relevante prestatiemaatstaven identificeren, intern of extern, door de informatie die de entiteit gebruikt om de activiteiten te beheren, te overwegen. Als een dergelijk verzoek om in- lichtingen duidt op een afwezigheid van prestatiemeting of beoordeling kan er een verhoogd risico zijn dat afwijkingen niet worden gedetecteerd en gecorrigeerd.

A77 Belangrijke indicatoren die worden gebruikt voor het evalueren van financiële prestaties kun- nen omvatten:
- belangrijke (financiële en niet-financiële) prestatie-indicatoren en kernratio's, trends en be- drijfsstatistieken;
- vergelijkingen van financiële prestaties tussen verslagperiodes;
- budgetten, prognoses, verschillenanalyses, gesegmenteerde informatie en prestatieversla- gen op divisie-, afdelings- of ander niveau;
- maatstaven voor de personeelsprestaties en beleidslijnen inzake op stimulansen geba- seerde beloningen;
- vergelijkingen van de prestaties van een entiteit met die van concurrenten.

Schaalbaarheid (Zie Par. 19(a)(iii))

A78. The procedures undertaken to understand the entity's measures may vary depending on the size or complexity of the entity, as well as the involvement of owners or those charged with governance in the management of the entity.	A78 De werkzaamheden die worden ondernomen om inzicht te verwerven in de maatstaven van de entiteit, kunnen variëren, afhankelijk van de grootte of complexiteit van de entiteit, evenals de betrokkenheid van eigenaren of de met governance belaste personen in het management van de entiteit.
Other considerations A79. External parties may also review and analyze the entity's financial performance, in particular for entities where financial information is publicly available. The auditor may also consider publicly available information to help the auditor further understand the business or identify contradictory information such as information from: • Analysts or credit agencies. • News and other media, including social media. • Taxation authorities. • Regulators. • Trade unions. • Providers of finance. Such financial information can often be obtained from the entity being audited. A80. The measurement and review of financial performance is not the same as the monitoring of the system of internal control (discussed as a component of the system of internal control in paragraphs A114–A122), though their purposes may overlap: • The measurement and review of performance is directed at whether business performance is meeting the objectives set by management (or third parties). • In contrast, monitoring of the system of internal control is concerned with monitoring the effectiveness of controls including those related to management's measurement and review of financial performance. In some cases, however, performance indicators also provide information that enables management to identify control deficiencies.	Andere overwegingen A79 Externe partijen kunnen ook de financiële prestaties van de entiteit beoordelen en analyseren, met name van entiteiten waar financiële informatie openbaar is. De accountant kan ook open- baar beschikbare informatie beschouwen om de accountant te helpen beter inzicht te verwer- ven in de activiteiten of tegenstrijdige informatie te identificeren zoals informatie van: • analisten of kredietbeoordelaars; • nieuws en andere media, inclusief sociale media; • belastingautoriteiten; • regelgevers of toezichthouders; • vakbonden; • financiers. Dergelijke financiële informatie kan vaak worden verkregen van de gecontroleerde entiteit. A80 Het meten en beoordelen van financiële prestaties is niet hetzelfde als het monitoren van het systeem van interne beheersing (besproken als onderdeel van het systeem van interne be- heersing in paragrafen A114 – A122), hoewel hun doelen elkaar kunnen overlappen: • de meting en beoordeling van prestaties is gericht op de vraag of bedrijfsprestaties voldoen aan de doelstellingen van het management (of van derden); • het monitoren van het systeem van interne beheersing heeft daarentegen betrekking op het monitoren van de effectiviteit van interne beheersingsmaatregelen, inclusief degenen met betrekking tot de meting en beoordeling van de financiële prestatie door het manage- ment. In sommige gevallen bieden prestatie-indicatoren echter ook informatie die het management in staat stelt om tekortkomingen in de interne beheersing te identificeren.
Considerations specific to public sector entities A81. In addition to considering relevant measures used by a public sector entity to assess the entity's financial performance, auditors of public sector entities may also consider non-financial information such as achievement of public benefit outcomes (for example, the number of people assisted by a specific program).	Overwegingen specifiek voor entiteiten in de publieke sector A81 Naast het overwegen van relevante maatstaven die door een entiteit in de publieke sector wor- den gebruikt om de financiële prestaties van de entiteit in te schatten, kunnen accountants van entiteiten in de publieke sector ook niet-financiële informatie overwegen zoals het behalen van resultaten van algemeen nut (bijvoorbeeld het aantal mensen dat wordt bijgestaan door een specifiek programma).
The Applicable Financial Reporting Framework (Ref: Para. 19(b)) Understanding the Applicable Financial Reporting Framework and the Entity's Accounting Policies	Het van toepassing zijnde stelsel inzake financiële verslaggeving (Zie Par. 19(b)) Inzicht in het van toepassing zijnde stelsel inzake financiële verslaggeving en de grondslagen voor financiële verslaggeving van de entiteit

A82. Matters that the auditor may consider when obtaining an understanding of the entity's applicable financial reporting framework, and how it applies in the context of the nature and circumstances of the entity and its environment include: • The entity's financial reporting practices in terms of the applicable financial reporting framework, such as: o Accounting principles and industry-specific practices, including for industry-specific significant classes of transactions, account balances and related disclosures in the financial statements (for example, loans and investments for banks, or research and development for pharmaceuticals). o Revenue recognition. o Accounting for financial instruments, including related credit losses. o Foreign currency assets, liabilities and transactions. o Accounting for unusual or complex transactions including those in controversial or emerging areas (for example, accounting for cryptocurrency). • An understanding of the entity's selection and application of accounting policies, including any changes thereto as well as the reasons therefore, may encompass such matters as: o The methods the entity uses to recognize, measure, present and disclose significant and unusual transactions. o The effect of significant accounting policies in controversial or emerging areas for which there is a lack of authoritative guidance or consensus. o Changes in the environment, such as changes in the applicable financial reporting framework or tax reforms that may necessitate a change in the entity's accounting policies. o Financial reporting standards and laws and regulations that are new to the entity and when and how the entity will adopt, or comply with, such requirements. A83. Obtaining an understanding of the entity and its environment may assist the auditor in considering where changes in the entity's financial reporting (e.g., from prior periods) may be expected. Considerations specific to public sector entities A84. The applicable financial reporting framework in a public sector entity is determined by the legislative and regulatory frameworks relevant to each jurisdiction or within each geographical area. Matters that may be considered in the entity's application of the applicable financial reporting requirements, and how it applies in the context of the nature and circumstances of the entity and its environment, include whether the entity applies a full accrual basis of accounting or a cash basis of accounting in accordance with the International Public Sector Accounting Standards, or a hybrid. How Inherent Risk Factors Affect Susceptibility of Assertions to Misstatement (Ref: Para. 19(c)) Why the auditor understands inherent risk factors when understanding the entity and its environment and the applicable financial reporting framework A85. Understanding the entity and its environment, and the applicable financial reporting framework, assists the auditor in identifying events or conditions, the characteristics of which may affect the susceptibility of assertions	A82 Aangelegenheden die de accountant kan overwegen bij het verkrijgen van inzicht in het van toepassing zijnde stelsel voor financiële verslaggeving van de entiteit en hoe dit van toepas- sing is in de context van de aard en omstandigheden van de entiteit en haar omgeving omvat- ten: • de financiële verslaggevingspraktijken van de entiteit in termen van het van toepassing zijnde stelsel inzake financiële verslaggeving, zoals: o verslaggevingsprincipes en sectorspecifieke praktijken, inclusief sectorspecifieke signi- ficante transactiestromen, rekeningsaldi en daarmee verband houdende toelichtingen in de financiële overzichten (bijvoorbeeld leningen en investeringen bij banken, of on- derzoek en ontwikkeling bij farmaceutische bedrijven); o opbrengstverantwoording; o administratieve verwerking van financiële instrumenten, inclusief gerelateerde krediet- verliezen; o activa, passiva en transacties in vreemde valuta; o administratieve verwerking van ongebruikelijke of complexe transacties, waaronder transacties in controversiële of nieuwe gebieden (bijvoorbeeld crypto valuta). • inzicht in de keuze en toepassing van de grondslagen voor financiële verslaggeving door de entiteit, inclusief eventuele wijzigingen daarin, evenals de redenen daarvoor, kan aan- gelegenheden omvatten zoals: o de methoden die de entiteit gebruikt om significante en ongebruikelijke transacties te herkennen, te waarderen, te presenteren en toe te lichten; o het effect van significante grondslagen voor financiële verslaggeving in controversiële of nieuwe gebieden waarvoor er een gebrek is aan gezaghebbende leidraden of con- sensus; o wijzigingen in haar omgeving, zoals wijzigingen in het van toepassing zijnde stelsel in- zake financiële verslaggeving of belastinghervormingen die een wijziging in de grond- slagen voor financiële verslaggeving van de entiteit noodzakelijk maken; o standaarden inzake financiële verslaggeving en wet- en regelgeving die nieuw zijn voor de entiteit en wanneer en hoe de entiteit dergelijke vereisten zal toepassen of na- leven. A83 Het verwerven van inzicht in de entiteit en haar omgeving kan de accountant helpen bij het overwegen waar wijzigingen in de financiële verslaggeving van de entiteit (bijvoorbeeld vanuit voorgaande verslagperioden) kunnen worden verwacht. Overwegingen specifiek voor entiteiten in de publieke sector A84 Het van toepassing zijnde stelsel voor financiële verslaggeving in een entiteit in de publieke sector wordt bepaald door de wet- en regelgevingskaders die relevant zijn voor elke jurisdictie of binnen elk geografisch gebied. Aangelegenheden die overwogen kunnen worden bij de toe- passing door de entiteit van het van toepassing zijnde stelsel inzake financiële verslaggeving en hoe het van toepassing is in de context van de aard en omstandigheden van de entiteit en haar omgeving, omvatten of de entiteit financiële verslaggeving volledig op basis van toereke- ning of op kasbasis toepast in overeenstemming met de International Public Sector Accounting Standards, of een hybride vorm. Hoe inherente risicofactoren de vatbaarheid van beweringen voor afwijkingen beïnvloeden (Zie Par. 19(c)) Waarom de accountant inzicht verwerft in inherente risicofactoren bij het verwerven van inzicht in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving

about classes of transactions, account balances or disclosures to misstatement. These characteristics are inherent risk factors. Inherent risk factors may affect susceptibility of assertions to misstatement by influencing the likelihood of occurrence of a misstatement or the magnitude of the misstatement if it were to occur. Understanding how inherent risk factors affect the susceptibility of assertions to misstatement may assist the auditor with a preliminary understanding of the likelihood or magnitude of misstatements, which assists the auditor in identifying risks of material misstatement at the assertion level in accordance with paragraph 28(b). Understanding the degree to which inherent risk factors affect susceptibility of assertions to misstatement also assists the auditor in assessing the likelihood and magnitude of a possible misstatement when assessing inherent risk in accordance with paragraph 31(a). Accordingly, understanding the inherent risk factors may also assist the auditor in designing and performing further audit procedures in accordance with ISA 330. A86. The auditor's identification of risks of material misstatement at the assertion level and assessment of inherent risk may also be influenced by audit evidence obtained by the auditor in performing other risk assessment procedures, further audit procedures or in fulfilling other requirements in the ISAs (see paragraphs A95, A103, A111, A121, A124 and A151). The effect of inherent risk factors on a class of transactions, account balance or disclosure A87. The extent of susceptibility to misstatement of a class of transactions, account balance or disclosure arising from complexity or subjectivity is often closely related to the extent to which it is subject to change or uncertainty. A88. The greater the extent to which a class of transactions, account balance or disclosure is susceptible to misstatement because of complexity or subjectivity, the greater the need for the auditor to apply professional skepticism. Further, when a class of transactions, account balance or disclosure is susceptible to misstatement because of complexity, subjectivity, change or uncertainty, these inherent risk factors may create opportunity for management bias, whether unintentional or intentional, and affect susceptibility to misstatement due to management bias. The auditor's identification of risks of material misstatement, and assessment of inherent risk at the assertion level, are also affected by the interrelationships among inherent risk factors. A89. Events or conditions that may affect susceptibility to misstatement due to management bias may also affect susceptibility to misstatement due to other fraud risk factors. Accordingly, this may be relevant information for use in accordance with paragraph 24 of ISA 240, which requires the auditor to evaluate whether the information obtained from the other risk assessment procedures and related activities indicates that one or more fraud risk factors are present. Obtaining an Understanding of the Entity's System of Internal Control (Ref: Para. 21–27)	A85 Inzicht in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving, helpt de accountant bij het identificeren van gebeurtenissen of omstandigheden, waarvan de kenmerken de vatbaarheid van beweringen over transactiestromen, rekeningsaldi of toelichtingen voor afwijkingen beïnvloeden. Deze kenmerken zijn inherente risicofactoren. Inherente risicofactoren kunnen de vatbaarheid van beweringen voor afwijkingen beïnvloeden door de waarschijnlijkheid van het voorkomen of de orde van grootte van de afwijking als deze zich zou voordoen te beïnvloeden. Inzicht in hoe inherente risicofactoren de vatbaarheid van beweringen voor afwijkingen beïnvloeden, kan de accountant helpen met een voorlopig inzicht in de waarschijnlijkheid of orde van grootte van afwijkingen, dat de accountant helpt bij het identificeren van risico's op een afwijking van materieel belang op het niveau van beweringen in overeenstemming met paragraaf 28 (b). Inzicht in de mate waarin inherente risicofactoren de vatbaarheid van beweringen voor afwijkingen beïnvloeden, helpt de accountant ook bij het in- schatten van de waarschijnlijkheid en de orde van grootte van een mogelijke afwijking bij het inschatten van het inherente risico in overeenstemming met paragraaf 31(a). Overeenkomstig, kan inzicht in de inherente risicofactoren de accountant ook helpen bij het opzetten en verder uitvoeren van controlewerkzaamheden in overeenstemming met Standaard 330. A86 De identificatie door de accountant van risico's op een afwijking van materieel belang op het niveau van beweringen en de inschatting van inherent risico kan ook worden beïnvloed door controle-informatie die de accountant heeft verkregen bij het uitvoeren van andere risico-in-schattingswerkzaamheden, verdere controlewerkzaamheden of bij het voldoen aan andere ver- eisten in de Standaarden (Zie Par. A95, A103, A111, A121, A124 en A151). Het effect van inherente risicofactoren op een transactiestroom, rekeningsaldo of toelichting A87 De mate van vatbaarheid voor een afwijking van een transactiestroom, rekeningsaldo of toe-lichting die voortkomt uit complexiteit of subjectiviteit hangt vaak nauw samen met de mate waaraan deze is onderworpen aan wijzigingen of onzekerheid. A88 Hoe groter de mate waarin een transactiestroom, rekeningsaldo of toelichting vatbaar is voor een afwijking als gevolg van complexiteit of subjectiviteit, des te groter is de noodzaak voor de accountant om een professioneel-kritische instelling toe te passen. Wanneer een transactie- stroom, rekeningsaldo of toelichting vatbaar is voor afwijkingen vanwege complexiteit, subjecti- viteit, wijzigingen of onzekerheid, kunnen deze inherente risicofactoren mogelijkheden creëren voor tendentie bij het management, hetzij onopzettelijk of opzettelijk, en de vatbaarheid voor een afwijking als gevolg van tendentie bij het management beïnvloeden. De identificatie door de accountant van risico's op een afwijking van materieel belang en een inschatting van het inherente risico op het niveau van beweringen worden ook beïnvloed door de onderlinge rela- ties tussen inherente risicofactoren. A89 Gebeurtenissen of omstandigheden die van invloed kunnen zijn op de vatbaarheid voor afwij-kingen als gevolg van tendentie bij het management, kunnen ook van invloed zijn op de vat- baarheid voor afwijkingen als gevolg van andere frauderisicofactoren. Dienovereenkomstig kan dit relevante informatie zijn om te gebruiken in overeenstemming met paragraaf 24 van Stan- daard 240, die van de accountant vereist om te evalueren of de informatie verkregen uit de an- dere risico-inschattingswerkzaamheden en daarmee verband houdende activiteiten erop dui- den dat een of meer frauderisicofactoren aanwezig zijn. Het verwerven van inzicht in het interne beheersingssysteem van de entiteit (Zie Par. 21 – 27)

A90. The auditor's understanding of the entity's system of internal control is obtained through risk assessment procedures performed to understand and evaluate each of the components of the system of internal control as set out in paragraphs 21 to 27.
A91. The components of the entity's system of internal control for the purpose of this ISA may not necessarily reflect how an entity designs, implements and maintains its system of internal control, or how it may classify any particular component. Entities may use different terminology or frameworks to describe the various aspects of the system of internal control. For the purpose of an audit, auditors may also use different terminology or frameworks provided all the components described in this ISA are addressed.

Scalability
A92. The way in which the entity's system of internal control is designed, implemented and maintained varies with an entity's size and complexity. For example, less complex entities may use less structured or simpler controls (i.e., policies and procedures) to achieve their objectives.

Considerations Specific to Public Sector Entities
A93. Auditors of public sector entities often have additional responsibilities with respect to internal control, for example, to report on compliance with an established code of practice or reporting on spending against budget. Auditors of public sector entities may also have responsibilities to report on compliance with law, regulation or other authority. As a result, their considerations about the system of internal control may be broader and more detailed.

Information Technology in the Components of the Entity's System of Internal Control
A94. The overall objective and scope of an audit does not differ whether an entity operates in a mainly manual environment, a completely automated environment, or an environment involving some combination of manual and automated elements (i.e., manual and automated controls and other resources used in the entity's system of internal control).

Understanding the Nature of the Components of the Entity's System of Internal Control
A95. In evaluating the effectiveness of the design of controls and whether they have been implemented (see paragraphs A175 to A181) the auditor's understanding of each of the components of the entity's system of internal control provides a preliminary understanding of how the entity identifies business risks and how it responds to them. It may also influence the auditor's identification and assessment of the risks of material misstatement in different ways (see paragraph A86). This assists the auditor in designing and performing further audit procedures, including any plans to test the operating effectiveness of controls. For example:
- The auditor's understanding of the entity's control environment, the entity's risk assessment process, and the entity's process to monitor controls components are more likely to affect the identification and assessment of risks of material misstatement at the financial statement level.
- The auditor's understanding of the entity's information system and communication, and the entity's control activities component, are more likely to affect the identification and assessment of risks of material misstatement at the assertion level.

A90 Het inzicht van de accountant in het interne beheersingssysteem van de entiteit wordt verwor- ven door risico inschattingswerkzaamheden die worden uitgevoerd om inzicht te verwerven in alle componenten van het systeem van interne beheersing zoals beschreven in de paragrafen 21-27 en deze te evalueren.

A91 Voor het doel van deze Standaard, hoeven de componenten van het interne beheersingssys- teem van de entiteit niet noodzakelijkerwijs te weerspiegelen hoe een entiteit het systeem van

interne beheersing opzet, implementeert en onderhoudt, of hoe zij een specifieke component kan classificeren. Entiteiten kunnen verschillende terminologie of stelsels gebruiken om de ver- schillende aspecten van het systeem van interne beheersing te beschrijven. Voor de doelstel- ling van een controle kunnen accountants ook andere terminologie of stelsels gebruiken, mits alle componenten die in deze Standaard worden beschreven in aanmerking worden genomen.

Schaalbaarheid

A92 De manier waarop het interne beheersingssysteem van de entiteit is ontworpen, geïmplemen- teerd en onderhouden varieert met de grootte en complexiteit van een entiteit. Minder com- plexe entiteiten kunnen bijvoorbeeld minder gestructureerde of eenvoudigere interne beheer- singsmaatregelen (d.w.z. beleidslijnen en procedures) gebruiken om hun doelstellingen te be- reiken.

Overwegingen specifiek voor entiteiten in de publieke sector

A93 Accountants van entiteiten in de publieke sector hebben vaak aanvullende verplichtingen met betrekking tot interne beheersing, bijvoorbeeld om te rapporteren over de naleving van een vastgestelde gedragscode of om te rapporteren over uitgaven ten opzichte van het budget. Ac- countants van entiteiten in de publieke sector kunnen ook verantwoordelijkheden hebben om te rapporteren over naleving van wet- en regelgeving of andere van kracht zijnde voorschriften.
Als gevolg hiervan, kunnen hun overwegingen over het systeem van interne beheersing breder en gedetailleerder zijn.

Informatietechnologie in de componenten van het interne beheersingssysteem van de entiteit

A94 De algehele doelstelling en reikwijdte van een controle verschilt niet bij een entiteit die hoofd- zakelijk actief is in een handmatige omgeving, een volledig geautomatiseerde omgeving of een omgeving met een combinatie van handmatige en geautomatiseerde elementen (d.w.z. hand- matige en geautomatiseerde interne beheersingsmaatregelen en andere middelen die worden gebruikt in het interne beheersingssysteem van de entiteit).

Inzicht in de aard van de componenten van het interne beheersingssysteem van de entiteit

A95 Bij het evalueren van de effectiviteit van de opzet van interne beheersingsmaatregelen en of deze zijn geïmplementeerd (zie paragrafen A175 tot en met A181), verschaft het inzicht van de accountant in elk van de componenten van het systeem van interne beheersing van de entiteit een voorlopig inzicht in hoe de entiteit bedrijfsrisico's identificeert en hoe het daarop inspeelt. Het kan ook de identificatie en inschatting door de accountant van de risico's op een afwijking van materieel belang op verschillende manieren beïnvloeden (zie paragraaf A86). Dit helpt de accountant bij het opzetten en uitvoeren van verdere controlewerkzaamheden, inclusief even- tuele plannen om de effectieve werking van interne beheersingsmaatregelen te toetsen. Bij- voorbeeld:
- Het inzicht van de accountant in de interne beheersingsomgeving van de entiteit, het risico- inschattingsproces van de entiteit, en het proces van de entiteit om componenten van in- terne

	beheersingsmaatregelen te monitoren, heeft waarschijnlijk meer invloed op de identi- ficatie en inschatting van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten; • Het inzicht van de accountant in het informatiesysteem en de communicatie van de entiteit, en de component 'interne beheersingsactiviteiten' van de entiteit heeft waarschijnlijk [A41]meer invloed op de identificatie en inschatting van risico's op een afwijking van materieel belang op het niveau van beweringen.
Control Environment, The Entity's Risk Assessment Process and the Entity's Process to Monitor the System of Internal Control (Ref: Para. 21–24) A96. The controls in the control environment, the entity's risk assessment process and the entity's process to monitor the system of internal control are primarily indirect controls (i.e., controls that are not sufficiently precise to prevent, detect or correct misstatements at the assertion level but which support other controls and may therefore have an indirect effect on the likelihood that a misstatement will be detected or prevented on a timely basis). However, some controls within these components may also be direct controls.	Interne beheersingsomgeving, het risico-inschattingsproces van de entiteit en het proces van de enti- teit om het systeem van interne beheersing te monitoren (Zie Par. 21 – 24) A96 De interne beheersingsmaatregelen in de interne beheersingsomgeving, het risico-inschat- tingsproces van de entiteit en het proces van de entiteit om het systeem van interne beheer- sing te monitoren, zijn voornamelijk indirecte interne beheersingsmaatregelen (d.w.z. interne
Why the auditor is required to understand the control environment, the entity's risk assessment process and the entity's process to monitor the system of internal control A97. The control environment provides an overall foundation for the operation of the other components of the system of internal control. The control environment does not directly prevent, or detect and correct, misstatements. It may, however, influence the effectiveness of controls in the other components of the system of internal control. Similarly, the entity's risk assessment process and its	beheersingsmaatregelen die niet voldoende nauwkeurig zijn om afwijkingen op het niveau van beweringen te voorkomen, detecteren of te corrigeren, maar die andere interne beheersings- maatregelen ondersteunen en daarom een indirect effect kunnen hebben op de waarschijnlijk- heid dat een afwijking tijdig gedetecteerd of voorkomen wordt). Sommige interne beheersings- maatregelen binnen deze componenten kunnen echter ook directe interne beheersingsmaatre- gelen zijn. Waarom van de accountant vereist wordt inzicht te verwerven in de interne beheersingsomgeving, het risico-inschattingsproces van de entiteit en het proces van de entiteit om het systeem van interne beheersing te monitoren
process for monitoring the system of internal control are designed to operate in a manner that also supports the entire system of internal control. A98. Because these components are foundational to the entity's system of internal control, any deficiencies in their operation could have pervasive effects on the preparation of the financial statements. Therefore, the auditor's understanding and evaluations of these components affect the auditor's identification and assessment of risks of material misstatement at the financial statement level, and may also affect the identification and assessment of risks of material misstatement at the assertion level. Risks of material misstatement at the financial statement level affect the auditor's design of overall responses, including, as explained in ISA 330, an influence on the nature, timing and extent of the auditor's further procedures.35	A97 De interne beheersingsomgeving biedt een algemeen fundament voor de werking van de an- dere componenten van het systeem van interne beheersing. De interne beheersingsomgeving voorkomt, detecteert en corrigeert niet rechtstreeks afwijkingen. Het kan echter de effectiviteit van interne beheersingsmaatregelen in de andere componenten van het systeem van interne beheersing beïnvloeden. Evenzo zijn het risico-inschattingsproces van de entiteit en het proces voor het monitoren van het systeem van interne beheersing ontworpen om op een manier te werken die ook het hele systeem van interne beheersing ondersteunt. A98 Omdat deze componenten fundamenteel zijn voor het interne beheersingssysteem van de enti- teit, kunnen tekortkomingen in hun werking gevolgen met een diepgaande invloed hebben voor het opstellen van de financiële overzichten. Daarom hebben het inzicht en de inschattingen van de accountant van deze componenten invloed op de identificatie en inschatting door de accountant van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten en kan dit ook van invloed zijn op de identificatie en inschatting van risico's op een afwijking van materieel belang op het niveau van beweringen. Risico's op een afwijking van materieel belang op het niveau van de financiële overzichten beïnvloeden de opzet van alge- hele manieren van inspelen door de accountant inclusief, zoals uitgelegd in Standaard 330, een invloed op de aard, timing en omvang van de verdere werkzaamheden van de accoun- tant.36
Obtaining an understanding of the control environment (Ref: Para. 21) Scalability A99. The nature of the control environment in a less complex entity is likely to be different from the control environment in a more complex entity. For example, those charged with governance in less complex entities may not include an independent or outside member, and the role of governance may be undertaken directly by the	Inzicht verwerven in de interne beheersingsomgeving (Zie Par. 21) Schaalbaarheid A99 De aard van de interne beheersingsomgeving in een minder complexe entiteit zal waarschijnlijk verschillen van de interne beheersingsomgeving in een meer complexe entiteit. Zo is het bij- voorbeeld mogelijk dat zich onder de met governance belaste personen in minder complexe entiteiten geen onafhankelijk of extern lid bevindt, en dat de governancefunctie direct door de eigenaar-bestuurder wordt waargenomen als er geen andere eigenaren zijn. Dienovereenkom- stig zijn

owner-manager where there are no other owners. Accordingly, some considerations about the entity's control environment may be less relevant or may not be applicable. A100. In addition, audit evidence about elements of the control environment in less complex entities may not be available in documentary form, in particular where communication between management and other personnel is informal, but the evidence may still be appropriately relevant and reliable in the circumstances. Understanding the control environment (Ref: Para. 21(a)) A101. Audit evidence for the auditor's understanding of the control environment may be obtained through a combination of inquiries and other risk assessment procedures (i.e., corroborating inquiries through observation or inspection of documents).	sommige overwegingen over de interne beheersingsomgeving van de entiteit mogelijk minder relevant of niet van toepassing. A100 Bovendien is het mogelijk dat controle-informatie over elementen van de interne beheersings-omgeving in minder complexe entiteiten niet beschikbaar is in documentvorm, met name waar communicatie tussen management en ander personeel informeel is, maar de informatie kan nog steeds relevant en betrouwbaar zijn in de omstandigheden.
35 ISA 330, paragraphs A1–A3	36 Standaard 330, paragrafen A1-A3.
A102. In considering the extent to which management demonstrates a commitment to integrity and ethical values, the auditor may obtain an understanding through inquiries of management and employees, and through considering information from external sources, about: • How management communicates to employees its views on business practices and ethical behavior; and • Inspecting management's written code of conduct and observing whether management acts in a manner that supports that code. Evaluating the control environment (Ref: Para. 21(b)) Why the auditor evaluates the control environment A103. The auditor's evaluation of how the entity demonstrates behavior consistent with the entity's commitment to integrity and ethical values; whether the control environment provides an appropriate foundation for the other components of the entity's system of internal control; and whether any identified control deficiencies undermine the other components of the system of internal control, assists the auditor in identifying potential issues in the other components of the system of internal control. This is because the control environment is foundational to the other components of the entity's system of internal control. This evaluation may also assist the auditor in understanding risks faced by the entity and therefore in identifying and assessing the risks of material misstatement at the financial statement and assertion levels (see paragraph A86). The auditor's evaluation of the control environment	Inzicht in de interne beheersingsomgeving (Zie Par. 21(a)) A101 Controle-informatie voor het inzicht van de accountant in de interne beheersingsomgeving kan worden verkregen via een combinatie van verzoeken om inlichtingen en andere risico-inschat-tingswerkzaamheden (d.w.z. bevestigende verzoeken om inlichtingen door waarneming of in- spectie van documenten). A102 Bij het overwegen van de mate waarin het management blijk geeft van toewijding aan integriteit en ethische waarden, kan de accountant inzicht verwerven door verzoeken om inlichtingen bij het management en werknemers en door informatie uit externe bronnen te overwegen, over: • hoe het management zijn visie op bedrijfspraktijken en ethisch gedrag aan werknemers communiceert; en • inspectie van de schriftelijke gedragscode van het management en waarnemen of het ma-nagement handelt op een manier die die code ondersteunt. Evalueren van de interne beheersingsomgeving (Zie Par. 21(b)) Waarom de accountant de interne beheersingsomgeving evalueert A103 De evaluatie door de accountant: • van hoe de entiteit gedrag vertoont dat consistent is met de toewijding van de entiteit aan integriteit en ethische waarden; • of de interne beheersingsomgeving een geschikte basis biedt voor de andere componen- ten van het interne beheersingssysteem van de entiteit; en • of geïdentificeerde tekortkomingen in de interne beheersing de andere componenten van het systeem van interne beheersing ondermijnen, helpt de accountant bij het identificeren van potentiële kwesties in de andere componenten van het interne beheersingssysteem. Dit komt omdat de interne beheersingsomgeving fundamen- teel is voor de andere componenten van het interne beheersingssysteem van de entiteit. Deze evaluatie kan de accountant ook helpen bij het verwerven van inzicht in risico's waarmee de entiteit geconfronteerd wordt en daarom bij het identificeren en inschatten van de risico's op een afwijking van materieel belang op het niveau van de financiële overzichten en op het ni- veau van beweringen (zie paragraaf A86). De evaluatie van de accountant van de interne beheersingsomgeving

A104. The auditor's evaluation of the control environment is based on the understanding obtained in accordance with paragraph 21(a). A105. Some entities may be dominated by a single individual who may exercise a great deal of discretion. The actions and attitudes of that individual may have a pervasive effect on the culture of the entity, which in turn may have a pervasive effect on the control environment. Such an effect may be positive or negative. A106. The auditor may consider how the different elements of the control environment may be influenced by the philosophy and operating style of senior management taking into account the involvement of independent members of those charged with governance. A107. Although the control environment may provide an appropriate foundation for the system of internal control and may help reduce the risk of fraud, an appropriate control environment is not necessarily an effective deterrent to fraud.	A104 De evaluatie van de accountant van de interne beheersingsomgeving is gebaseerd op het in- zicht verkregen in overeenstemming met paragraaf 21(a). A105 Sommige entiteiten kunnen worden gedomineerd door een enkele persoon die veel zelf kan bepalen. De handelingen en houding van die persoon kunnen een diepgaande invloed hebben op de cultuur van de entiteit, die wederom een diepgaande invloed kan hebben op de interne beheersingsomgeving. Een dergelijk effect kan positief of negatief zijn. A106 De accountant kan overwegen hoe de verschillende elementen van de interne beheersingsom- geving kunnen worden beïnvloed door de filosofie en werkstijl van het senior management, re- kening houdend met de betrokkenheid van onafhankelijke leden van de met governance be- laste personen. A107 Hoewel de interne beheersingsomgeving een geschikte basis kan vormen voor het systeem van interne beheersing en kan helpen het risico op fraude te verminderen, is een geschikte in- terne beheersingsomgeving niet noodzakelijk een effectief afschrikmiddel tegen fraude.
A108. The auditor's evaluation of the control environment as it relates to the entity's use of IT may include such matters as: • Whether governance over IT is commensurate with the nature and complexity of the entity and its business operations enabled by IT, including the complexity or maturity of the entity's technology platform or architecture and the extent to which the entity relies on IT applications to support its financial reporting. • The management organizational structure regarding IT and the resources allocated (for example, whether the entity has invested in an appropriate IT environment and necessary enhancements, or whether a sufficient number of appropriately skilled individuals have been employed including when the entity uses commercial software (with no or limited modifications)).	A108 De evaluatie van de accountant van de interne beheersingsomgeving met betrekking tot het gebruik van IT door de entiteit kan aangelegenheden omvatten als: • de vraag of governance over IT in verhouding staat tot de aard en complexiteit van de enti- teit en de bedrijfsactiviteiten mogelijk gemaakt door IT, inclusief de complexiteit of volwas- senheid van het technologieplatform of architectuur van de entiteit en de mate waarin de entiteit afhankelijk is van IT-applicaties ter ondersteuning van de financiële verslaggeving; • de organisatiestructuur van het management met betrekking tot IT en de toegewezen mid- delen (bijvoorbeeld of de entiteit in een geschikte IT-omgeving en noodzakelijke verbeterin- gen heeft geïnvesteerd, of dat een voldoende aantal geschikte deskundige personen in dienst zijn, ook wanneer de entiteit commerciële software gebruikt (met geen of beperkte) modificaties)).
Obtaining an understanding of the entity's risk assessment process (Ref: Para. 22–23) Understanding the entity's risk assessment process (Ref: Para. 22(a)) A109. As explained in paragraph A62, not all business risks give rise to risks of material misstatement. In understanding how management and those charged with governance have identified business risks relevant to the preparation of the financial statements, and decided about actions to address those risks, matters the auditor may consider include how management or, as appropriate, those charged with governance, has: • Specified the entity's objectives with sufficient precision and clarity to enable the identification and assessment of the risks relating to the objectives; • Identified the risks to achieving the entity's objectives and analyzed the risks as a basis for determining how the risks should be managed; and • Considered the potential for fraud when considering the risks to achieving the entity's objectives.36 A110. The auditor may consider the implications of such business risks for the preparation of the entity's financial statements and other aspects of its system of internal control.	Verwerven van inzicht in het risico-inschattingsproces van de entiteit (Zie Par. 22 – 23) Inzicht in het risico-inschattingsproces van de entiteit (Zie Par. 22(a)) A109 Zoals uitgelegd in paragraaf A62, geven niet alle bedrijfsrisico's aanleiding tot risico's op een afwijking van materieel belang. Bij het verwerven van inzicht in hoe het management en de met governance belaste personen bedrijfsrisico's hebben geïdentificeerd die relevant zijn voor het opstellen van de financiële overzichten en hebben besloten over handelingen om op deze ri- sico's in te spelen, zijn aangelegenheden die de accountant kan overwegen onder meer hoe het management of, in voorkomend geval, de personen belast met governance: • de doelstellingen van de entiteit met voldoende precisie en duidelijkheid heeft gespecifi- ceerd om de identificatie en inschatting van de risico's met betrekking tot de doelstellingen mogelijk te maken; • de risico's voor het bereiken van de doelstellingen van de entiteit heeft gespecificeerd en de risico's heeft geanalyseerd als basis voor het bepalen hoe de risico's moeten worden beheerd; en • het potentieel voor fraude heeft beschouwd bij het overwegen van de risico's om de doel- stellingen van de entiteit te bereiken.37 A110 De accountant kan de implicaties van dergelijke bedrijfsrisico's voor het opstellen van de finan- ciële overzichten van de entiteit en andere aspecten van het interne beheersingssysteem over- wegen.
Evaluating the entity's risk assessment process (Ref: Para. 22(b)) Why the auditor evaluates whether the entity's risk assessment process is appropriate	Evalueren van het risico-inschattingsproces van de entiteit (Zie Par. 22(b)) Waarom de accountant evalueert of het risico-inschattingsproces van de entiteit geschikt is

A111. The auditor's evaluation of the entity's risk assessment process may assist the auditor in understanding where the entity has identified risks that may occur, and how the entity has responded to those risks. The auditor's evaluation of how the entity identifies its business risks, and how it assesses and addresses those risks assists the auditor in understanding whether the risks faced by the entity have been identified, assessed and addressed as appropriate to the nature and complexity of the entity. This evaluation may also assist the auditor with identifying and assessing financial statement level and assertion level risks of material misstatement (see paragraph A86). Evaluating whether the entity's risk assessment process is appropriate (Ref: Para. 22(b)) A112. The auditor's evaluation of the appropriateness of the entity's risk assessment process is based on the understanding obtained in accordance with paragraph 22(a). Scalability A113. Whether the entity's risk assessment process is appropriate to the entity's circumstances considering the nature and complexity of the entity is a matter of the auditor's professional judgment. Obtaining an understanding of the entity's process to monitor the entity's system of internal control (Ref: Para. 24) Scalability A114. In less complex entities, and in particular owner-manager entities, the auditor's understanding of the entity's process to monitor the system of internal control is often focused on how management or the owner-manager is directly involved in operations, as there may not be any other monitoring activities. A115. For entities where there is no formal process for monitoring the system of internal control, understanding the process to monitor the system of internal control may include understanding periodic reviews of management accounting information that are designed to contribute to how the entity prevents or detects misstatements. Understanding the entity's process to monitor the system of internal control (Ref: Para. 24(a)) A116. Matters that may be relevant for the auditor to consider when understanding how the entity monitors its system of internal control include: • The design of the monitoring activities, for example whether it is periodic or ongoing monitoring; • The performance and frequency of the monitoring activities; • The evaluation of the results of the monitoring activities, on a timely basis, to determine whether the controls have been effective; and	A111 De evaluatie door de accountant van het risico-inschattingsproces van de entiteit kan de ac-countant helpen bij het verwerven van inzicht waar de entiteit risico's heeft geïdentificeerd die kunnen voorkomen en hoe de entiteit heeft ingespeeld op die risico's. De evaluatie van de ac- countant hoe de entiteit de bedrijfsrisico's identificeert, inschat en erop inspeelt, helpt de ac- countant bij het inzicht of deze risico's als passend voor de aard en complexiteit van de entiteit zijn geïdentificeerd, ingeschat en hoe erop is ingespeeld. Deze evaluatie kan de accountant ook helpen bij het identificeren en inschatten van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten en op het niveau van beweringen (Zie Par. A86). Evalueren of het risico-inschattingsproces van de entiteit geschikt is (Zie Par. 22(b)) 37 Standaard 240, paragraaf 19. A112 De evaluatie door de accountant van de geschiktheid van het risico-inschattingsproces van de entiteit is gebaseerd op het inzicht verkregen in overeenstemming met paragraaf 22(a). Schaalbaarheid A113 Of het risico-inschattingsproces van de entiteit geschikt is voor de omstandigheden gezien de aard en complexiteit van de entiteit is een kwestie van professionele oordeelsvorming door de accountant. Het verwerven van inzicht in het proces van de entiteit om het interne beheersingssysteem van de entiteit te monitoren (Zie Par. 24) Schaalbaarheid A114 In minder complexe entiteiten, en met name door de eigenaar bestuurde entiteiten, is het in-zicht van de accountant in het proces van de entiteit om het systeem van interne beheersing te monitoren vaak gericht op hoe het management of de eigenaar-bestuurder direct betrokken is bij activiteiten, omdat er mogelijk geen andere monitoringactiviteiten zijn. A115 Er zijn entiteiten die geen formeel proces voor het monitoren van het systeem van interne be-heersing hebben. Bij deze entiteiten kan inzicht in het proces om het systeem van interne be- heersing te monitoren inzicht in periodieke beoordelingen van management accounting infor- matie die is opgezet om bij te dragen aan hoe de entiteit afwijkingen voorkomt of detecteert, omvatten. Inzicht in het proces van de entiteit om het systeem van interne beheersing te monitoren (Zie Par. 24(a)) A116 Aangelegenheden die relevant kunnen zijn voor de accountant om te overwegen bij het ver-werven van inzicht hoe de entiteit het systeem van interne beheersing monitort, omvatten: • de opzet van de monitoringactiviteiten, bijvoorbeeld of het periodieke of doorlopende moni-toring is; • de prestaties [A42]en frequentie van de monitoringactiviteiten; • de evaluatie van de resultaten van de monitoringactiviteiten, op een tijdige basis, om te be-palen of de interne beheersingsmaatregelen effectief zijn geweest; en

• How identified deficiencies have been addressed through appropriate remedial actions, including timely communication of such deficiencies to those responsible for taking remedial action. A117. The auditor may also consider how the entity's process to monitor the system of internal control addresses monitoring information processing controls that involve the use of IT. This may include, for example: • Controls to monitor complex IT environments that: o Evaluate the continuing design effectiveness of information processing controls and modify them, as appropriate, for changes in conditions; or o Evaluate the operating effectiveness of information processing controls. • Controls that monitor the permissions applied in automated information processing controls that enforce the segregation of duties. • Controls that monitor how errors or control deficiencies related to the automation of financial reporting are identified and addressed. Understanding the entity's internal audit function (Ref: Para. 24(a)(ii)) A118. The auditor's inquiries of appropriate individuals within the internal audit function help the auditor obtain an understanding of the nature of the internal audit function's responsibilities. If the auditor determines that the function's responsibilities are related to the entity's financial reporting, the auditor may obtain further understanding of the activities performed, or to be performed, by the internal audit function by reviewing the internal audit function's audit plan for the period, if any, and discussing that plan with the appropriate individuals within the function. This understanding, together with the information obtained from the auditor's inquiries, may also provide information that is directly relevant to the auditor's identification and assessment of the risks of material misstatement. If, based on the auditor's preliminary understanding of the internal audit function, the auditor expects to use the work of the internal audit function to modify the nature or timing, or reduce the extent, of audit procedures to be performed, ISA 610 (Revised 2013)37 applies. Other sources of information used in the entity's process to monitor the system of internal control Understanding the sources of information (Ref: Para. 24(b)) A119. Management's monitoring activities may use information in communications from external parties such as customer complaints or regulator comments that may indicate problems or highlight areas in need of improvement. Why the auditor is required to understand the sources of information used for the entity's monitoring of the system of internal control	• hoe vastgestelde tekortkomingen zijn behandeld door passende corrigerende maatregelen, inclusief tijdige communicatie van dergelijke tekortkomingen aan degenen die verantwoor- delijk zijn voor het nemen van corrigerende maatregelen. A117 De accountant kan ook overwegen hoe het proces van de entiteit om het systeem van interne beheersing te monitoren interne beheersingsmaatregelen met betrekking tot informatieverwer- king behandelt waarbij IT wordt gebruikt. Dit kan bijvoorbeeld omvatten: • interne beheersingsmaatregelen om complexe IT-omgevingen te monitoren die: o de voortdurende effectieve opzet van interne beheersingsmaatregelen met betrekking tot informatieverwerking evalueren en deze wijzigen, voor zover van toepassing, voor veranderingen in omstandigheden; of o de effectieve werking van interne beheersingsmaatregelen met betrekking tot informa- tieverwerking evalueren. • interne beheersingsmaatregelen die de toegangsrechten monitoren die zijn toegepast in geautomatiseerde interne beheersingsmaatregelen met betrekking tot informatieverwerking die de functiescheiding afdwingen; • interne beheersingsmaatregelen die monitoren hoe fouten of tekortkomingen in de interne beheersing met betrekking tot de automatisering van financiële verslaggeving worden ge- identificeerd en behandeld. Inzicht in de interne auditfunctie van de entiteit (Zie Par. 24(a)(ii)) A118 De verzoeken om inlichtingen van de accountant bij de juiste personen binnen de interne audit- functie helpen de accountant inzicht te verwerven in de aard van de verantwoordelijkheden van de interne auditfunctie. Als de accountant bepaalt dat de verantwoordelijkheden van de functie verband houden met de financiële verslaggeving van de entiteit, kan de accountant nader in- zicht verwerven in de activiteiten die door de interne audit zijn uitgevoerd of zullen worden uit- gevoerd door het auditplan van de interne auditfunctie voor de verslagperiode te beoordelen, voor zover dit bestaat, en dat plan te bespreken met de juiste personen binnen de functie. Dit inzicht, samen met de informatie die verkregen is uit verzoeken om inlichtingen van de accoun- tant, kan ook informatie verschaffen die direct relevant is voor de identificatie en inschatting van de accountant van de risico's op een afwijking van materieel belang. Als de accountant op basis van het voorlopige inzicht van de accountant van de interne auditfunctie verwacht ge- bruik te maken van het werk van de interne auditfunctie om de aard of timing van controlewerk- zaamheden te wijzigen of de omvang daarvan te verminderen, is Standaard 61038 van toepas- sing. Andere informatiebronnen die worden gebruikt in het proces van de entiteit om het systeem van in- terne beheersing te monitoren Inzicht verwerven in de informatiebronnen (Zie Par. 24(b)) A119 Tot de monitoringactiviteiten van het management kan behoren het gebruikmaken van informa- tie die uit communicatie met externe partijen is verkregen zoals klachten van klanten of opmer- kingen van regelgevende instanties die kunnen duiden op problemen of die de aandacht vesti- gen op gebieden waarop verbeteringen nodig zijn. Waarom van de accountant vereist wordt inzicht te verwerven in de informatiebronnen die worden gebruikt voor het monitoren van het systeem van interne beheersing van de entiteit

A120. The auditor's understanding of the sources of information used by the entity in monitoring the entity's system of internal control, including whether the information used is relevant and reliable, assists the auditor in evaluating whether the entity's process to monitor the entity's system of internal control is appropriate. If management assumes that information used for monitoring is relevant and reliable without having a basis for that assumption, errors that may exist in the information could potentially lead management to draw incorrect conclusions from its monitoring activities.	A120 Het inzicht van de accountant in de informatiebronnen die door de entiteit worden gebruikt bij het monitoren van het systeem van interne beheersing van de entiteit, inclusief of de gebruikte informatie relevant en betrouwbaar is, helpt de accountant bij het evalueren of het proces van de entiteit om het systeem van interne beheersing van de entiteit te monitoren, geschikt is. Als het management veronderstelt dat informatie die wordt gebruikt voor monitoring relevant en betrouwbaar is zonder een basis voor die veronderstelling te hebben, kunnen eventuele fouten in de informatie ertoe leiden dat het management verkeerde conclusies trekt uit zijn monitoring-activiteiten.
Evaluating the entity's process to monitor the system of internal control (Ref: Para 24(c)) Why the auditor evaluates whether the entity's process to monitor the system of internal control is appropriate A121. The auditor's evaluation about how the entity undertakes ongoing and separate evaluations for monitoring the effectiveness of controls assists the auditor in understanding whether the other components of the entity's system of internal control are present and functioning, and therefore assists with understanding the other components of the entity's system of internal control. This evaluation may also assist the auditor with identifying and assessing financial statement level and assertion level risks of material misstatement (see paragraph A86).	Evalueren van het proces van de entiteit om het systeem van interne beheersing te monitoren (Zie Par. 24(c)) Waarom de accountant evalueert of het proces van de entiteit om het systeem van interne beheer-sing te monitoren, geschikt is
Evaluating whether the entity's process to monitor the system of internal control is appropriate (Ref: Para. 24(c)) A122. The auditor's evaluation of the appropriateness of the entity's process to monitor the system of internal control is based on the auditor's understanding of the entity's process to monitor the system of internal control.	A121 De evaluatie van de accountant over hoe de entiteit doorlopende en afzonderlijke evaluaties onderneemt voor het monitoren van de effectiviteit van interne beheersingsmaatregelen, helpt
Information System and Communication, and Control Activities (Ref: Para. 25–26) A123. The controls in the information system and communication, and control activities components are primarily direct controls (i.e., controls that are sufficiently precise to prevent, detect or correct misstatements at the assertion level).	38 Standaard 610 (herzien 2013), Gebruikmaken van het werk van interne auditors. de accountant bij het verwerven van inzicht of de ander componenten van het interne beheer-singssysteem van de entiteit aanwezig zijn en functioneren. Dit helpt daarom bij het verwerven van inzicht in de andere componenten van het interne beheersingssysteem van de entiteit.
37 ISA 610 (Revised 2013), Using the Work of Internal Auditors	Deze evaluatie kan de accountant ook helpen bij het identificeren en inschatten van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten en op het ni- veau van beweringen (zie paragraaf A86). Evalueren of het proces van de entiteit om het systeem van interne beheersing te controleren, ge-schikt is (Zie Par. 24(c))
	A122 De evaluatie door de accountant van de geschiktheid van het proces van de entiteit om het systeem van interne beheersing te monitoren, is gebaseerd op het inzicht van de accountant in het proces van de entiteit om het systeem van interne beheersing te monitoren.
	Informatiesysteem en communicatie en interne beheersingsactiviteiten (Zie Par. 25 – 26)
	A123 De componenten interne beheersingsmaatregelen in het 'informatiesysteem en communicatie' en 'interne beheersingsactiviteiten' zijn primair directe interne beheersingsmaatregelen (d.w.z. interne beheersingsmaatregelen die voldoende nauwkeurig zijn om afwijkingen op het niveau van beweringen te voorkomen, detecteren of corrigeren).
Why the auditor Is required to understand the information system and communication and controls in the control activities component A124. The auditor is required to understand the entity's information system and communication because understanding the entity's policies that define the flows of transactions and other aspects of the entity's information processing activities relevant to the preparation of the financial statements, and evaluating whether the component appropriately supports the preparation of the entity's financial statements, supports the auditor's identification and assessment of risks of material misstatement at the assertion level. This understanding and evaluation may also result in the identification of risks of material misstatement at the financial statement level when the results of the auditor's procedures are inconsistent with expectations about the entity's system of	Waarom van de accountant vereist wordt inzicht te verwerven in het informatiesysteem en communi-catie en interne beheersingsmaatregelen in de component 'interne beheersingsactiviteiten' A124 Van de accountant wordt vereist om inzicht te verwerven in het informatiesysteem en de com-municatie van de entiteit. Dit is nodig omdat inzicht in de beleidslijnen van de entiteit die de transactiestromen en andere aspecten van de informatieverwerkingsactiviteiten van de entiteit definiëren die relevant zijn voor het opstellen van de financiële overzichten en het evalueren of de component op passende wijze het opstellen van de financiële overzichten van de entiteit ondersteunt, de identificatie en inschatting van de accountant van risico's op een afwijking van materieel belang op

internal control that may have been set based on information obtained during the engagement acceptance or continuance process (see paragraph A86). A125. The auditor is required to identify specific controls in the control activities component, and evaluate the design and determine whether the controls have been implemented, as it assists the auditor's understanding about management's approach to addressing certain risks and therefore provides a basis for the design and performance of further audit procedures responsive to these risks as required by ISA 330. The higher on the spectrum of inherent risk a risk is assessed, the more persuasive the audit evidence needs to be. Even when the auditor does not plan to test the operating effectiveness of identified controls, the auditor's understanding may still affect the design of the nature, timing and extent of substantive audit procedures that are responsive to the related risks of material misstatement. The iterative nature of the auditor's understanding and evaluation of the information system and communication, and control activities A126. As explained in paragraph A49, the auditor's understanding of the entity and its environment, and the applicable financial reporting framework, may assist the auditor in developing initial expectations about the classes of transactions, account balances and disclosures that may be significant classes of transactions, account balances and disclosures. In obtaining an understanding of the information system and communication component in accordance with paragraph 25(a), the auditor may use these initial expectations for the purpose of determining the extent of understanding of the entity's information processing activities to be obtained. A127. The auditor's understanding of the information system includes understanding the policies that define flows of information relating to the entity's significant classes of transactions, account balances, and disclosures, and other related aspects of the entity's information processing activities. This information, and the information obtained from the auditor's evaluation of the information system may confirm or further influence the auditor's expectations about the significant classes of transactions, account balances and disclosures initially identified (see paragraph A126). A128. In obtaining an understanding of how information relating to significant classes of transactions, account balances and disclosures flows into, through, and out of the entity's information system, the auditor may also identify controls in the control activities component that are required to be identified in accordance with paragraph 26(a). The auditor's identification and evaluation of controls in the control activities component may first focus on controls over journal entries and controls that the auditor plans to test the operating effectiveness of in designing the nature, timing and extent of substantive procedures. A129. The auditor's assessment of inherent risk may also influence the identification of controls in the control activities component. For example, the auditor's identification of controls relating to significant risks may only be identifiable when the auditor has assessed inherent risk at the assertion level in accordance with paragraph 31.	het niveau van beweringen ondersteunt. Dit inzicht en deze evaluatie kun- nen ook leiden tot de identificatie van risico's op een afwijking van materieel belang op het ni- veau van de financiële overzichten, wanneer de resultaten van de werkzaamheden van de ac- countant niet consistent zijn met verwachtingen over het systeem van interne beheersing van de entiteit dat mogelijk was gebaseerd op informatie die verkregen is tijdens het proces voor aanvaarding of continuering van de opdracht. (Zie Par. A86) A125 Van de accountant wordt vereist om specifieke interne beheersingsmaatregelen in de compo- nent 'interne beheersingsactiviteiten' te identificeren, de opzet te evalueren en te bepalen of de interne beheersingsmaatregelen zijn geïmplementeerd, aangezien dit de accountant helpt in- zicht te verwerven in de aanpak van het management om in te spelen op bepaalde risico's. Dit biedt daarom een basis voor de opzet en de uitvoering van verdere controlewerkzaamheden die inspelen op deze risico's, zoals vereist door Standaard 330. Hoe hoger in het spectrum van inherent risico een risico is ingeschat, hoe overtuigender de controle-informatie moet zijn. Zelfs wanneer de accountant niet van plan is om de effectieve werking van geïdentificeerde interne beheersingsmaatregelen te toetsen, kan het inzicht van de accountant nog steeds van invloed zijn op de opzet van de aard, timing en omvang van gegevensgerichte controlewerkzaamhe- den die inspelen op de daarmee samenhangende risico's op een afwijking van materieel be- lang. De iteratieve aard van het inzicht en de evaluatie van de accountant van het informatiesysteem en communicatie- en interne beheersingsactiviteiten A126 Zoals uitgelegd in paragraaf A49, verwerft de accountant inzicht in de entiteit en haar omge- ving en het van toepassing zijnde stelsel inzake financiële verslaggeving. Dit inzicht kan de ac- countant helpen bij het ontwikkelen van initiële verwachtingen over de transactiestromen, reke- ningsaldi en toelichtingen die significante transactiestromen, rekeningsaldi en toelichtingen kunnen zijn. Bij het verwerven van inzicht in de component 'informatie systeem en communica- tie' in overeenstemming met paragraaf 25(a), kan de accountant deze initiële verwachtingen gebruiken om de mate van inzicht in de informatieverwerkingsactiviteiten van de entiteit die moet worden verkregen, te bepalen. A127 Het inzicht van de accountant in het informatiesysteem omvat het verwerven van inzicht in de beleidslijnen die informatiestromen met betrekking tot de significante transactiestromen, reke- ningsaldi en toelichtingen van de entiteit en andere gerelateerde aspecten van de informatie- verwerkingsactiviteiten van de entiteit definiëren. Deze informatie, en de informatie verkregen uit de evaluatie van de accountant van het informatiesysteem, kan de verwachtingen van de accountant over de significante transactiestromen, rekeningsaldi en toelichtingen die aanvan- kelijk zijn geïdentificeerd, bevestigen of verder beïnvloeden (Zie Par. A126). A128 Om inzicht te verwerven in hoe informatie met betrekking tot significante transactiestromen, rekeningsaldi en toelichtingen in, door en uit het informatiesysteem van de entiteit stroomt, kan de accountant ook interne beheersingsmaatregelen in de component 'interne beheersingsacti- viteiten' identificeren die moeten worden geïdentificeerd in overeenstemming met paragraaf 26 (a). De identificatie en evaluatie van interne beheersingsmaatregelen door de accountant in de component 'interne beheersingsactiviteiten' kan zich eerst richten op interne beheersingsmaat- regelen op journaalboekingen en interne beheersingsmaatregelen waarvan de accountant van plan is om de effectieve werking te toetsen bij het opzetten van de aard, timing en omvang van gegevensgerichte werkzaamheden. A129 De inschatting door de accountant van inherent risico kan ook het onderkennen van interne be- heersingsmaatregelen in de component 'interne beheersingsactiviteiten' beïnvloeden. De iden- tificatie van interne beheersingsmaatregelen door de accountant met betrekking tot significante

Furthermore, controls addressing risks for which the auditor has determined that substantive procedures alone do not provide sufficient appropriate audit evidence (in accordance with paragraph 33) may also only be identifiable once the auditor's inherent risk assessments have been undertaken. A130. The auditor's identification and assessment of risks of material misstatement at the assertion level is influenced by both the auditor's: • Understanding of the entity's policies for its information processing activities in the information system and communication component, and • Identification and evaluation of controls in the control activities component. Obtaining an understanding of the information system and communication (Ref: Para. 25) Scalability A131. The information system, and related business processes, in less complex entities are likely to be less sophisticated than in larger entities, and are likely to involve a less complex IT environment; however, the role of the information system is just as important. Less complex entities with direct management involvement may not need extensive descriptions of accounting procedures, sophisticated accounting records, or written policies. Understanding the relevant aspects of the entity's information system may therefore require less effort in an audit of a less complex entity, and may involve a greater amount of inquiry than observation or inspection of documentation. The need to obtain an understanding, however, remains important to provide a basis for the design of further audit procedures in accordance with ISA 330 and may further assist the auditor in identifying or assessing risks of material misstatement (see paragraph A86). Obtaining an understanding of the information system (Ref: Para. 25(a)) A132. Included within the entity's system of internal control are aspects that relate to the entity's reporting objectives, including its financial reporting objectives, but may also include aspects that relate to its operations or compliance objectives, when such aspects are relevant to financial reporting. Understanding how the entity initiates transactions and captures information as part of the auditor's understanding of the information system may include information about the entity's systems (its policies) designed to address compliance and operations objectives because such information is relevant to the preparation of the financial statements. Further, some entities may have information systems that are highly integrated such that controls may be designed in a manner to simultaneously achieve financial reporting, compliance and operational objectives, and combinations thereof. A133. Understanding the entity's information system also includes an understanding of the resources to be used in the entity's information processing activities. Information about the human resources involved that may be relevant to understanding risks to the integrity of the information system include:	risico's kan bijvoorbeeld alleen te onderkennen zijn wanneer de accountant het inherente risico op het niveau van beweringen heeft ingeschat in overeenstemming met paragraaf 31. Boven- dien kunnen interne beheersingsmaatregelen die inspelen op risico's waarvoor de accountant heeft vastgesteld dat gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie verschaffen, (in overeenstemming met paragraaf 33), ook pas te onderken- nen zijn als de inschattingen van het inherente risico door de accountant zijn uitgevoerd. A130 De identificatie en inschatting door de accountant van risico's op een afwijking van materieel belang op het niveau van beweringen wordt beïnvloed door zowel: • inzicht van de accountant in de beleidslijnen van de entiteit voor de informatieverwerkings- activiteiten in de component 'informatiesysteem- en communicatie'; en • identificatie en evaluatie van de accountant van interne beheersingsmaatregelen in de component 'interne beheersingsactiviteiten'. Inzicht verwerven in het informatiesysteem en de communicatie (Zie Par. 25) Schaalbaarheid A131 Het informatiesysteem en gerelateerde bedrijfsprocessen in minder complexe entiteiten zullen waarschijnlijk minder geavanceerd zijn dan in grotere entiteiten, en zal waarschijnlijk een min- der complexe IT-omgeving met zich meebrengen; echter, de rol van het informatiesysteem is net zo belangrijk. Minder complexe entiteiten met een directe betrokkenheid van het manage- ment hebben mogelijk geen behoefte aan uitgebreide beschrijvingen van administratieve ver- werkingsprocedures, geavanceerde administratieve vastleggingen of uitgeschreven beleidslij- nen. Inzicht in de relevante aspecten van het informatiesysteem van de entiteit kan daarom minder inspanning vergen bij een controle van een minder complexe entiteit en kan een groter aantal verzoeken om inlichtingen dan waarneming of inspectie van documentatie inhouden. De noodzaak om inzicht te verwerven blijft echter belangrijk om een basis te vormen voor de opzet van verdere controlewerkzaamheden in overeenstemming met Standaard 330 en kan de ac- countant verder helpen bij het identificeren of inschatten van risico's op een afwijking van ma- terieel belang. (Zie Par. A86) Inzicht verwerven in het informatiesysteem (Zie Par. 25(a)) A132 In het interne beheersingssysteem van de entiteit zijn aspecten opgenomen die betrekking hebben op de verslaggevingsdoelstellingen van de entiteit, inclusief de financiële verslagge- vingsdoelstellingen, maar kunnen ook aspecten omvatten die betrekking hebben op de doel- stellingen op het gebied van de activiteiten of de naleving van wet- en regelgeving, wanneer dergelijke aspecten relevant zijn voor financiële verslaggeving. Inzicht in hoe de entiteit trans- acties initieert en informatie vastlegt als onderdeel van het inzicht van de accountant in het in- formatiesysteem kan informatie omvatten over de systemen van de entiteit (de beleidslijnen) die zijn opgezet om nalevings- en operationele doelstellingen te bereiken, omdat dergelijke in- formatie relevant is voor het opstellen van de financiële overzichten. Verder kunnen sommige entiteiten informatie systemen hebben die in hoge mate geïntegreerd zijn zodat interne beheer- singsmaatregelen op een manier kunnen worden opgezet om tegelijkertijd financiële verslag- gevings-, compliance- en operationele doelstellingen en combinaties daarvan te bereiken. A133 Inzicht in het informatiesysteem van de entiteit omvat ook inzicht in de middelen die worden gebruikt bij de informatieverwerkingsactiviteiten van de entiteit. Informatie over de betrokken

• The competence of the individuals undertaking the work; • Whether there are adequate resources; and • Whether there is appropriate segregation of duties. A134. Matters the auditor may consider when understanding the policies that define the flows of information relating to the entity's significant classes of transactions, account balances, and disclosures in the information system and communication component include the nature of: (a) The data or information relating to transactions, other events and conditions to be processed; (b) The information processing to maintain the integrity of that data or information; and (c) The information processes, personnel and other resources used in the information processing process. A135. Obtaining an understanding of the entity's business processes, which include how transactions are originated, assists the auditor in obtaining an understanding of the entity's information system in a manner that is appropriate to the entity's circumstances. A136. The auditor's understanding of the information system may be obtained in various ways and may include: • Inquiries of relevant personnel about the procedures used to initiate, record, process and report transactions or about the entity's financial reporting process; • Inspection of policy or process manuals or other documentation of the entity's information system; • Observation of the performance of the policies or procedures by entity's personnel; or • Selecting transactions and tracing them through the applicable process in the information system (i.e., performing a walk-through). Automated tools and techniques A137. The auditor may also use automated techniques to obtain direct access to, or a digital download from, the databases in the entity's information system that store accounting records of transactions. By applying automated tools or techniques to this information, the auditor may confirm the understanding obtained about how transactions flow through the information system by tracing journal entries, or other digital records related to a particular transaction, or an entire population of transactions, from initiation in the accounting records through to recording in the general ledger. Analysis of complete or large sets of transactions may also result in the identification of variations from the normal, or expected, processing procedures for these transactions, which may result in the identification of risks of material misstatement. Information obtained from outside of the general and subsidiary ledgers A138. Financial statements may contain information that is obtained from outside of the general and subsidiary ledgers. Examples of such information that the auditor may consider include: • Information obtained from lease agreements relevant to disclosures in the financial statements. • Information disclosed in the financial statements that is produced by an entity's risk management system. • Fair value information produced by management's experts and disclosed in the financial statements.	personele inzet die relevant kan zijn voor het verwerven van inzicht in risico's voor de integriteit van het informatiesysteem zijn onder meer: • de competentie van de personen die het werk uitvoeren; • of er voldoende middelen zijn; en • of er sprake is van een passende functiescheiding. A134 Aangelegenheden die de accountant kan overwegen bij het verwerven van inzicht in de be- leidslijnen die de informatiestromen definiëren met betrekking tot de significante transactiestro- men, rekeningsaldi en toelichtingen van de entiteit in de component 'informatiesysteem en communicatie' omvatten de aard van: a De gegevens of informatie met betrekking tot te verwerken transacties, andere gebeurte- nissen en omstandigheden; b De informatieverwerking om de integriteit van die gegevens of informatie te handhaven; en c De informatieprocessen, personeel en andere middelen die bij het informatieverwerkings- proces worden gebruikt. A135 Verwerven van inzicht in de bedrijfsprocessen van de entiteit, waaronder hoe transacties zijn ontstaan, helpt de accountant bij het verwerven van inzicht in het informatiesysteem van de en- titeit op een manier die geschikt is voor de omstandigheden van de entiteit. A136 Het inzicht van de accountant in het informatiesysteem kan op verschillende manieren worden verkregen en kan omvatten: • verzoeken om inlichtingen bij relevant personeel over de procedures die worden gebruikt voor het initiëren, vastleggen, verwerken en rapporteren van transacties of over het financi- ele verslaggevingsproces van de entiteit; • inspectie van beleidslijnen of proceshandboeken of andere documentatie van het informa- tiesysteem van de entiteit; • waarneming van de uitvoering van de beleidslijnen of de procedures door het personeel van de entiteit; of • transacties selecteren en traceren via het van toepassing zijnde proces in het informatie- systeem (d.w.z. een lijncontrole uitvoeren). Geautomatiseerde hulpmiddelen en technieken A137 De accountant kan ook geautomatiseerde technieken gebruiken om directe toegang tot of een digitale download te verkrijgen van de databases in het informatiesysteem van de entiteit die administratieve vastleggingen van transacties opslaan. Door geautomatiseerde hulpmiddelen of technieken op deze informatie toe te passen, kan de accountant het verkregen inzicht be- vestigen over hoe transacties door het informatiesysteem stromen door journaalboekingen of andere digitale vastleggingen met betrekking tot een bepaalde transactie of een volledige po- pulatie van transacties, te traceren van initiatie in de administratieve vastleggingen tot opname in het grootboek. Analyse van complete of grote sets transacties kan ook leiden tot het identifi- ceren van variaties van de normale of verwachte verwerkingsprocedures voor deze transac- ties, die kunnen leiden tot de identificatie van risico's op een afwijking van materieel belang. Informatie verkregen buiten het grootboek en subgrootboeken A138 Financiële overzichten kunnen informatie bevatten die is verkregen buiten het grootboek en subgrootboeken. Voorbeelden van dergelijke informatie die de accountant kan overwegen om- vatten:

• Information disclosed in the financial statements that has been obtained from models, or from other calculations used to develop accounting estimates recognized or disclosed in the financial statements, including information relating to the underlying data and assumptions used in those models, such as: o Assumptions developed internally that may affect an asset's useful life; or o Data such as interest rates that are affected by factors outside the control of the entity. • Information disclosed in the financial statements about sensitivity analyses derived from financial models that demonstrates that management has considered alternative assumptions. • Information recognized or disclosed in the financial statements that has been obtained from an entity's tax returns and records. • Information disclosed in the financial statements that has been obtained from analyses prepared to support management's assessment of the entity's ability to continue as a going concern, such as disclosures, if any, related to events or conditions that have been identified that may cast significant doubt on the entity's ability to continue as a going concern.38 A139. Certain amounts or disclosures in the entity's financial statements (such as disclosures about credit risk, liquidity risk, and market risk) may be based on information obtained from the entity's risk management system. However, the auditor is not required to understand all aspects of the risk management system, and uses professional judgment in determining the necessary understanding.	• Informatie verkregen uit leaseovereenkomsten die relevant zijn voor toelichtingen in de financiële overzichten; • Informatie toegelicht in de financiële overzichten die wordt gegenereerd door het risicomanagementsysteem van een entiteit; • Informatie over reële waarde die door deskundigen ingeschakeld door het management is opgesteld en toegelicht in de financiële overzichten; • Informatie toegelicht in de financiële overzichten die is verkregen uit modellen of uit andere berekeningen die gebruikt zijn om schattingen te ontwikkelen die zijn opgenomen of toege- licht worden in de financiële overzichten, inclusief informatie met betrekking tot de onderlig- gende gegevens en veronderstellingen die gebruikt zijn in die modellen, zoals: o intern ontwikkelde veronderstellingen die de gebruiksduur van een actief kunnen beïnvloeden; of o gegevens zoals rentevoeten die worden beïnvloed door factoren waarop de entiteit geen invloed heeft. • Informatie toegelicht in de financiële overzichten over gevoeligheidsanalyses afgeleid van financiële modellen die aantoont dat het management alternatieve veronderstellingen heeft overwogen; • Informatie opgenomen of toegelicht in de financiële overzichten die is verkregen uit de belastingaangiften en vastleggingen van de entiteit; • Informatie toegelicht in de financiële overzichten die is verkregen uit analyses die zijn opgesteld om de beoordeling van het management van de mogelijkheid van de entiteit om de continuïteit te handhaven te ondersteunen, zoals eventuele toelichtingen met betrekking tot gebeurtenissen of omstandigheden die zijn geïdentificeerd die gerede twijfel kunnen doen ontstaan over de mogelijkheid van de entiteit om de continuïteit te handhaven.39 A139 Bepaalde bedragen of toelichtingen in de financiële overzichten van de entiteit (zoals toelichtingen over kredietrisico, liquiditeitsrisico en marktrisico) kunnen gebaseerd zijn op informatie verkregen uit het risicomanagementsysteem van de entiteit. De accountant hoeft echter geen in- zicht te verwerven in alle aspecten van het risicomanagementsysteem, en past professionele oordeelsvorming toe bij het bepalen van het benodigde inzicht.
The entity's use of information technology in the information system Why does the auditor understand the IT environment relevant to the information system A140. The auditor's understanding of the information system includes the IT environment relevant to the flows of transactions and processing of information in the entity's information system because the entity's use of IT applications or other aspects in the IT environment may give rise to risks arising from the use of IT. 38 ISA 570 (Revised), paragraphs 19–20 A141. The understanding of the entity's business model and how it integrates the use of IT may also provide useful context to the nature and extent of IT expected in the information system.	Het gebruik van informatietechnologie door de entiteit in het informatiesysteem Waarom verwerft de accountant inzicht in de IT-omgeving die relevant is voor het informatiesysteem A140 Het inzicht van de accountant in het informatiesysteem omvat de IT-omgeving die relevant is voor de transactiestromen en informatieverwerking in het informatiesysteem van de entiteit om- dat het gebruik van IT-applicaties door de entiteit of andere aspecten in de IT-omgeving aanlei- ding kan geven tot risico's door het gebruik van IT. A141 Het inzicht in het bedrijfsmodel van de entiteit en hoe het gebruik van IT wordt geïntegreerd, kan ook nuttige context bieden voor de aard en omvang van IT die in het informatiesysteem wordt verwacht.
Understanding the entity's use of IT A142. The auditor's understanding of the IT environment may focus on identifying, and understanding the nature and number of, the specific IT applications and other aspects of the IT environment that are relevant to the flows of transactions and processing of information in the information system. Changes in the flow of transactions, or information within the information system may result from program changes to IT applications, or direct changes to data in databases involved in processing, or storing those transactions or information.	Inzicht in het gebruik van IT door de entiteit A142 Het inzicht van de accountant in de IT-omgeving kan gericht zijn op het identificeren en verwerven van inzicht in de aard en het aantal van de specifieke IT-applicaties en andere aspecten van de IT-omgeving die relevant zijn voor de stromen van transacties en informatieverwerking in het informatiesysteem. Veranderingen in de stroom van transacties of informatie binnen het informatiesysteem kunnen het gevolg zijn van programma wijzigingen in IT-applicaties of di- recte wijzigingen in gegevens in databases die betrokken zijn bij de verwerking of opslag van die transacties of informatie.

A143. The auditor may identify the IT applications and supporting IT infrastructure concurrently with the auditor's understanding of how information relating to significant classes of transactions, account balances and disclosures flows into, through and out the entity's information system.	A143 De accountant kan de IT-applicaties en de ondersteunende IT-infrastructuur gelijktijdig identificeren met het inzicht van de accountant in hoe informatie met betrekking tot significante transactiestromen, rekening saldi en toelichtingen in, door en uit het informatiesysteem van de enti- teit stromen.
Obtaining an understanding of the entity's communication (Ref: Para. 25(b)) Scalability A144. In larger, more complex entities, information the auditor may consider when understanding the entity's communication may come from policy manuals and financial reporting manuals. A145. In less complex entities, communication may be less structured (e.g., formal manuals may not be used) due to fewer levels of responsibility and management's greater visibility and availability. Regardless of the size of the entity, open communication channels facilitate the reporting of exceptions and acting on them.	Het verwerven van inzicht in de communicatie van de entiteit (Zie Par. 25(b)) 39 Standaard 570, paragrafen 19–20. Schaalbaarheid A144 In grotere, meer complexe entiteiten, kan informatie die de accountant kan overwegen bij het verwerven van inzicht in de communicatie van de entiteit afkomstig zijn van handboeken over beleidsprocedures en over financiële verslaggeving. A145 In minder complexe entiteiten kan communicatie minder gestructureerd zijn (formele handboeken worden bijvoorbeeld niet gebruikt) vanwege minder verantwoordelijkheidsniveaus en een grotere zichtbaarheid en beschikbaarheid van het management. Ongeacht de grootte van de entiteit vergemakkelijken open communicatiekanalen de rapportage van uitzonderingen en het opvolgen daarvan.
Evaluating whether the relevant aspects of the information system support the preparation of the entity's financial statements (Ref: Para. 25(c)) A146. The auditor's evaluation of whether the entity's information system and communication appropriately supports the preparation of the financial statements is based on the understanding obtained in paragraphs 25(a)–(b).	Evalueren of de relevante aspecten van het informatiesysteem het opstellen van de financiële overzichten van de entiteit ondersteunen (Zie Par. 25(c)) A146 De evaluatie door de accountant of het informatiesysteem en de communicatie van de entiteit de opstelling van de financiële overzichten op passende wijze ondersteunt, is gebaseerd op het inzicht verkregen in paragraaf 25(a)-(b).
Control Activities (Ref: Para. 26) Controls in the control activities component A147. The control activities component includes controls that are designed to ensure the proper application of policies (which are also controls) in all the other components of the entity's system of internal control, and includes both direct and indirect controls.	Interne beheersingsactiviteiten (Zie Par. 26) Interne beheersingsmaatregelen in de component 'interne beheersingsactiviteiten' A147 De component 'interne beheersingsactiviteiten' omvat interne beheersingsmaatregelen die zijn opgezet om te zorgen voor de juiste toepassing van beleidslijnen (die ook interne beheersingsmaatregelen zijn) in alle andere componenten van het interne beheersingssysteem van de enti- teit en omvat zowel directe als indirecte interne beheersingsmaatregelen.
A148. The auditor's identification and evaluation of controls in the control activities component is focused on information processing controls, which are controls applied during the processing of information in the entity's information system that directly address risks to the integrity of information (i.e., the completeness, accuracy and validity of transactions and other information). However, the auditor is not required to identify and evaluate all information processing controls related to the entity's policies that define the flows of transactions and other aspects of the entity's information processing activities for the significant classes of transactions, account balances and disclosures. A149. There may also be direct controls that exist in the control environment, the entity's risk assessment process or the entity's process to monitor the system of internal control, which may be identified in accordance with paragraph 26. However, the more indirect the relationship between controls that support other controls and the control that is being considered, the less effective that control may be in preventing, or detecting and correcting, related misstatements. A150. Paragraph 26 also requires the auditor to identify and evaluate general IT controls for IT applications and other aspects of the IT environment that the auditor has determined to be subject to risks arising from the use of IT, because general IT controls support the continued effective functioning of information processing controls. A general IT control alone is typically not sufficient to address a risk of material misstatement at the assertion level. A151. The controls that the auditor is required to identify and evaluate the design, and determine the implementation of, in accordance with paragraph 26 are those: • Controls which the auditor plans to test the operating effectiveness of in determining the nature, timing and extent of substantive procedures. The evaluation of such controls provides the basis for the auditor's design of test of control procedures in accordance with ISA 330. These controls also include controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence. • Controls include controls that address significant risks and controls over journal entries. The auditor's identification and evaluation of such controls may also influence the auditor's understanding of the risks of	A148 De identificatie en evaluatie van interne beheersingsmaatregelen door de accountant in de component 'interne beheersingsactiviteiten' is gericht op interne beheersingsmaatregelen met betrekking tot informatieverwerking. Dit zijn interne beheersingsmaatregelen die worden toege- past tijdens de verwerking van informatie in het informatiesysteem van de entiteit die direct in- spelen op risico's voor de integriteit van informatie (d.w.z. de volledigheid, nauwkeurigheid en geldigheid van transacties en andere informatie). Van de accountant wordt echter niet vereist om alle interne beheersingsmaatregelen met betrekking tot informatieverwerking met betrek- king tot de beleidslijnen van de entiteit die de transactiestromen en andere aspecten van de informatieverwerkingsactiviteiten van de entiteit definiëren voor de significante transactiestro- men, rekeningsaldi en toelichtingen te identificeren en te evalueren.

material misstatement, including the identification of additional risks of material misstatement (see paragraph A95). This understanding also provides the basis for the auditor's design of the nature, timing and extent of substantive audit procedures that are responsive to the related assessed risks of material misstatement. • Other controls that the auditor considers are appropriate to enable the auditor to meet the objectives of paragraph 13 with respect to risks at the assertion level, based on the auditor's professional judgment. A152. Controls in the control activities component are required to be identified when such controls meet one or more of the criteria included in paragraph 26(a). However, when multiple controls each achieve the same objective, it is unnecessary to identify each of the controls related to such objective.	A149 Er kunnen ook directe interne beheersingsmaatregelen zijn die bestaan in de interne beheer- singsomgeving, het risico-inschattingsproces van de entiteit of het proces van de entiteit om het systeem van interne beheersing te monitoren, die kunnen worden geïdentificeerd in over- eenstemming met paragraaf 26. Hoe indirecter de relatie tussen interne beheersingsmaatrege- len die andere interne beheersingsmaatregelen ondersteunen en de interne beheersingsmaat- regel die worden overwogen echter is, hoe minder effectief die interne beheersingsmaatregel kan zijn bij het voorkomen, of detecteren en corrigeren van gerelateerde afwijkingen. A150 Paragraaf 26 vereist ook dat de accountant general IT controls voor IT-applicaties en andere aspecten van de IT-omgeving identificeert en evalueert, waarvan de accountant heeft vastge- steld dat deze onderhevig zijn aan risico's die voortkomen uit het gebruik van IT, omdat gene- ral IT controls de blijvende effectieve werking van interne beheersingsmaatregelen met betrek- king tot informatieverwerking ondersteunen. Een general IT-control alleen is meestal niet vol- doende om in te spelen op een risico op een afwijking van materieel belang op het niveau van beweringen. A151 De interne beheersingsmaatregelen waarvan de accountant de opzet moet identificeren en evalueren en de implementatie daarvan moet bepalen in overeenstemming met paragraaf 26, zijn: • Interne beheersingsmaatregelen waarvan de accountant van plan is om de effectieve wer- king te toetsen voor het bepalen van de aard, timing en omvang van gegevensgerichte werkzaamheden. De evaluatie van dergelijke interne beheersingsmaatregelen vormt de ba- sis voor de opzet van de accountant van het toetsen van interne beheersingsmaatregelen in overeenstemming met Standaard 330. Deze interne beheersingsmaatregelen omvatten ook interne beheersingsmaatregelen die inspelen op risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie verschaffen; • Interne beheersingsmaatregelen die inspelen op significante risico's en interne beheer- singsmaatregelen met betrekking tot journaalboekingen. De identificatie en evaluatie van dergelijke interne beheersingsmaatregelen door de accountant kunnen ook van invloed zijn op het inzicht van de accountant in de risico's op een afwijking van materieel belang, inclu- sief de identificatie van aanvullende risico's op een afwijking van materieel belang (zie pa- ragraaf A95). Dit inzicht biedt ook de basis voor de opzet van de accountant van de aard, timing en omvang van gegevensgerichte controlewerkzaamheden die inspelen op de gere- lateerde ingeschatte risico's op een afwijking van materieel belang; • Andere interne beheersingsmaatregelen die de accountant overweegt zijn geschikt om de accountant in staat te stellen de doelstellingen van paragraaf 13 met betrekking tot risico's op het niveau van beweringen te bereiken, gebaseerd op de professionele oordeelsvor- ming van de accountant. A152 Interne beheersingsmaatregelen in de component 'interne beheersingsactiviteiten' moeten wor- den geïdentificeerd wanneer dergelijke interne beheersingsmaatregelen voldoen aan een of meer van de criteria in paragraaf 26(a). Wanneer echter meerdere interne beheersingsmaatre- gelen dezelfde doelstelling bereiken, is het niet nodig om elk van de interne beheersingsmaat- regelen met betrekking tot een dergelijke doelstelling te identificeren.
Types of controls in the control activities component (Ref: Para. 26)	Typen interne beheersingsmaatregelen in de component 'interne beheersingsactiviteiten' (Zie Par. 26)

A153. Examples of controls in the control activities component include authorizations and approvals, reconciliations, verifications (such as edit and validation checks or automated calculations), segregation of duties, and physical or logical controls, including those addressing safeguarding of assets.
A154. Controls in the control activities component may also include controls established by management that address risks of material misstatement related to disclosures not being prepared in accordance with the applicable financial reporting framework. Such controls may relate to information included in the financial statements that is obtained from outside of the general and subsidiary ledgers.
A155. Regardless of whether controls are within the IT environment or manual systems, controls may have various objectives and may be applied at various organizational and functional levels.

Scalability (Ref: Para. 26)
A156. Controls in the control activities component for less complex entities are likely to be similar to those in larger entities, but the formality with which they operate may vary. Further, in less complex entities, more controls may be directly applied by management.
A157. It may be less practicable to establish segregation of duties in less complex entities that have fewer employees. However, in an owner-managed entity, the owner-manager may be able to exercise more effective oversight through direct involvement than in a larger entity, which may compensate for the generally more limited opportunities for segregation of duties. Although, as also explained in ISA 240, domination of management by a single individual can be a potential control deficiency since there is an opportunity for management override of controls.39

39 ISA 240, paragraph A28

Controls that address risks of material misstatement at the assertion level (Ref: Para. 26(a)) Controls that address risks that are determined to be a significant risk (Ref: Para. 26(a)(i))
A158. Regardless of whether the auditor plans to test the operating effectiveness of controls that address significant risks, the understanding obtained about management's approach to addressing those risks may provide a basis for the design and performance of substantive procedures responsive to significant risks as required by ISA 330.40 Although risks relating to significant non-routine or judgmental matters are often less likely to be subject to routine controls, management may have other responses intended to deal with such risks. Accordingly, the auditor's understanding of whether the entity has designed and implemented controls for significant risks arising from non-routine or judgmental matters may include whether and how management responds to the risks. Such responses may include:
- Controls, such as a review of assumptions by senior management or experts.
- Documented processes for accounting estimations.
- Approval by those charged with governance.

A153 Voorbeelden van interne beheersingsmaatregelen in de component 'interne beheersingsactivi- teiten' zijn autorisaties en goedkeuringen, aansluitingen, verificaties (zoals bewerkings- en vali- datie controles of geautomatiseerde berekeningen), functiescheiding en fysieke of logische in- terne beheersingsmaatregelen, inclusief die voor de bescherming van activa.

A154 Interne beheersingsmaatregelen in de component 'interne beheersingsactiviteiten' kunnen ook interne beheersingsmaatregelen omvatten die zijn vastgesteld door het management die inspe- len op risico's op een afwijking van materieel belang in verband met toelichtingen die niet in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving zijn opgesteld. Dergelijke interne beheersingsmaatregelen kunnen betrekking hebben op informatie die is opgenomen in de financiële overzichten die is verkregen buiten het grootboek en sub- grootboeken.

A155 Ongeacht of interne beheersingsmaatregelen zich binnen de IT-omgeving of in handmatige systemen bevinden, kunnen interne beheersingsmaatregelen verschillende doelstellingen heb- ben en kunnen ze worden toegepast op verschillende organisatorische en functionele niveaus.

Schaalbaarheid (Zie Par. 26)

A156 Interne beheersingsmaatregelen in de component 'interne beheersingsactiviteiten' voor minder complexe entiteiten zijn waarschijnlijk vergelijkbaar met die in grotere entiteiten, maar de for- maliteit waarmee ze werken kan variëren. Verder kunnen in minder complexe entiteiten meer interne beheersingsmaatregelen direct door het management worden toegepast.

A157 Het kan minder praktisch uitvoerbaar zijn om functiescheiding in minder complexe entiteiten met minder medewerkers tot stand te brengen. In een door de eigenaar bestuurde entiteit kan de eigenaar-bestuurder echter mogelijk meer effectief toezicht uitoefenen door directe betrok- kenheid dan bij een grotere entiteit, wat de over het algemeen beperktere mogelijkheden voor functiescheiding kan compenseren. Hoewel, zoals ook uitgelegd in Standaard 240, overheer- sing van het management door een enkel persoon kan een potentiële tekortkoming in de in- terne beheersing zijn, omdat er een mogelijkheid is voor het management om de interne be- heersing te doorbreken.40

Interne beheersingsmaatregelen die inspelen op de risico's op een afwijking van materieel belang op het niveau van beweringen (Zie Par. 26(a))

Interne beheersingsmaatregelen die inspelen op risico's waarvan is bepaald dat ze een significant risico zijn (Zie Par. 26(a)(i))

A158 Ongeacht of de accountant van plan is om de effectieve werking van interne beheersingsmaat- regelen te toetsen die inspelen op significante risico's, kan het verkregen inzicht over de aan- pak van het management om in te spelen op deze risico's een basis vormen voor de opzet en de uitvoering van gegevensgerichte werkzaamheden die inspelen op significante risico's zoals vereist door Standaard 330.41 Hoewel risico's met betrekking tot significante niet-routinematige of oordeelsvormende aangelegenheden waarschijnlijk vaak minder onderworpen zijn aan routi- nematige interne beheersingsmaatregelen, is het mogelijk dat het management op een andere manier op dergelijke risico's inspeelt. Dienovereenkomstig kan het inzicht van de accountant of de entiteit interne beheersingsmaatregelen heeft opgezet en geïmplementeerd voor signifi- cante risico's die voortkomen uit niet-routinematige of oordeelsvormende aangelegenheden omvatten of en hoe het management inspeelt op de risico's. De manieren om op risico's in te spelen kunnen omvatten:
- interne beheersingsmaatregelen, zoals een beoordeling van veronderstellingen door het senior management of deskundigen;

	• gedocumenteerde processen voor schattingen; • goedkeuring door de met governance belaste personen.
A159. ISA 24041 requires the auditor to understand controls related to assessed risks of material misstatement due to fraud (which are treated as significant risks), and further explains that it is important for the auditor to obtain an understanding of the controls that management has designed, implemented and maintained to prevent and detect fraud. Controls over journal entries (Ref: Para. 26(a)(ii)) A160. Controls that address risks of material misstatement at the assertion level that are expected to be identified for all audits are controls over journal entries, because the manner in which an entity incorporates information from transaction processing into the general ledger ordinarily involves the use of journal entries, whether standard or non-standard, or automated or manual. The extent to which other controls are identified may vary based on the nature of the entity and the auditor's planned approach to further audit procedures.	A159 Standaard 24042 vereist dat de accountant inzicht verwerft in de interne beheersingsmaatrege- len met betrekking tot ingeschatte risico's op een afwijking van materieel belang als gevolg van fraude (die worden behandeld als significante risico's), en legt verder uit dat het belangrijk is voor de accountant om inzicht te verwerven in de interne beheersingsmaatregelen die het ma- nagement heeft opgezet, geïmplementeerd en onderhouden om fraude te voorkomen en te de- tecteren. Interne beheersingsmaatregelen met betrekking tot journaalboekingen (Zie Par. 26(a)(ii)) A160 Interne beheersingsmaatregelen die inspelen op de risico's op een afwijking van materieel be- lang op het beweringenniveau die naar verwachting voor alle controles worden geïdentificeerd, zijn interne beheersingsmaatregelen met betrekking tot journaalboekingen. De manier waarop een entiteit informatie van transactieverwerking opneemt in het grootboek omvat normaal ge- sproken het gebruik van journaalboekingen, hetzij standaard of niet-standaard, of geautomati- seerd of handmatig. De mate waarin andere interne beheersingsmaatregelen worden geïdenti- ficeerd, kan variëren op basis van de aard van de entiteit en de geplande aanpak van de ac- countant van verdere controlewerkzaamheden.
40 ISA 330, paragraph 21 41 ISA 240, paragraphs 28 and A33	40 Standaard 240, paragraaf A28. 41 Standaard 330, paragraaf 21. 42 Standaard 240, punten 28 en A33.
Automated tools and techniques A161. In manual general ledger systems, non-standard journal entries may be identified through inspection of ledgers, journals, and supporting documentation. When automated procedures are used to maintain the general ledger and prepare financial statements, such entries may exist only in electronic form and may therefore be more easily identified through the use of automated techniques.	Geautomatiseerde hulpmiddelen en technieken A161 Bij handmatige grootboeksystemen kunnen niet-standaard journaalboekingen mogelijk worden geïdentificeerd door inspectie van grootboeken, dagboeken en ondersteunende documentatie. Wanneer geautomatiseerde procedures worden gebruikt voor het bijhouden van het grootboek en het opstellen van financiële overzichten, is het mogelijk dat dergelijke boekingen alleen in elektronische vorm bestaan waardoor ze gemakkelijker zijn te identificeren door het gebruik van geautomatiseerde technieken.
Controls for which the auditor plans to test the operating effectiveness (Ref: Para. 26(a)(iii)) A162. The auditor determines whether there are any risks of material misstatement at the assertion level for which it is not possible to obtain sufficient appropriate audit evidence through substantive procedures alone. The auditor is required, in accordance with ISA 330,42 to design and perform tests of controls that address such risks of material misstatement when substantive procedures alone do not provide sufficient appropriate audit evidence at the assertion level. As a result, when such controls exist that address these risks, they are required to be identified and evaluated.	Interne beheersingsmaatregelen waarvoor de accountant van plan is de effectieve werking te toetsen (Zie Par. 26(a)(iii)) A162 De accountant bepaalt of er risico's op een afwijking van materieel belang op het niveau van beweringen bestaan waarvoor het niet mogelijk is om voldoende en geschikte controle-infor- matie te verkrijgen door gegevensgerichte werkzaamheden alleen. Van de accountant wordt vereist, in overeenstemming met Standaard 330,43, om toetsingen van interne beheersings- maatregelen op te zetten en uit te voeren die inspelen op dergelijke risico's op een afwijking van materieel belang wanneer gegevensgerichte werkzaamheden alleen niet voldoende en ge- schikte controle-informatie verschaffen op het niveau van beweringen. Als gevolg hiervan moe- ten, wanneer dergelijke interne beheersingsmaatregelen bestaan die inspelen op deze risico's, deze worden geïdentificeerd en geëvalueerd.

A163. In other cases, when the auditor plans to take into account the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures in accordance with ISA 330, such controls are also required to be identified because ISA 33043 requires the auditor to design and perform tests of those controls.	A163 In andere gevallen, wanneer de accountant van plan is rekening te houden met de effectieve werking van interne beheersingsmaatregelen bij het bepalen van de aard, timing en omvang van gegevensgerichte werkzaamheden in overeenstemming met Standaard 330, moeten der- gelijke interne beheersingsmaatregelen ook worden geïdentificeerd omdat Standaard 33044 vereist dat de accountant toetsingen van die interne beheersingsmaatregelen opzet en uitvoert.
42 ISA 330, paragraph 8(b) 43 ISA 330, paragraph 8(a)	43 Standaard 330, paragraaf 8(b). 44 Standaard 330, paragraaf 8(a).
A164. The auditor's plans to test the operating effectiveness of controls may also be influenced by the identified risks of material misstatement at the financial statement level. For example, if deficiencies are identified related to the control environment, this may affect the auditor's overall expectations about the operating effectiveness of direct controls.	A164 De plannen van de accountant om de effectieve werking van interne beheersingsmaatregelen te toetsen kunnen ook worden beïnvloed door de geïdentificeerde risico's op een afwijking van materieel belang op het niveau van de financiële overzichten. Bijvoorbeeld als tekortkomingen zijn geïdentificeerd met betrekking tot de interne beheersingsomgeving, kan dit de algemene verwachtingen van de accountant met betrekking tot de effectieve werking van directe interne beheersingsmaatregelen beïnvloeden.
Other controls that the auditor considers appropriate (Ref: Para. 26(a)(iv)) A165. Other controls that the auditor may consider are appropriate to identify, and evaluate the design and determine the implementation, may include: • Controls that address risks assessed as higher on the spectrum of inherent risk but have not been determined to be a significant risk; • Controls related to reconciling detailed records to the general ledger; or • Complementary user entity controls, if using a service organization.44	Andere interne beheersingsmaatregelen die de accountant geschikt acht (Zie Par. 26 (a) (iv)) A165 Andere interne beheersingsmaatregelen die de accountant kan overwegen die geschikt zijn om de opzet te identificeren en te evalueren en om de implementatie te bepalen, kunnen omvat- ten: • interne beheersingsmaatregelen die inspelen op risico's die als hoger worden ingeschat in het spectrum van inherent risico maar die niet als significant risico bepaald zijn; • interne beheersingsmaatregelen met betrekking tot het aansluiten van gedetailleerde vast-leggingen met het grootboek; of • aanvullende interne beheersingsmaatregelen van de gebruikersorganisatie bij gebruik van een serviceorganisatie.45
Identifying IT applications and other aspects of the IT environment, risks arising from the use of IT and general IT controls (Ref: Para. 26(b)–(c)) Identifying IT applications and other aspects of the IT environment (Ref: Para. 26(b)) Why the auditor identifies risks arising from the use of IT and general IT controls related to identified IT applications and other aspects of the IT environment	Identificatie van IT-applicaties en andere aspecten van de IT-omgeving, risico's die voortkomen uit het gebruik van IT en general IT controls (Zie Par. 26(b)-(c)) Het identificeren van IT-applicaties en andere aspecten van de IT-omgeving (Zie Par. 26(b)) Waarom de accountant risico's identificeert die voortkomen uit het gebruik van IT en general IT con-trols met betrekking tot geïdentificeerde IT-applicaties en andere aspecten van de IT-omgeving
A166. Understanding the risks arising from the use of IT and the general IT controls implemented by the entity to address those risks may affect: • The auditor's decision about whether to test the operating effectiveness of controls to address risks of material misstatement at the assertion level; • The auditor's assessment of control risk at the assertion level; • The auditor's strategy for testing information produced by the entity that is produced by or involves information from the entity's IT applications; • The auditor's assessment of inherent risk at the assertion level; or	A166 Inzicht in de risico's die voortkomen uit het gebruik van IT en de general IT controls die door de entiteit zijn geïmplementeerd om in te spelen op deze risico's[A43], kan van invloed zijn op: • De beslissing van de accountant over het al dan niet toetsen van de effectieve werking van de interne beheersingsmaatregelen die inspelen op risico's op een afwijking van materieel belang op het niveau van beweringen; • De inschatting door de accountant van het interne beheersingsrisico op het niveau van be-weringen; • De strategie van de accountant voor het toetsen van informatie afkomstig van de entiteit die wordt gegenereerd door of betreft informatie ~~betreft~~ uit de IT-applicaties van de entiteit; • De inschatting door de accountant van inherent risico op het niveau van beweringen;

• The design of further audit procedures.	• De opzet van verdere controlewerkzaamheden.
Identifying IT applications that are subject to risks arising from the use of IT	Het identificeren van IT-applicaties die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT
A167. For the IT applications relevant to the information system, understanding the nature and complexity of the specific IT processes and general IT controls that the entity has in place may assist the auditor in determining which IT applications the entity is relying upon to accurately process and maintain the integrity of information in the entity's information system. Such IT applications may be subject to risks arising from the use of IT.	A167 Voor de IT-applicaties die relevant zijn voor het informatiesysteem, kan inzicht in de aard en complexiteit van de specifieke IT-processen en general IT controls die de entiteit heeft[A44], de accountant helpen bij het bepalen op welke IT-applicaties de entiteit steunt om de integriteit van informatie in het informatiesysteem van de entiteit nauwkeurig te verwerken en onderhouden.[A45] Dergelijke IT-applicaties kunnen onderhevig zijn aan risico's die voortkomen uit het gebruik van IT.
A168. Identifying the IT applications that are subject to risks arising from the use of IT involves taking into account controls identified by the auditor because such controls may involve the use of IT or rely on IT. The auditor may focus on whether an IT application includes automated controls that management is relying on and that the auditor has identified, including controls that address risks for which substantive procedures alone do not provide sufficient appropriate audit evidence. The auditor may also consider how information is stored and processed in the information system relating to significant classes of transactions, account balances and disclosures and whether management is relying on general IT controls to maintain the integrity of that information.	A168 Bij het identificeren van de IT-applicaties die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT, moet rekening worden gehouden met interne beheersingsmaatregelen die door de accountant zijn geïdentificeerd omdat dergelijke controlemaatregelen [A46]het gebruik van IT of het steunen op IT kunnen inhouden. De accountant kan zich concentreren op de vraag of een IT-applicatie geautomatiseerde interne beheersingsmaatregelen bevat waarop het manage- ment steunt en die de accountant heeft geïdentificeerd, inclusief interne beheersingsmaatrege- len die inspelen op risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie verschaffen. De accountant kan ook overwegen hoe informa- tie wordt opgeslagen en verwerkt in het informatiesysteem met betrekking tot significante trans- actiestromen, rekeningsaldi en toelichtingen en of het management steunt op general IT con- trols om de integriteit van die informatie te handhaven[A47].
A169. The controls identified by the auditor may depend on system-generated reports, in which case the IT applications that produce those reports may be subject to risks arising from the use of IT. In other cases, the auditor may not plan to rely on controls over the system-generated reports and plan to directly test the inputs and outputs of such reports, in which case the auditor may not identify the related IT applications as being subject to risks arising from IT.	A169 De door de accountant geïdentificeerde interne beheersingsmaatregelen kunnen afhankelijk zijn van door het systeem gegenereerde rapporten, in welk geval de IT-applicaties die deze rapporten genereren onderhevig kunnen zijn aan risico's die voortkomen uit het gebruik van IT. In andere gevallen is het mogelijk dat de accountant niet van plan is om te steunen op interne beheersingsmaatregelen met betrekking tot de door het systeem gegenereerde rapporten en van plan is om direct de inputs en outputs [A48]van dergelijke rapporten te toetsen, in welk geval de accountant mogelijk niet de gerelateerde IT-applicaties identificeert als onderhevig aan risico's die voortkomen uit IT.
Scalability	Schaalbaarheid
A170. The extent of the auditor's understanding of the IT processes, including the extent to which the entity has general IT controls in place, will vary with the nature and the circumstances of the entity and its IT environment, as well as based on the nature and extent of controls identified by the auditor. The number of IT applications that are subject to risks arising from the use of IT also will vary based on these factors.	A170 De mate van inzicht van de accountant in de IT-processen, inclusief de mate waarin de entiteit beschikt over general IT controls, zal variëren met de aard en de omstandigheden van de enti- teit en de [A49]IT-omgeving, evenals op basis van de aard en omvang van de interne beheersings- maatregelen die door de accountant zijn geïdentificeerd. Het aantal IT-applicaties dat onderhe- vig is aan risico's die voortkomen uit het gebruik van IT zal ook variëren op basis van deze fac- toren.
Examples: • An entity that uses commercial software and does not have access to the source code to make any program changes is unlikely to have a process for program changes, but may have a process or procedures to configure the software (e.g., the chart of accounts, reporting parameters or thresholds). In addition, the entity may have a process or procedures to manage access to the application (e.g., a designated individual with administrative access to the commercial software). In such circumstances, the entity is unlikely to have or need formalized general IT controls. • In contrast, a larger entity may rely on IT to a great extent and the IT environment may involve multiple IT applications and the IT processes to manage the IT environment may be complex (e.g., a dedicated IT department	

exists that develops and implements program changes and manages access rights), including that the entity has implemented formalized general IT controls over its IT processes. • When management is not relying on automated controls or general IT controls to process transactions or maintain the data, and the auditor has not identified any automated controls or other information processing controls (or any that depend on general IT controls), the auditor may plan to directly test any information produced by the entity involving IT and may not identify any IT applications that are subject to risks arising from the use of IT. • When management relies on an IT application to process or maintain data and the volume of data is significant, and management relies upon the IT application to perform automated controls that the auditor has also identified, the IT application is likely to be subject to risks arising from the use of IT.	
A171. When an entity has greater complexity in its IT environment, identifying the IT applications and other aspects of the IT environment, determining the related risks arising from the use of IT, and identifying general IT controls is likely to require the involvement of team members with specialized skills in IT. Such involvement is likely to be essential, and may need to be extensive, for complex IT environments.	A171 Wanneer een entiteit een grotere complexiteit in de IT-omgeving heeft, vereist het identificeren van de IT-applicaties en andere aspecten van de IT-omgeving, het bepalen van de gerela- teerde risico's die voortkomen uit het gebruik van IT en het identificeren van general IT-controls waarschijnlijk de betrokkenheid van teamleden met gespecialiseerde IT-vaardigheden. Een dergelijke betrokkenheid is waarschijnlijk essentieel en moet mogelijk uitgebreid zijn voor com- plexe IT-omgevingen.
Identifying other aspects of the IT environment that are subject to risks arising from the use of IT	Identificeren van andere aspecten van de IT-omgeving die onderhevig zijn aan risico's die voortko- men uit het gebruik van IT
A172. The other aspects of the IT environment that may be subject to risks arising from the use of IT include the network, operating system and databases, and, in certain circumstances, interfaces between IT applications. Other aspects of the IT environment are generally not identified when the auditor does not identify IT applications that are subject to risks arising from the use of IT. When the auditor has identified IT applications that are subject to risks arising from IT, other aspects of the IT environment (e.g., database, operating system, network) are likely to be identified because such aspects support and interact with the identified IT applications.	A172 De andere aspecten van de IT-omgeving die onderhevig kunnen zijn aan risico's die voortko- men uit het gebruik van IT, omvatten het netwerk, besturingssysteem en databases en, in be- paalde omstandigheden, interfaces tussen IT-applicaties. Andere aspecten van de IT- omgeving worden over het algemeen niet geïdentificeerd wanneer de accountant geen IT- applicaties identificeert die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT. Wanneer de accountant IT-applicaties heeft geïdentificeerd die onderhevig zijn aan risico's die voortkomen uit IT, worden andere aspecten van de IT-omgeving (bijvoorbeeld database, bestu- ringssysteem, netwerk) waarschijnlijk geïdentificeerd omdat dergelijke aspecten de geïdentifi- ceerde IT-applicaties ondersteunen en daarmee interactie hebben.
Identifying risks arising from the use of IT and general IT controls (Ref: Para. 26(c))	Identificeren van risico's die voortkomen uit het gebruik van IT en general IT controls (Zie Par. 26(c)) Bijlage 6 bevat overwegingen voor het verwerven van inzicht in general IT controls.
A173. In identifying the risks arising from the use of IT, the auditor may consider the nature of the identified IT application or other aspect of the IT environment and the reasons for it being subject to risks arising from the use of IT. For some identified IT applications or other aspects of the IT environment, the auditor may identify applicable risks arising from the use of IT that relate primarily to unauthorized access or unauthorized program changes, as well as that address risks related to inappropriate data changes (e.g., the risk of inappropriate changes to the data through direct database access or the ability to directly manipulate information).	A173 Bij het identificeren van de risico's die voortkomen uit het gebruik van IT, kan de accountant rekening houden met de aard van de geïdentificeerde IT-applicatie of een ander aspect van de IT-omgeving en de redenen waarom risico's kunnen ontstaan uit het gebruik van IT. Voor som- mige geïdentificeerde IT-applicaties of andere aspecten van de IT-omgeving, kan de accoun- tant van toepassing zijnde risico's identificeren die voortkomen uit het gebruik van IT en die voornamelijk betrekking hebben op niet-geautoriseerde toegang of ongeautoriseerde program- mawijzigingen, evenals risico's die verband houden met ongepaste gegevenswijzigingen (bij- voorbeeld het risico op ongepaste wijzigingen in de gegevens door directe databasetoegang of de mogelijkheid om informatie rechtstreeks te manipuleren).
A174. The extent and nature of the applicable risks arising from the use of IT vary depending on the nature and characteristics of the identified IT applications and other aspects of the IT environment. Applicable IT risks may result when the entity uses external or internal service providers for identified aspects of its IT environment (e.g., outsourcing the hosting of its IT environment to a third party or using a shared service center for central management of IT processes in a group). Applicable risks arising from the use of IT may also be identified related to cybersecurity. It is more likely that there will be more risks arising from the use of IT when the volume or complexity of automated application controls is higher and management is placing greater reliance on those	A174 De omvang en aard van de van toepassing zijnde risico's die voortkomen uit het gebruik van IT variëren afhankelijk van de aard en kenmerken van de geïdentificeerde IT-applicaties en an- dere aspecten van de IT-omgeving. Van toepassing zijnde IT-risico's kunnen ontstaan wanneer de entiteit voor geïdentificeerde aspecten van de IT-omgeving (bijvoorbeeld het uitbesteden van de hosting van de IT-omgeving aan een derde of het gebruikmaken van een shared ser- vice center voor centraal beheer van IT-processen in een groep) externe of interne dienstverle- ners gebruikt. Van toepassing zijnde risico's die voortkomen uit het gebruik van IT kunnen ook worden geïdentificeerd met

controls for effective processing of transactions or the effective maintenance of the integrity of underlying information.	betrekking tot cybersecurity. Het is waarschijnlijker dat er meer ri- sico's zullen voortkomen uit het gebruik van IT wanneer de hoeveelheid of de complexiteit van geautomatiseerde application controls hoger is en het management meer steunt op deze in- terne beheersingsmaatregelen voor de effectieve verwerking van transacties of het effectieve onderhoud van de integriteit van onderliggende informatie.
Evaluating the design, and determining implementation, of identified controls in the control activities component (Ref: Para 26(d))	Evalueren van de opzet en het bepalen van de implementatie van geïdentificeerde interne beheer- singsmaatregelen met betrekking tot de component 'interne beheersingsactiviteiten'. (Zie Par. 26(d))
A175. Evaluating the design of an identified control involves the auditor's consideration of whether the control, individually or in combination with other controls, is capable of effectively preventing, or detecting and correcting, material misstatements (i.e., the control objective).	A175 Bij het evalueren van de opzet van een geïdentificeerde interne beheersingsmaatregel omvat de overweging van de accountant of de interne beheersingsmaatregel, afzonderlijk of in combi- natie met andere interne beheersingsmaatregelen, in staat is om effectief afwijkingen van ma- terieel belang te voorkomen of te detecteren en te corrigeren van (d.w.z. de interne beheer- singsdoelstelling).
A176. The auditor determines the implementation of an identified control by establishing that the control exists and that the entity is using it. There is little point in the auditor assessing the implementation of a control that is not designed effectively. Therefore, the auditor evaluates the design of a control first. An improperly designed control may represent a control deficiency.	A176 De accountant bepaalt de implementatie van een geïdentificeerde interne beheersingsmaatre- gel door vast te stellen dat de interne beheersingsmaatregel bestaat en dat de entiteit deze toepast. Het heeft weinig zin dat de accountant de implementatie beoordeelt van een interne beheersingsmaatregel die niet effectief is opgezet. Daarom evalueert de accountant de opzet van een interne beheersingsmaatregel eerst. Een niet-adequaat opgezette interne beheer- singsmaatregel kan een tekortkoming in de interne beheersing vormen.
A177. Risk assessment procedures to obtain audit evidence about the design and implementation of identified controls in the control activities component may include: • Inquiring of entity personnel. • Observing the application of specific controls. • Inspecting documents and reports. Inquiry alone, however, is not sufficient for such purposes.	A177 Risico-inschattingswerkzaamheden om controle-informatie te verkrijgen over de opzet en de implementatie van geïdentificeerde interne beheersingsmaatregelen in de component 'interne beheersingsactiviteiten' kunnen omvatten: • verzoeken om inlichtingen bij personeel van de entiteit; • waarneming van de toepassing van specifieke interne beheersingsmaatregelen; • inspectie van documenten en rapporten. Verzoek om inlichtingen alleen is echter niet voldoende voor dergelijke doeleinden.
A178. The auditor may expect, based on experience from the previous audit or based on current period risk assessment procedures, that management does not have effectively designed or implemented controls to address a significant risk. In such instances, the procedures performed to address the requirement in paragraph 26(d) may consist of determining that such controls have not been effectively designed or implemented. If the results of the procedures indicate that controls have been newly designed or implemented, the auditor is required to perform the procedures in paragraph 26(b)–(d) on the newly designed or implemented controls.	A178 De accountant kan verwachten, op basis van ervaring uit de vorige controle of op basis van de risico-inschattingswerkzaamheden in de huidige verslagperiode, dat het management geen ef- fectieve interne beheersingsmaatregelen heeft opgezet of geïmplementeerd om in te spelen op een significant risico. In dergelijke gevallen kunnen de werkzaamheden die worden uitgevoerd om het vereiste in paragraaf 26 (d) te adresseren, bestaan uit het vaststellen dat dergelijke in- terne beheersingsmaatregelen niet effectief zijn opgezet of geïmplementeerd. Als de resultaten van de werkzaamheden aangeven dat interne beheersingsmaatregelen nieuw zijn opgezet of geïmplementeerd, dan moet de accountant de werkzaamheden in paragraaf 26(b)-(d) uitvoe- ren voor de nieuw opgezette of geïmplementeerde interne beheersingsmaatregelen.
A179. The auditor may conclude that a control, which is effectively designed and implemented, may be appropriate to test in order to take its operating effectiveness into account in designing substantive procedures. However, when a control is not designed or implemented effectively, there is no benefit in testing it. When the auditor plans to test a control, the information obtained about the extent to which the control addresses the risk(s) of material misstatement is an input to the auditor's control risk assessment at the assertion level. A180. Evaluating the design and determining the implementation of identified controls in the control activities component is not sufficient to test their operating effectiveness. However, for automated controls, the auditor may plan to test the operating effectiveness of automated controls by identifying and testing general IT controls that provide for the consistent operation of an automated control instead of performing tests of operating effectiveness on the automated controls directly. Obtaining audit evidence about the implementation of a manual control at a point in time does not provide audit evidence about the operating effectiveness of the control at other times during the period under audit. Tests of the operating effectiveness of controls, including tests of indirect controls, are further described in ISA 330.45 A181. When the auditor does not plan to test the operating effectiveness of identified controls, the auditor's understanding may still assist in the design of the nature, timing and extent of substantive audit procedures that are responsive to the related risks of material misstatement.	A179 De accountant kan concluderen dat een interne beheersingsmaatregel, die effectief is opgezet en geïmplementeerd, geschikt kan zijn om de effectieve werking te toetsen, zodat de accoun- tant de effectieve werking in overweging kan nemen bij het opzetten van gegevensgerichte werkzaamheden. Als een interne beheersingsmaatregel echter niet effectief is opgezet of ge- implementeerd, heeft het geen zin om deze te toetsen. Wanneer de accountant van plan is een interne beheersingsmaatregel te toetsen, is de informatie die verkregen is over de mate waarin de interne beheersingsmaatregel inspeelt op risico(s) op een afwijking van materieel belang, een factor voor de risico-inschatting van de accountant van de interne beheersingsmaatregel op het niveau van beweringen.

	A180 Het evalueren van de opzet en het bepalen van de implementatie van geïdentificeerde interne beheersingsmaatregelen in de component 'interne beheersingsactiviteiten' is niet voldoende om hun effectieve werking te toetsen. Voor geautomatiseerde interne beheersingsmaatregelen kan de accountant echter van plan zijn om de effectieve werking van geautomatiseerde interne beheersingsmaatregelen te toetsen door general IT controls, die zorgen voor de consistente werking van een geautomatiseerde controle, te identificeren en te toetsen. Dit in plaats van het direct toetsen van de effectieve werking van de geautomatiseerde interne beheersingsmaatre- gelen. Het verkrijgen van controle-informatie over de implementatie van een handmatige in- terne beheersingsmaatregel op een bepaald tijdstip levert geen controle-informatie op over de effectieve werking van de interne beheersingsmaatregel op andere tijdstippen tijdens de ge- controleerde periode. Toetsingen van de effectieve werking van interne beheersingsmaatrege- len, inclusief toetsingen van indirecte interne beheersingsmaatregelen, zijn verder beschreven in Standaard 330.46 A181 Wanneer de accountant niet van plan is om de effectieve werking van geïdentificeerde interne beheersingsmaatregelen te toetsen, kan het verworven inzicht van de accountant nog steeds helpen bij de opzet van de aard, timing en omvang van gegevensgerichte controlewerkzaam- heden die inspelen op de gerelateerde risico's op een afwijking van materieel belang.
Control Deficiencies Within the Entity's System of Internal Control (Ref: Para. 27) A182. In performing the evaluations of each of the components of the entity's system of internal control,46 the auditor may determine that certain of the entity's policies in a component are not appropriate to the nature and circumstances of the entity. Such a determination may be an indicator that assists the auditor in identifying control deficiencies. If the auditor has identified one or more control deficiencies, the auditor may consider the effect of those control deficiencies on the design of further audit procedures in accordance with ISA 330. A183. If the auditor has identified one or more control deficiencies, ISA 26547 requires the auditor to determine whether, individually or in combination, the deficiencies constitute a significant deficiency. The auditor uses professional judgment in determining whether a deficiency represents a significant control deficiency.48 Identifying and Assessing the Risks of Material Misstatement (Ref: Para. 28–37) Why the Auditor Identifies and Assesses the Risks of Material Misstatement A184. Risks of material misstatement are identified and assessed by the auditor in order to determine the nature, timing and extent of further audit procedures necessary to obtain sufficient appropriate audit evidence. This evidence enables the auditor to express an opinion on the financial statements at an acceptably low level of audit risk. A185. Information gathered by performing risk assessment procedures is used as audit evidence to provide the basis for the identification and assessment of the risks of material misstatement. For example, the audit evidence obtained when evaluating the design of identified controls and determining whether those controls have been implemented in the control activities component, is used as audit evidence to support the risk assessment. Such evidence also provides a basis for the auditor to design overall responses to address the assessed risks of material misstatement at the financial statement level, as well as designing and performing further audit procedures whose nature, timing and extent are responsive to the assessed risks of material misstatement at the assertion level, in accordance with ISA 330.	Tekortkomingen in interne beheersing binnen het interne beheersingssysteem van de entiteit (Zie Par. 27) A182 Bij het uitvoeren van de evaluaties van elk van de componenten van het interne beheersings- systeem van de entiteit,47 kan de accountant bepalen dat bepaalde beleidslijnen van de entiteit 46 Standaard 330, paragrafen 8–11. 47 Paragrafen 21(b), 22(b), 24(c), 25(c) en 26(d). in een component niet geschikt zijn voor de aard en omstandigheden van de entiteit. Een der- gelijke bepaling kan een indicator zijn die de accountant helpt bij het identificeren van tekortko- mingen in de interne beheersing. Als de accountant een of meer tekortkomingen in de interne beheersing heeft geïdentificeerd, kan de accountant het effect van die tekortkomingen in de interne beheersing overwegen bij het opzetten van verdere controlewerkzaamheden in over- eenstemming met Standaard 330. A183 Als de accountant een of meer tekortkomingen in de interne beheersing heeft geïdentificeerd, vereist Standaard 26548 van de accountant om te bepalen of de tekortkomingen, afzonderlijk of in combinatie, een significante tekortkoming vormen. De accountant past professionele oordeelsvorming toe om te bepalen of een tekortkoming een significante tekortkoming in de interne beheersing vormt.49 De risico's op een afwijking van materieel belang identificeren en inschatten (Zie Par. 28 - 37) Waarom de accountant de risico's op een afwijking van materieel belang identificeert en inschat A184 Risico's op een afwijking van materieel belang worden geïdentificeerd en ingeschat door de accountant om de aard, timing en omvang van verdere controlewerkzaamheden die nodig zijn om voldoende en geschikte controle-informatie te verkrijgen, te bepalen. Deze informatie stelt de accountant in staat om een oordeel geven over de financiële overzichten bij een aanvaard- baar laag niveau van controlerisico.

	A185 Informatie die wordt verzameld door het uitvoeren van risico-inschattingswerkzaamheden wordt gebruikt als controle-informatie om de basis voor de identificatie en inschatting van de risico's op een afwijking van materieel belang te verschaffen. De controle-informatie verkregen bij het evalueren van de opzet van geïdentificeerde interne beheersingsmaatregelen en het be- palen of die interne beheersingsmaatregelen zijn geïmplementeerd in de component 'interne beheersingsactiviteiten', wordt bijvoorbeeld als controle -informatie gebruikt om de risico-in- schatting te ondersteunen. Dergelijke informatie biedt ook een basis voor de accountant om algehele manieren op te zetten om in te spelen op de ingeschatte risico's op een afwijking van materieel belang op het niveau van de financiële overzichten, evenals het opzetten en uitvoe- ren van verdere controlewerkzaamheden waarvan de aard, timing en omvang inspelen op de ingeschatte risico's op een afwijking van materieel belang op het niveau van beweringen, in overeenstemming met Standaard 330.
Identifying Risks of Material Misstatement (Ref: Para. 28) A186. The identification of risks of material misstatement is performed before consideration of any related controls (i.e., the inherent risk), and is based on the auditor's preliminary consideration of misstatements that have a reasonable possibility of both occurring, and being material if they were to occur.49	Identificeren van risico's op een afwijking van materieel belang (Zie Par. 28) A186 De identificatie van risico's op een afwijking van materieel belang wordt uitgevoerd voordat re- kening wordt gehouden met eventuele daarop betrekking hebbende interne beheersingsmaat- regelen (d.w.z. het inherente risico) en is gebaseerd op de voorlopige overweging van de ac- countant van afwijkingen die een redelijke mogelijkheid hebben om zowel voor te komen als om van materieel belang te zijn als ze voorkomen.50
A187. Identifying the risks of material misstatement also provides the basis for the auditor's determination of relevant assertions, which assists the auditor's determination of the significant classes of transactions, account balances and disclosures.	A187 Het identificeren van de risico's op een afwijking van materieel belang vormt ook de basis voor de vaststelling door de accountant van relevante beweringen, die de accountant helpen bij het bepalen van de significante transactiestromen, rekeningsaldi en toelichtingen.
Assertions Why the Auditor Uses Assertions A188. In identifying and assessing the risks of material misstatement, the auditor uses assertions to consider the different types of potential misstatements that may occur. Assertions for which the auditor has identified related risks of material misstatement are relevant assertions.	Beweringen Waarom de accountant beweringen gebruikt A188 Bij het identificeren en inschatten van de risico's op een afwijking van materieel belang gebruikt de accountant beweringen om rekening houden met de verschillende soorten potentiële afwij- kingen die kunnen voorkomen. Beweringen waarvoor de accountant gerelateerde risico's op een afwijking van materieel belang heeft geïdentificeerd, zijn relevante beweringen.
The Use of Assertions A189. In identifying and assessing the risks of material misstatement, the auditor may use the categories of assertions as described in paragraph A190(a)–(b) below or may express them differently provided all aspects described below have been covered. The auditor may choose to combine the assertions about classes of transactions and events, and related disclosures, with the assertions about account balances, and related disclosures.	Het gebruik van beweringen A189 Bij het identificeren en inschatten van de risico's op een afwijking van materieel belang kan de accountant de categorieën van beweringen gebruiken zoals beschreven in paragraaf A190 (a) - (b) hieronder of kan deze anders weergeven mits alle hieronder beschreven aspecten zijn be- handeld. De accountant kan ervoor kiezen om de beweringen over transactiestromen en ge- beurtenissen en daarop betrekking hebbende toelichtingen te combineren met de beweringen over rekeningsaldi en daarop betrekking hebbende toelichtingen.
A190. Assertions used by the auditor in considering the different types of potential misstatements that may occur may fall into the following categories: (a) Assertions about classes of transactions and events, and related disclosures, for the period under audit: (i) Occurrence—transactions and events that have been recorded or disclosed have occurred, and such transactions and events pertain to the entity. (ii) Completeness—all transactions and events that should have been recorded have been recorded, and all related disclosures that should have been included in the financial statements have been included. (iii) Accuracy—amounts and other data relating to recorded transactions and events have been recorded appropriately, and related disclosures have been appropriately measured and described. (iv) Cutoff—transactions and events have been recorded in the correct accounting period. (v) Classification—transactions and events have been recorded in the proper accounts. (vi) Presentation—transactions and events are appropriately aggregated or disaggregated and clearly described, and related disclosures are relevant and understandable in the context of the requirements of the applicable financial reporting framework. (b) Assertions about account balances, and related disclosures, at the period end:	A190 Beweringen die door de accountant worden gebruikt bij het overwegen van de verschillende soorten potentiële afwijkingen die kunnen voorkomen, kunnen in de volgende categorieën val- len: a Beweringen over transactiestromen en gebeurtenissen en daarop betrekking hebbende toelichtingen tijdens de gecontroleerde periode: i Voorkomen - de vastgelegde of toegelichte transacties en gebeurtenissen hebben in- derdaad plaatsgevonden en dergelijke transacties en gebeurtenissen hebben betrek- king op de entiteit;

(i) Existence—assets, liabilities and equity interests exist.
(ii) Rights and obligations—the entity holds or controls the rights to assets, and liabilities are the obligations of the entity.

(iii) Completeness—all assets, liabilities and equity interests that should have been recorded have been recorded, and all related disclosures that should have been included in the financial statements have been included.
(iv) Accuracy, valuation and allocation—assets, liabilities and equity interests have been included in the financial statements at appropriate amounts and any resulting valuation or allocation adjustments have been appropriately recorded, and related disclosures have been appropriately measured and described.
(v) Classification—assets, liabilities and equity interests have been recorded in the proper accounts.
(vi) Presentation—assets, liabilities and equity interests are appropriately aggregated or disaggregated and clearly described, and related disclosures are relevant and understandable in the context of the requirements of the applicable financial reporting framework.
A191. The assertions described in paragraph A190(a)–(b) above, adapted as appropriate, may also be used by the auditor in considering the different types of misstatements that may occur in disclosures not directly related to recorded classes of transactions, events or account balances.

Considerations Specific to Public Sector Entities
A192. When making assertions about the financial statements of public sector entities, in addition to those assertions set out in paragraph A190(a)–(b), management may often assert that transactions and events have been carried out in accordance with law, regulation or other authority. Such assertions may fall within the scope of the financial statement audit.

Risks of Material Misstatement at the Financial Statement Level (Ref: Para. 28(a) and 30)
Why the Auditor Identifies and Assesses Risks of Material Misstatement at the Financial Statement Level A193. The auditor identifies risks of material misstatement at the financial statement level to determine whether the risks have a pervasive effect on the financial statements, and would therefore require an overall response in accordance with ISA 330.50
A194. In addition, risks of material misstatement at the financial statement level may also affect individual assertions, and identifying these risks may assist the auditor in assessing risks of material

50 ISA 330, paragraph 5

misstatement at the assertion level, and in designing further audit procedures to address the identified risks.

ii Volledigheid - alle transacties en gebeurtenissen die hadden moeten worden vastge- legd, zijn ook vastgelegd en alle daarop betrekking toelichtingen die hadden moeten worden opgenomen in de financiële overzichten, zijn opgenomen;
iii Nauwkeurigheid - bedragen en andere gegevens die betrekking hebben op vastge- legde transacties en gebeurtenissen zijn op de juiste wijze vastgelegd en daarop be- trekking hebbende toelichtingen zijn op de juiste wijze vastgelegd en beschreven;
iv Afgrenzing - transacties en gebeurtenissen zijn in de juiste verslagperiode vastgelegd; v Classificatie - transacties en gebeurtenissen zijn op de juiste rekeningen vastgelegd; vi Presentatie - transacties en gebeurtenissen zijn op de juiste wijze samengevoegd of uitgesplitst en duidelijk beschreven, en daarop betrekking hebbende toelichtingen zijn relevant en begrijpelijk in de context van de vereisten van het van toepassing zijnde stelsel inzake financiële verslaggeving.
b Beweringen over rekeningsaldi en daarop betrekking hebbende toelichtingen aan het einde van de verslagperiode:
i Bestaan - activa, passiva en eigenvermogensbelangen bestaan;
ii Rechten en verplichtingen - de entiteit bezit of heeft zeggenschap over de rechten op activa, en de verplichtingen zijn de verplichtingen voor de entiteit;
iii Volledigheid: - alle activa, passiva en eigenvermogensbelangen die hadden moeten worden vastgelegd, zijn ook vastgelegd en alle daarop betrekking hebbende toelichtin- gen die hadden moeten worden opgenomen in de financiële overzichten, zijn ook op- genomen;
iv Nauwkeurigheid, waardering en toerekening - activa, passiva en eigenvermogensbe- langen zijn voor de juiste bedragen in de financiële overzichten opgenomen en de daaruit voortvloeiende waarderings- en toerekeningscorrecties zijn juist vastgelegd en daarop betrekking hebbende toelichtingen zijn juist vastgelegd en beschreven;
v Classificatie - activa, passiva en eigenvermogensbelangen zijn vastgelegd op de juiste rekeningen;
vi Presentatie - activa, passiva en eigenvermogensbelangen zijn op juiste wijze samen- gevoegd of uitgesplitst en duidelijk beschreven en daarop betrekking hebbende toe- lichtingen zijn relevant en begrijpelijk in de context van de vereisten van het van toe- passing zijnde stelsel inzake financiële verslaggeving.

A191 De beweringen beschreven in paragraaf A190(a)-(b) hierboven, zo nodig aangepast, kunnen ook worden gebruikt door de accountant bij het overwegen van de verschillende soorten afwij- kingen die kunnen voorkomen in toelichtingen die niet direct verband houden met vastgelegde transactiestromen, gebeurtenissen of rekeningsaldi.

Overwegingen specifiek voor entiteiten in de publieke sector

A192 Bij het maken van beweringen over de financiële overzichten van entiteiten in de publieke sec- tor, in aanvulling op die beweringen die uiteengezet zijn in paragraaf A190 (a) - (b), kan het management vaak beweren dat transacties en gebeurtenissen zijn uitgevoerd in overeenstem- ming met wet- en regelgeving of andere van kracht zijnde voorschriften. Dergelijke beweringen kunnen binnen de reikwijdte van de controle van de financiële overzichten vallen.

Risico’s op een afwijking van materieel belang op het niveau van de financiële overzichten (Zie Par. 28(a) en 30)
Waarom de accountant risico's op een afwijking van materieel belang op het niveau van de financiële overzichten identificeert en inschat

	A193 De accountant identificeert de risico's op een afwijking van materieel belang op het niveau van de financiële overzichten om te bepalen of de risico's een diepgaande invloed hebben op de financiële overzichten en daarom een algehele manier van inspelen vereisen in overeenstem- ming met Standaard 330.51 A194 Bovendien kunnen risico's op een afwijking van materieel belang op het niveau van de financi- ele overzichten ook individuele beweringen beïnvloeden en het identificeren van deze risico's kan de accountant helpen bij het inschatten van risico's op een afwijking van materieel belang op het niveau van beweringen en bij het opzetten van verdere controlewerkzaamheden om in te spelen op de geïdentificeerde risico's.
Identifying and Assessing Risks of Material Misstatement at the Financial Statement Level A195. Risks of material misstatement at the financial statement level refer to risks that relate pervasively to the financial statements as a whole, and potentially affect many assertions. Risks of this nature are not necessarily risks identifiable with specific assertions at the class of transactions, account balance or disclosure level (e.g., risk of management override of controls). Rather, they represent circumstances that may pervasively increase the risks of material misstatement at the assertion level. The auditor's evaluation of whether risks identified relate pervasively to the financial statements supports the auditor's assessment of the risks of material misstatement at the financial statement level. In other cases, a number of assertions may also be identified as susceptible to the risk, and may therefore affect the auditor's risk identification and assessment of risks of material misstatement at the assertion level. A196. The auditor's identification and assessment of risks of material misstatement at the financial statement level is influenced by the auditor's understanding of the entity's system of internal control, in particular the auditor's understanding of the control environment, the entity's risk assessment process and the entity's process to monitor the system of internal control, and: • The outcome of the related evaluations required by paragraphs 21(b), 22(b), 24(c) and 25(c); and • Any control deficiencies identified in accordance with paragraph 27. In particular, risks at the financial statement level may arise from deficiencies in the control environment or from external events or conditions such as declining economic conditions. A197. Risks of material misstatement due to fraud may be particularly relevant to the auditor's consideration of the risks of material misstatement at the financial statement level.	Het identificeren en inschatten van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten A195 Risico's op een afwijking van materieel belang op het niveau van de financiële overzichten be- treffen risico's die een diepgaande invloed hebben op de financiële overzichten als geheel en hebben mogelijk invloed op een groot aantal beweringen. Risico's van deze aard zijn niet noodzakelijkerwijs risico's die in verband kunnen worden gebracht met specifieke beweringen op het niveau van transactiestromen, rekeningsaldi of toelichtingen (bijv. het risico dat het ma- nagement de interne beheersingsmaatregelen doorbreekt). Ze vertegenwoordigen eerder om- standigheden die de risico's op een afwijking van materieel belang op het niveau van bewerin- gen diepgaand kunnen vergroten. De evaluatie door de accountant van de vraag of geïdentifi- ceerde risico's diepgaand verband houden met de financiële overzichten ondersteunt de in- schatting door de accountant van de risico's op een afwijking van materieel belang op het ni- veau van de financiële overzichten. In andere gevallen kan een aantal beweringen ook worden geïdentificeerd als vatbaar voor het risico en kan daarom van invloed zijn op de risico-identifi- catie en inschatting van de accountant van risico's op een afwijking van materieel belang op het niveau van bewering. A196 De identificatie en inschatting door de accountant van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten wordt beïnvloed door het inzicht van de ac- countant in het interne beheersingssysteem van de entiteit, in het bijzonder het inzicht van de accountant in de interne beheersingsomgeving, het risico-inschattingsproces van de entiteit en het proces van de entiteit om het systeem van interne beheersing te monitoren, en: • Het resultaat van de bijbehorende evaluaties vereist op grond van paragrafen 21(b), 22(b), 24(c) en 25(c); en • Eventuele tekortkomingen in de interne beheersing die zijn geïdentificeerd in overeenstem- ming met paragraaf 27. In het bijzonder kunnen risico's op het niveau van de financiële overzichten voortkomen uit te- kortkomingen in de interne beheersingsomgeving of uit externe gebeurtenissen of omstandig- heden zoals verslechterende economische omstandigheden. A197 Risico's op een afwijking van materieel belang als gevolg van fraude kunnen met name rele- vant zijn voor de overweging van de accountant van de risico's op een afwijking van materieel belang op het niveau van de financiële overzichten.
A198. The auditor's understanding, including the related evaluations, of the control environment and other components of the system of internal control may raise doubts about the auditor's ability to obtain audit evidence on which to base the audit opinion or be cause for withdrawal from the engagement where withdrawal is possible under applicable law or regulation. A199. ISA 705 (Revised)51 establishes requirements and provides guidance in determining whether there is a need for the auditor to express a qualified opinion or disclaim an opinion or, as may be required in some cases, to withdraw from the engagement where withdrawal is possible under applicable law or regulation. Considerations Specific to Public Sector Entities A200. For public sector entities, the identification of risks at the financial statement level may include consideration of matters related to the political climate, public interest and program sensitivity.	A198 Het inzicht van de accountant, inclusief de bijbehorende evaluaties, van de interne beheer- singsomgeving en andere componenten van het systeem van interne beheersing kunnen twij- fels doen rijzen over de mogelijkheid van de accountant om controle-informatie te verkrijgen waarop het

	controleoordeel kan worden gebaseerd of kan reden zijn om de opdracht terug te geven indien dat onder de van toepassing zijnde wet- of regelgeving mogelijk is. A199 Standaard 705 52 stelt eisen en geeft leidraden bij het bepalen of het nodig is voor de accountant om een gekwalificeerd oordeel te geven of een oordeelonthouding af te geven of, indien vereist in sommige gevallen, om de opdracht terug te geven indien dat onder de van toepas- sing zijnde wet of regelgeving mogelijk is. Overwegingen specifiek voor entiteiten in de publieke sector A200 Voor entiteiten in de publieke sector kan de identificatie van risico's op het niveau van de financiële overzichten overweging van aangelegenheden omvatten die verband houden met het po- litieke klimaat, het publieke belang en de programma gevoeligheid.
Risks of Material Misstatement at the Assertion Level (Ref: Para. 28(b)) A201. Risks of material misstatements that do not relate pervasively to the financial statements are risks of material misstatement at the assertion level.	Risico's op een afwijking van materieel belang op het niveau van beweringen (Zie Par. 28(b)) A201 Risico's op afwijkingen van materieel belang die niet diepgaand betrekking hebben op de financiële overzichten zijn risico's op afwijkingen van materieel belang op het niveau van bewerin- gen.
Relevant Assertions and Significant Classes of Transactions, Account Balances and Disclosures (Ref: Para. 29) Why Relevant Assertions and Significant Classes of Transactions, Account Balances and Disclosures Are Determined A202. Determining relevant assertions and the significant classes of transactions, account balances and disclosures provides the basis for the scope of the auditor's understanding of the entity's information system required to be obtained in accordance with paragraph 25(a). This understanding may further assist the auditor in identifying and assessing risks of material misstatement (see A86). Automated Tools and Techniques A203. The auditor may use automated techniques to assist in the identification of significant classes of transactions, account balances and disclosures. Disclosures that May Be Significant A204. Significant disclosures include both quantitative and qualitative disclosures for which there is one or more relevant assertions. Examples of disclosures that have qualitative aspects and that may have relevant assertions and may therefore be considered significant by the auditor include disclosures about: • Liquidity and debt covenants of an entity in financial distress. • Events or circumstances that have led to the recognition of an impairment loss. • Key sources of estimation uncertainty, including assumptions about the future. • The nature of a change in accounting policy, and other relevant disclosures required by the applicable financial reporting framework, where, for example, new financial reporting requirements are expected to have a significant impact on the financial position and financial performance of the entity. • Share-based payment arrangements, including information about how any amounts recognized were determined, and other relevant disclosures. • Related parties, and related party transactions. • Sensitivity analysis, including the effects of changes in assumptions used in the entity's valuation techniques intended to enable users to understand the underlying measurement uncertainty of a recorded or disclosed amount. Assessing Risks of Material Misstatement at the Assertion Level	Relevante beweringen en significante transactiestromen, rekeningsaldi en toelichtingen (Zie Par. 29) Waarom relevante beweringen en significante transactiestromen, rekeningsaldi en toelichtingen worden bepaald A202 Bepaling van relevante beweringen en de significante transactiestromen, rekeningsaldi en toelichtingen vormen de basis voor de reikwijdte van het inzicht van de accountant in het informatiesysteem van de entiteit zoals vereist in overeenstemming met paragraaf 25 (a). Dit inzicht kan de accountant verder helpen bij het identificeren en inschatten van risico's op een afwijking van materieel belang (Zie Par. A86). Geautomatiseerde hulpmiddelen en technieken A203 De accountant kan geautomatiseerde technieken gebruiken om te helpen bij de identificatie van significante transactiestromen, rekeningsaldi en toelichtingen. Toelichtingen die significant kunnen zijn A204 Significante toelichtingen omvatten zowel kwantitatieve als kwalitatieve toelichtingen waarvoor er een of meer relevante beweringen zijn. Voorbeelden van toelichtingen die kwalitatieve as- pecten hebben en die mogelijk relevante beweringen hebben en die daarom door de accoun- tant als significant kunnen worden beschouwd, omvatten toelichtingen over: • liquiditeits- en schuldconvenanten van een entiteit in financiële nood; • gebeurtenissen of omstandigheden die hebben geleid tot de opname van een bijzondere waardevermindering; • belangrijkste bronnen van schattingsonzekerheid, inclusief veronderstellingen over de toekomst; • de aard van een wijziging in de grondslagen voor financiële verslaggeving en andere relevante toelichtingen vereist door het van toepassing zijnde stelsel inzake financiële verslag- geving,

Assessing Inherent Risk (Ref: Para. 31–33) Assessing the likelihood and magnitude of misstatement (Ref: Para: 31) Why the auditor assesses likelihood and magnitude of misstatement A205. The auditor assesses the likelihood and magnitude of misstatement for identified risks of material misstatement because the significance of the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement were the misstatement to occur determines where on the spectrum of inherent risk the identified risk is assessed, which informs the auditor's design of further audit procedures to address the risk.	waar bijvoorbeeld nieuwe vereisten inzake financiële verslaggeving naar verwach- ting een significante invloed op de financiële positie en de financiële prestaties van de enti- teit zullen hebben; • op aandelen gebaseerde betalingsregelingen, inclusief informatie over hoe alle opgenomen bedragen werden bepaald, en andere relevante toelichtingen; • verbonden partijen en transacties met verbonden partijen; • gevoeligheidsanalyse, inclusief de effecten van veranderingen in veronderstellingen die in de waarderingsmethoden van de entiteit gebruikt worden met de bedoeling om gebruikers in staat te stellen de onderliggende waarderingsonzekerheid van een vastgelegd of toege- licht bedrag te begrijpen. Inschatting van risico's op een afwijking van materieel belang op het niveau van beweringen Inschatting van het inherente risico (Zie Par. 31–33) Inschatting van de waarschijnlijkheid en de orde van grootte van een afwijking (Zie Par. 31) Waarom de accountant de waarschijnlijkheid en de orde van grootte van een afwijking inschat A205 De accountant beoordeelt de waarschijnlijkheid en de orde van grootte van afwijkingen voor geïdentificeerde risico's op een afwijking van materieel belang. De significantie van de combi- natie van de waarschijnlijkheid dat een afwijking voorkomt en de orde van grootte van de mo- gelijke afwijking waar de afwijking zou voorkomen, bepaalt waar op het spectrum van het inhe- rente risico het geïdentificeerde risico wordt ingeschat, hetgeen de opzet van verdere controle- werkzaamheden van de accountant om in te spelen op risico's aangeeft.
A206. Assessing the inherent risk of identified risks of material misstatement also assists the auditor in determining significant risks. The auditor determines significant risks because specific responses to significant risks are required in accordance with ISA 330 and other ISAs. A207. Inherent risk factors influence the auditor's assessment of the likelihood and magnitude of misstatement for the identified risks of material misstatement at the assertion level. The greater the degree to which a class of transactions, account balance or disclosure is susceptible to material misstatement, the higher the inherent risk assessment is likely to be. Considering the degree to which inherent risk factors affect the susceptibility of an assertion to misstatement assists the auditor in appropriately assessing inherent risk for risks of material misstatement at the assertion level and in designing a more precise response to such a risk. Spectrum of inherent risk	A206 Het inschatten van het inherente risico op geïdentificeerde risico's op een afwijking van materi- eel belang helpt de accountant ook bij het bepalen van significante risico's. De accountant be- paalt significante risico's omdat specifieke manieren van inspelen op significante risico's vereist zijn in overeenstemming met Standaard 330 en andere Standaarden. A207 Inherente risicofactoren beïnvloeden de inschatting van de accountant van de waarschijnlijk- heid en de orde van grootte van afwijking voor de geïdentificeerde risico's op een afwijking van materieel belang op het niveau van beweringen. Hoe groter de mate waarin een transactie- stroom, rekeningsaldo of toelichting gevoelig is voor een afwijking van materieel belang, hoe hoger de inherente risico-inschatting waarschijnlijk is. Overwegen van de mate waarin inhe- rente risicofactoren de vatbaarheid van een bewering voor afwijking beïnvloeden, helpt de ac- countant bij een passende inschatting van het inherente risico voor risico's op een afwijking van materieel belang op het niveau van beweringen en in een nauwkeurigere manier van in- spelen op een dergelijk risico.
A208. In assessing inherent risk, the auditor uses professional judgment in determining the significance of the combination of the likelihood and magnitude of a misstatement. A209. The assessed inherent risk relating to a particular risk of material misstatement at the assertion level represents a judgment within a range, from lower to higher, on the spectrum of inherent risk. The judgment about where in the range inherent risk is assessed may vary based on the nature, size and complexity of the entity, and takes into account the assessed likelihood and magnitude of the misstatement and inherent risk factors. A210. In considering the likelihood of a misstatement, the auditor considers the possibility that a misstatement may occur, based on consideration of the inherent risk factors. A211. In considering the magnitude of a misstatement, the auditor considers the qualitative and quantitative aspects of the possible misstatement (i.e., misstatements in assertions about classes of transactions, account balances or disclosures may be judged to be material due to size, nature or circumstances).	Spectrum van inherent risico A208 Bij het inschatten van het inherente risico past de accountant professionele oordeelsvorming toe bij het bepalen van de significantie van de combinatie van de waarschijnlijkheid en de orde van grootte van een afwijking.
A212. The auditor uses the significance of the combination of the likelihood and magnitude of a possible misstatement in determining where on the spectrum of inherent risk (i.e., the range) inherent risk is assessed. The higher the combination of likelihood and magnitude, the higher the assessment of inherent risk; the lower the combination of likelihood and magnitude, the lower the assessment of inherent risk. A213. For a risk to be assessed as higher on the spectrum of inherent risk, it does not mean that both the magnitude and likelihood need to be assessed as high. Rather, it is the intersection of the magnitude and likelihood of the material misstatement on the spectrum of inherent risk that will determine whether the assessed inherent risk is higher or lower on the spectrum of inherent risk. A higher inherent risk assessment may	A209 Het ingeschatte inherente risico met betrekking tot een bepaald risico op een afwijking van ma- terieel belang op het niveau van beweringen vertegenwoordigt een oordeelsvorming binnen een interval van lager naar hoger in het spectrum van inherent risico. De oordeelsvorming over waar in het interval het inherente risico wordt ingeschat, kan variëren op basis van de aard, omvang en complexiteit van de entiteit en houdt rekening met de geschatte waarschijnlijkheid en orde van grootte van de afwijkingen en inherente risicofactoren. A210 Bij het overwegen van de waarschijnlijkheid van een afwijking, overweegt de accountant de mogelijkheid dat er een afwijking kan voorkomen, rekening houdend met de inherente risico- factoren.

also arise from different combinations of likelihood and magnitude, for example a higher inherent risk assessment could result from a lower likelihood but a very high magnitude.	A211 Bij het overwegen van de orde van grootte van een afwijking beschouwt de accountant de kwalitatieve en kwantitatieve aspecten van de mogelijke afwijking (d.w.z. afwijkingen in beweringen over transactiestromen, rekeningsaldi of toelichtingen kunnen als van materieel belang worden beoordeeld vanwege de omvang, aard of omstandigheden). A212 De accountant gebruikt de significantie van de combinatie van de waarschijnlijkheid en de orde van grootte van een mogelijke afwijking bij het bepalen waar op het spectrum van inherent ri- sico (d.w.z. het interval) het inherente risico is ingeschat. Hoe hoger de combinatie van waarschijnlijkheid en orde van grootte, hoe hoger de inschatting van inherent risico; hoe lager de combinatie van waarschijnlijkheid en orde van grootte, hoe lager de inschatting van inherent risico. A213 Voor een risico dat als hoger wordt ingeschat in het spectrum van inherent risico, betekent dit niet dat zowel orde van grootte als waarschijnlijkheid als hoog moeten worden ingeschat. Het is eerder het kruispunt van de grootte en waarschijnlijkheid van de afwijking van materieel be- lang in het spectrum van inherent risico dat zal bepalen of het ingeschatte inherente risico ho- ger of lager is in het spectrum van inherent risico. Een hogere inherente risico-inschatting kan ook voortkomen uit verschillende combinaties van waarschijnlijkheid en orde van grootte. Een hogere inherente risico-inschatting zou bijvoorbeeld kunnen resulteren uit een lagere waar- schijnlijkheid maar een zeer hoge orde van grootte.
A214. In order to develop appropriate strategies for responding to risks of material misstatement, the auditor may designate risks of material misstatement within categories along the spectrum of inherent risk, based on their assessment of inherent risk. These categories may be described in different ways. Regardless of the method of categorization used, the auditor's assessment of inherent risk is appropriate when the design and implementation of further audit procedures to address the identified risks of material misstatement at the assertion level is appropriately responsive to the assessment of inherent risk and the reasons for that assessment. Pervasive Risks of Material Misstatement at the Assertion Level (Ref: Para 31(b)) A215. In assessing the identified risks of material misstatement at the assertion level, the auditor may conclude that some risks of material misstatement relate more pervasively to the financial statements as a whole and potentially affect many assertions, in which case the auditor may update the identification of risks of material misstatement at the financial statement level. A216. In circumstances in which risks of material misstatement are identified as financial statement level risks due to their pervasive effect on a number of assertions, and are identifiable with specific assertions, the auditor is required to take into account those risks when assessing inherent risk for risks of material misstatement at the assertion level. Considerations Specific to Public Sector Entities A217. In exercising professional judgment as to the assessment of the risk of material misstatement, public sector auditors may consider the complexity of the regulations and directives, and the risks of non- compliance with authorities. Significant Risks (Ref: Para. 32) Why significant risks are determined and the implications for the audit A218. The determination of significant risks allows for the auditor to focus more attention on those risks that are on the upper end of the spectrum of inherent risk, through the performance of certain required responses, including: • Controls that address significant risks are required to be identified in accordance with paragraph 26(a)(i), with a requirement to evaluate whether the control has been designed effectively and implemented in accordance with paragraph 26(d).	A214 Om geschikte strategieën te ontwikkelen om te reageren op risico's op een afwijking van materieel belang, kan de accountant risico's op een afwijking van materieel belang aanduiden bin- nen categorieën in het spectrum van inherent risico, op basis van hun inschatting van inherent risico. Deze categorieën kunnen op verschillende manieren worden beschreven. Ongeacht de gebruikte methode van categorisatie, is de inschatting door de accountant van inherent risico passend wanneer de opzet en de uitvoering van verdere controlewerkzaamheden om de ge- identificeerde risico's op een afwijking van materieel belang op het niveau van beweringen te behandelen, adequaat inspelen op de inschatting van inherent risico en de redenen voor die inschatting. Risico's met een diepgaande invloed op een afwijking van materieel belang op het niveau van beweringen (Zie Par. 31(b)) A215 Bij het inschatten van de geïdentificeerde risico's op een afwijking van materieel belang op het niveau van beweringen, kan de accountant concluderen dat sommige risico's op een afwijking van materieel belang meer diepgaand verband houden met de financiële overzichten als ge- heel en mogelijk van invloed zijn op een groot aantal beweringen, in welk geval de accountant de identificatie van risico's op een afwijking van materieel belang op het niveau van de financi- ele overzichten bijwerkt. A216 In omstandigheden waarin risico's op een afwijking van materieel belang worden geïdentificeerd als risico's op het niveau van de financiële overzichten vanwege hun diepgaande invloed op een aantal beweringen en identificeerbaar zijn met specifieke beweringen, is van de ac- countant vereist om rekening houden met die risico's bij het inschatten van het inherente risico voor risico's op een afwijking van materieel belang op het niveau van beweringen. Overwegingen specifiek voor entiteiten in de publieke sector

• ISA 330 requires controls that address significant risks to be tested in the current period (when the auditor intends to rely on the operating effectiveness of such controls) and substantive procedures to be planned and performed that are specifically responsive to the identified significant risk.52 • ISA 330 requires the auditor to obtain more persuasive audit evidence the higher the auditor's assessment of risk.53 • ISA 260 (Revised) requires communicating with those charged with governance about the significant risks identified by the auditor.54 • ISA 701 requires the auditor to take into account significant risks when determining those matters that required significant auditor attention, which are matters that may be key audit matters.55 • Timely review of audit documentation by the engagement partner at the appropriate stages during the audit allows significant matters, including significant risks, to be resolved on a timely basis to the engagement partner's satisfaction on or before the date of the auditor's report.56 • ISA 600 requires more involvement by the group engagement partner if the significant risk relates to a component in a group audit and for the group engagement team to direct the work required at the component by the component auditor.57 Determining significant risks A219. In determining significant risks, the auditor may first identify those assessed risks of material misstatement that have been assessed higher on the spectrum of inherent risk to form the basis for considering which risks may be close to the upper end. Being close to the upper end of the spectrum of inherent risk will differ from entity to entity, and will not necessarily be the same for an entity period on period. It may depend on the nature and circumstances of the entity for which the risk is being assessed. A220. The determination of which of the assessed risks of material misstatement are close to the upper end of the spectrum of inherent risk, and are therefore significant risks, is a matter of professional judgment, unless the risk is of a type specified to be treated as a significant risk in accordance with the requirements of another ISA. ISA 240 provides further requirements and guidance in relation to the identification and assessment of the risks of material misstatement due to fraud.58 A221. The auditor also takes into the account the relative effects of inherent risk factors when assessing inherent risk. The lower the effect of inherent risk factors, the lower the assessed risk is likely to be. Risks of material misstatement that may be assessed as having higher inherent risk and may therefore be determined to be a significant risk, may arise from matters such as the following: • Transactions for which there are multiple acceptable accounting treatments such that subjectivity is involved. • Accounting estimates that have high estimation uncertainty or complex models. • Complexity in data collection and processing to support account balances. • Account balances or quantitative disclosures that involve complex calculations. • Accounting principles that may be subject to differing interpretation. • Changes in the entity's business that involve changes in accounting, for example, mergers and acquisitions. Risks for Which Substantive Procedures Alone Do Not Provide Sufficient Appropriate Audit Evidence (Ref: Para. 33) Why risks for which substantive procedures alone do not provide sufficient appropriate audit evidence are required to be identified	A217 Bij het uitoefenen van professionele oordeelsvorming over de inschatting van het risico op een afwijking van materieel belang, kunnen accountants in de publieke sector rekening houden met de complexiteit van de voorschriften en leidraden, en met de risico's op niet-naleving van auto- riteiten. Significante risico's (Zie Par. 32) Waarom significante risico's worden bepaald en de implicaties voor de controle A218 De bepaling van significante risico's stelt de accountant in staat om meer aandacht te besteden aan die risico's die zich aan de bovengrens van het spectrum van inherent risico bevinden door de uitvoering van bepaalde vereiste manieren van inspelen, waaronder: • Interne beheersingsmaatregelen die inspelen op significante risico's, moeten worden ge- identificeerd in overeenstemming met paragraaf 26(a)(i), met een vereiste om te evalueren of de interne beheersingsmaatregel effectief is opgezet en geïmplementeerd in overeen- stemming met paragraaf 26(d); • Standaard 330 vereist dat interne beheersingsmaatregelen die inspelen op significante risi- co's, worden getoetst in de huidige verslagperiode (wanneer de accountant voornemens is te steunen op de effectieve werking van dergelijke interne beheersingsmaatregelen) en om gegevensgerichte werkzaamheden te plannen en uit te voeren die specifiek inspelen op het geïdentificeerde significante risico;53 • Standaard 330 vereist dat de accountant meer overtuigende controle-informatie verkrijgt naarmate de risico-inschatting van de accountant hoger is;54 • Standaard 260 vereist communicatie met de met governance belaste personen over de significante risico's geïdentificeerd door de accountant;55 • Standaard 701 vereist dat de accountant bij het bepalen van significante risico's rekening houdt met die aangelegenheden die significante aandacht van de accountant vereisen, het- geen aangelegenheden zijn die kernpunten van controle kunnen zijn;56 • Tijdige beoordeling van controledocumentatie door de opdrachtpartner in de geschikte fa- sen tijdens de controle staat toe dat significante aangelegenheden, waaronder significante risico's, tijdig kunnen worden opgelost tot tevredenheid van de opdrachtpartner op of vóór de datum van de controleverklaring;57 • Standaard 600 vereist meer betrokkenheid van de opdrachtpartner op groepsniveau als het significante risico betrekking heeft op een groepsonderdeel in een groepscontrole en voor het opdrachtteam op groepsniveau om het vereiste werk bij het groepsonderdeel door de accountant van het groepsonderdeel te sturen.58 Bepaling van significante risico's A219 Bij het bepalen van significante risico's kan de accountant eerst die ingeschatte risico's op een afwijking van materieel belang identificeren die hoger zijn ingeschat op het spectrum van inhe- rent risico om de basis te vormen voor het overwegen welke risico's dicht bij de bovengrens kunnen liggen. Dit zal verschillen van entiteit tot entiteit, en zal niet noodzakelijk hetzelfde zijn voor een entiteit van verslagperiode op verslagperiode. Het kan afhankelijk zijn van de aard en omstandigheden van de entiteit waarvoor het risico ingeschat wordt. A220 De bepaling van welke van de ingeschatte risico's op een afwijking van materieel belang dicht bij de bovengrens van het spectrum van inherent risico ligt, en daarom significante risico's zijn, is een kwestie van professionele oordeelsvorming, tenzij het risico moet worden behandeld als een significant risico in overeenstemming met de vereisten van een andere Standaard. Stan- daard 240

	biedt verdere vereisten en leidraden met betrekking tot de identificatie en inschatting van de risico's op een afwijking van materieel belang als gevolg van fraude.59 A221 De accountant houdt bij de inschatting ook rekening met de relatieve effecten van inherente risicofactoren bij het inschatten van inherent risico. Hoe lager het effect van inherente risicofac- toren, hoe lager het ingeschatte risico waarschijnlijk zal zijn. Risico's op een afwijking van ma- terieel belang kunnen zijn ingeschat als een hoger inherent risico en daarom mogelijk als een significant risico worden beschouwd, als gevolg van de volgende aangelegenheden: • transacties waarvoor meerdere aanvaardbare wijzen van administratieve verwerking be- staan, zodat sprake is van subjectiviteit; • schattingen met een hoge schattingsonzekerheid of complexe modellen; • complexiteit in gegevensverzameling en -verwerking ter ondersteuning van rekeningsaldi; • rekeningsaldi of kwantitatieve toelichtingen met complexe berekeningen; • verslaggevingsprincipes die mogelijk op verschillende manieren worden geïnterpreteerd; • wijzigingen in de bedrijfsactiviteiten van de entiteit die veranderingen in de administratieve verwerking met zich meebrengen, bijvoorbeeld fusies en overnames. Risico's waarvoor gegevensgerichte werkzaamheden alleen geen voldoende en geschikte controle-informatie verschaffen (Zie Par. 33) Waarom risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie verschaffen, moeten worden geïdentificeerd A222 Vanwege de aard van een risico op een afwijking van materieel belang en de interne beheer- singsactiviteiten die inspelen op dat risico, is in sommige omstandigheden het toetsen van de effectieve werking van interne beheersingsmaatregelen de enige manier om voldoende en ge- schikte controle-informatie te verkrijgen. Dienovereenkomstig is er een vereiste voor de ac- countant om dergelijke risico's te identificeren vanwege de implicaties voor de opzet en de uit- voering van verdere controlewerkzaamheden in overeenstemming met Standaard 330 om in te spelen op risico's op een afwijking van materieel belang op het niveau van beweringen. A223 Paragraaf 26(a)(iii) vereist ook de identificatie van interne beheersingsmaatregelen die inspe- len op risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie kunnen verschaffen omdat van de accountant wordt vereist, in overeen- stemming met Standaard 330,60om dergelijke toetsingen van interne beheersingsmaatregelen op te zetten en uit te voeren. Bepalen van risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie bieden A224 Waar routinematige zakelijke transacties worden onderworpen aan hoog geautomatiseerde verwerking met weinig of geen handmatige interventie, is het niet altijd mogelijk om alleen ge- gevensgerichte werkzaamheden uit te voeren met betrekking tot het risico. Dit kan het geval zijn in omstandigheden waarin een significante hoeveelheid informatie van een entiteit alleen in elektronische vorm is geïnitieerd, vastgelegd, verwerkt of gerapporteerd zoals in een informa- tiesysteem dat een hoge mate van integratie in al de IT-applicaties bevat. In dergelijke geval- len: • Is controle-informatie mogelijk alleen beschikbaar in elektronische vorm en is de toerei- kendheid en geschiktheid ervan gewoonlijk afhankelijk van de effectiviteit van interne be- heersingsmaatregelen met betrekking tot de nauwkeurigheid en volledigheid ervan;
A222. Due to the nature of a risk of material misstatement, and the control activities that address that risk, in some circumstances the only way to obtain sufficient appropriate audit evidence is to test the operating effectiveness of controls. Accordingly, there is a requirement for the auditor to identify any such risks because of the implications for the design and performance of further audit procedures in accordance with ISA 330 to address risks of material misstatement at the assertion level. 58 ISA 240, paragraphs 26–28 A223. Paragraph 26(a)(iii) also requires the identification of controls that address risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence because the auditor is required, in accordance with ISA 330,59 to design and perform tests of such controls. Determining risks for which substantive procedures alone do not provide sufficient appropriate audit evidence A224. Where routine business transactions are subject to highly automated processing with little or no manual intervention, it may not be possible to perform only substantive procedures in relation to the risk. This may be the case in circumstances where a significant amount of an entity's information is initiated, recorded, processed, or reported only in electronic form such as in an information system that involves a high degree of integration across its IT applications. In such cases: • Audit evidence may be available only in electronic form, and its sufficiency and appropriateness usually depend on the effectiveness of controls over its accuracy and completeness. • The potential for improper initiation or alteration of information to occur and not be detected may be greater if appropriate controls are not operating effectively. A225. ISA 540 (Revised) provides further guidance related to accounting estimates about risks for which substantive procedures alone do not provide sufficient appropriate audit evidence.60 In relation to accounting estimates this may not be limited to automated processing, but may also be applicable to complex models. Assessing Control Risk (Ref: Para. 34) A226. The auditor's plans to test the operating effectiveness of controls is based on the expectation that controls are operating effectively, and this will form the basis of the auditor's assessment of control risk. The initial expectation of the operating effectiveness of controls is based on the auditor's evaluation of the design, and the determination of implementation, of the identified controls in the control activities component. Once the auditor has tested the operating effectiveness of the controls in accordance with ISA 330, the auditor will be able to confirm the initial expectation about the operating effectiveness of controls. If the controls are not operating	

effectively as expected, then the auditor will need to revise the control risk assessment in accordance with paragraph 37. 59 ISA 330, paragraph 8 60 ISA 540 (Revised), paragraphs A87–A89 A227. The auditor's assessment of control risk may be performed in different ways depending on preferred audit techniques or methodologies, and may be expressed in different ways. A228. If the auditor plans to test the operating effectiveness of controls, it may be necessary to test a combination of controls to confirm the auditor's expectation that the controls are operating effectively. The auditor may plan to test both direct and indirect controls, including general IT controls, and, if so, take into account the combined expected effect of the controls when assessing control risk. To the extent that the control to be tested does not fully address the assessed inherent risk , the auditor determines the implications on the design of further audit procedures to reduce audit risk to an acceptably low level. A229. When the auditor plans to test the operating effectiveness of an automated control, the auditor may also plan to test the operating effectiveness of the relevant general IT controls that support the continued functioning of that automated control to address the risks arising from the use of IT, and to provide a basis for the auditor's expectation that the automated control operated effectively throughout the period. When the auditor expects related general IT controls to be ineffective, this determination may affect the auditor's assessment of control risk at the assertion level and the auditor's further audit procedures may need to include substantive procedures to address the applicable risks arising from the use of IT. Further guidance about the procedures that the auditor may perform in these circumstances is provided in ISA 330.61 Evaluating the Audit Evidence Obtained from the Risk Assessment Procedures (Ref: Para 35) Why the Auditor Evaluates the Audit Evidence from the Risk Assessment Procedures A230. Audit evidence obtained from performing risk assessment procedures provides the basis for the identification and assessment of the risks of material misstatement. This provides the basis for the auditor's design of the nature, timing and extent of further audit procedures responsive to the assessed risks of material misstatement, at the assertion level, in accordance with ISA 330. Accordingly, the audit evidence obtained from the risk assessment procedures provides a basis for the identification and assessment of risks of material misstatement whether due to fraud or error, at the financial statement and assertion levels. The Evaluation of the Audit Evidence A231. Audit evidence from risk assessment procedures comprises both information that supports and corroborates management's assertions, and any information that contradicts such assertions.62	• Is de mogelijkheid dat onjuiste informatie tot stand wordt gebracht of gewijzigd zonder dat de fout wordt gedetecteerd mogelijk groter als geschikte interne beheersingsmaatregelen niet effectief werken. A225 Standaard 540 biedt verdere leidraden met betrekking tot schattingen van risico's waarvoor ge- gevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie bie- den.61 In relatie tot schattingen is dit mogelijk niet beperkt tot geautomatiseerde verwerking, maar kan dit ook van toepassing zijn op complexe modellen. Inschatting van het interne beheersingsrisico (Zie Par. 34) A226 De plannen van de accountant om de effectieve werking van interne beheersingsmaatregelen te toetsen zijn gebaseerd op de verwachting dat interne beheersingsmaatregelen effectief wer- ken en dit zal de basis vormen voor de inschatting door de accountant van het interne beheer- singsrisico. De aanvankelijke verwachting van de effectieve werking van interne beheersings- maatregelen is gebaseerd op de evaluatie van de accountant van de opzet en het vaststellen van de implementatie van de geïdentificeerde interne beheersingsmaatregelen in de compo- nent 'interne beheersingsactiviteiten'. Zodra de accountant de effectieve werking van de in- terne beheersingsmaatregelen heeft getoetst in overeenstemming met Standaard 330 zal de accountant de aanvankelijke verwachting over de effectieve werking van interne beheersings- maatregelen kunnen bevestigen. Als de interne beheersingsmaatregelen niet effectief werken zoals verwacht, dan moet de accountant de controle van het interne beheersingsrisico herzien in overeenstemming met paragraaf 37. A227 De inschatting door de accountant van het interne beheersingsrisico kan op verschillende ma- nieren worden uitgevoerd, afhankelijk van de voorkeurscontroletechnieken of -methodologieën, en kan op verschillende manieren worden uitgedrukt. A228 Als de accountant van plan is om de effectieve werking van interne beheersingsmaatregelen te toetsen, kan het nodig zijn om een combinatie van interne beheersingsmaatregelen te toetsen om de verwachting van de accountant dat de interne beheersingsmaatregelen effectief werken te bevestigen. De accountant kan van plan zijn om zowel directe als indirecte interne beheer- singsmaatregelen te toetsen, met inbegrip van general IT-controls, en, zo ja, bij de inschatting van het interne beheersingsrisico rekening te houden met het gecombineerde verwachte effect van de interne beheersingsmaatregelen. Naar de mate waarin de te toetsen interne beheer- singsmaatregel niet volledig inspeelt op het ingeschatte inherente risico, zal de accountant de implicaties bepalen voor de opzet van verdere controlewerkzaamheden om het controlerisico terug te brengen tot een aanvaardbaar laag niveau. A229 Wanneer de accountant van plan is om de effectieve werking van een geautomatiseerde in- terne beheersingsmaatregel te toetsen, kan de accountant ook van plan zijn om de effectieve werking van de relevante general IT-controls die de voortdurende werking van die geautomati- seerde controle ondersteunen, te toetsen om in te spelen op de risico's die voortkomen uit het gebruik van IT en een basis vormen voor de verwachting van de accountant dat de geautoma- tiseerde interne beheersingsmaatregel effectief werkte gedurende de verslagperiode. Wanneer de accountant verwacht dat gerelateerde general IT-controls niet effectief zijn, kan deze bepa- ling van invloed zijn op de inschatting van de accountant van het interne beheersingsrisico op het niveau van beweringen en moeten de verdere controlewerkzaamheden van de accountant mogelijk gegevensgerichte werkzaamheden omvatten om in te spelen op de van toepassing zijnde risico's die voortkomen uit het gebruik van IT. Verdere leidraden over de werkzaamhe- den die de accountant kan uitvoeren in deze omstandigheden zijn vermeld in Standaard 330.62

Professional Skepticism
A232. In evaluating the audit evidence from the risk assessment procedures, the auditor considers whether sufficient understanding about the entity and its environment, the applicable financial reporting framework and the entity's system of internal control has been obtained to be able to identify the risks

of material misstatement, as well as whether there is any evidence that is contradictory that may indicate a risk of material misstatement.

Classes of Transactions, Account Balances and Disclosures that Are Not Significant, but Which Are Material (Ref: Para. 36)
A233. As explained in ISA 320,63 materiality and audit risk are considered when identifying and assessing the risks of material misstatement in classes of transactions, account balances and disclosures. The auditor's determination of materiality is a matter of professional judgment, and is affected by the auditor's perception of the financial information needs of users of the financial statements.64 For the purpose of this ISA and paragraph 18 of ISA 330, classes of transactions, account balances or disclosures are material if omitting, misstating or obscuring information about them could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements as a whole.
A234. There may be classes of transactions, account balances or disclosures that are material but have not been determined to be significant classes of transactions, account balances or disclosures (i.e., there are no relevant assertions identified).
A235. Audit procedures to address classes of transactions, account balances or disclosures that are material but are not determined to be significant are addressed in ISA 330.65 When a class of transactions, account balance or disclosure is determined to be significant as required by paragraph 29, the class of transactions, account balance or disclosure is also a material class of transactions, account balance or disclosure for the purposes of paragraph 18 of ISA 330.

Revision of Risk Assessment (Ref: Para. 37)
A236. During the audit, new or other information may come to the auditor's attention that differs significantly from the information on which the risk assessment was based.

63 ISA 320, paragraph A1
64 ISA 320, paragraph 4
65 ISA 330, paragraph 18

Evalueren van de controle-informatie verkregen uit de risico-inschattingswerkzaamheden
(Zie Par. 35)
Waarom de accountant de controle-informatie evalueert op basis van de risico-inschattingswerk-zaamheden

A230 Controle-informatie verkregen bij het uitvoeren van risico-inschattingswerkzaamheden vormt de basis voor de identificatie en inschatting van de risico's op een afwijking van materieel be- lang. Dit vormt de basis voor de opzet van de accountant van de aard, timing en omvang van verdere controlewerkzaamheden die inspelen op de ingeschatte risico's op een afwijking van materieel belang op het niveau van beweringen in overeenstemming met Standaard 330. Dien-overeenkomstig vormt de controle-informatie verkregen uit de risico-inschattingswerkzaamhe- den een basis voor de identificatie en inschatting van risico's op een afwijking van materieel belang als gevolg van fraude of fouten, op het niveau van de financiële overzichten en bewe- ringen.

De evaluatie van de controle-informatie

A231 Controle-informatie uit risico-inschattingswerkzaamheden omvat zowel informatie die de bewe-ringen van het management ondersteunt en bevestigt en alle informatie die dergelijke bewerin- gen tegenspreekt.63

Een professioneel-kritische instelling

A232 Bij het evalueren van de controle-informatie uit de risico-inschattingswerkzaamheden over-weegt de accountant of voldoende inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het interne beheersingssysteem van de enti- teit is verkregen om de risico's op een afwijking van materieel belang te kunnen identificeren, evenals of er enige informatie is die tegenstrijdig is en die kan duiden op een risico op een af- wijking van materieel belang.

Transactiestromen, rekeningsaldi en toelichtingen die niet significant zijn, maar wel van materieel be-lang (Zie Par. 36)
A233 Zoals uitgelegd in Standaard 320, worden64 materialiteit en controlerisico in overweging geno-men bij het identificeren en inschatten van de risico's op een afwijking van materieel belang in transactiestromen, rekeningsaldi en toelichtingen. De bepaling van de materialiteit door de ac-countant is een kwestie van professionele oordeelsvorming en wordt beïnvloed door de per- ceptie van de accountant van de financiële informatiebehoeften van gebruikers van de financi- ele overzichten.65 Voor de doelstelling van deze Standaard en paragraaf 18 van Standaard 330, zijn transactiestromen, rekeningsaldi of toelichtingen van materieel belang als het wegla- ten, onjuist weergeven of verhullen van informatie daarover naar verwachting redelijkerwijs de economische beslissingen van gebruikers zou kunnen beïnvloeden gebaseerd op de financiële overzichten als geheel.

A234 Er kunnen transactiestromen, rekeningsaldi of toelichtingen zijn die van materieel belang zijn maar die niet zijn vastgesteld als significante transactiestromen, rekeningsaldi of toelichtingen (d.w.z. er zijn geen relevante beweringen geïdentificeerd).

A235 Controlewerkzaamheden om transactiestromen, rekeningsaldi of toelichtingen te behandelen die van materieel belang zijn, maar waarvan niet is vastgesteld dat ze significant zijn, worden behandeld in Standaard 330.66 Wanneer een transactiestroom, rekeningsaldo of toelichting wordt

	geacht significant te zijn zoals vereist door paragraaf 29, is de transactiestroom, reke- ningsaldo of toelichting ook een transactiestroom, rekeningsaldo of toelichting van materieel belang voor de doeleinden van paragraaf 18 van Standaard 330. Herziening van de risico-inschatting (Zie Par. 37) A236 Tijdens de controle kan nieuwe of andere informatie onder de aandacht van de accountant ko- men die significant verschilt van de informatie waarop de risico-inschatting was gebaseerd.
Documentation (Ref: Para. 38) A237. For recurring audits, certain documentation may be carried forward, updated as necessary to reflect changes in the entity's business or processes. A238. ISA 230 notes that, among other considerations, although there may be no single way in which the auditor's exercise of professional skepticism is documented, the audit documentation may nevertheless provide evidence of the auditor's exercise of professional skepticism.66 For example, when the audit evidence obtained from risk assessment procedures includes evidence that both corroborates and contradicts management's assertions, the documentation may include how the auditor evaluated that evidence, including the professional judgments made in evaluating whether the audit evidence provides an appropriate basis for the auditor's identification and assessment of the risks of material misstatement. Examples of other requirements in this ISA for which documentation may provide evidence of the exercise of professional skepticism by the auditor include: • Paragraph 13, which requires the auditor to design and perform risk assessment procedures in a manner that is not biased towards obtaining audit evidence that may corroborate the existence of risks or towards excluding audit evidence that may contradict the existence of risks; • Paragraph 17, which requires a discussion among key engagement team members of the application of the applicable financial reporting framework and the susceptibility of the entity's financial statements to material misstatement; • Paragraphs 19(b) and 20, which require the auditor to obtain an understanding of the reasons for any changes to the entity's accounting policies and to evaluate whether the entity's accounting policies are appropriate and consistent with the applicable financial reporting framework; • Paragraphs 21(b), 22(b), 23(b), 24(c), 25(c), 26(d) and 27, which require the auditor to evaluate, based on the required understanding obtained, whether the components of the entity's system of internal control are appropriate to the entity's circumstances considering the nature and complexity of the entity, and to determine whether one of more control deficiencies have been identified; • Paragraph 35, which requires the auditor to take into account all audit evidence obtained from the risk assessment procedures, whether corroborative or contradictory to assertions made by management, and to evaluate whether the audit evidence obtained from the risk assessment procedures provides an appropriate basis for the identification and assessment of the risks of material misstatement; and • Paragraph 36, which requires the auditor to evaluate, when applicable, whether the auditor's determination that there are no risks of material misstatement for a material class of transactions, account balance or disclosure remains appropriate. 66 ISA 230, paragraph A7	63 Standaard 500, paragraaf A1. 64 Standaard 320, paragraaf A1. 65 Standaard 320, lid 4. 66 Standaard 330, paragraaf 18.
Scalability A239. The manner in which the requirements of paragraph 38 are documented is for the auditor to determine using professional judgment. A240. More detailed documentation, that is sufficient to enable an experienced auditor, having no previous experience with the audit, to understand the nature, timing and extent of the audit procedures performed, may be required to support the rationale for difficult judgments made. A241. For the audits of less complex entities, the form and extent of documentation may be simple and relatively brief. The form and extent of the auditor's documentation is influenced by the nature, size and complexity of the	Documentatie (Zie Par. 38) A237 Voor doorlopende controles kan bepaalde documentatie worden overgedragen, zo nodig bijge- werkt om veranderingen in de activiteiten of processen van de entiteit te weerspiegelen. A238 Standaard 230 geeft aan dat, hoewel er misschien geen standaardmanier is waarop de uitoefe- ning van een professioneel-kritische instelling door de accountant is gedocumenteerd, de con- troledocumentatie niettemin informatie kan leveren over de uitoefening van een professioneel- kritische instelling van de accountant.67 Bijvoorbeeld wanneer de controle-informatie verkregen uit risico-inschattingswerkzaamheden informatie omvat die zowel beweringen van het manage- ment bevestigt als tegenspreekt, kan de documentatie omvatten hoe de accountant evalueerde dat informatie inclusief de professionele oordeelsvorming bij het evalueren of de controle-infor- matie een geschikte basis biedt voor de identificatie en inschatting van de risico's op een afwij- king van materieel belang door de accountant. Voorbeelden van andere vereisten in deze Standaard waarvoor documentatie informatie kan leveren over de uitoefening van een professi- oneel-kritische instelling door de accountant zijn onder andere: • Paragraaf 13, die van de accountant vereist dat de accountant risico-inschattingswerk- zaamheden opzet en uitvoert op een manier die niet tendeert naar het verkrijgen van con- trole-informatie die het bestaan van risico's kan bevestigen of om controle-informatie uit te sluiten die het bestaan van risico's kan tegenspreken; • Paragraaf 17, die een bespreking vereist onder de kernleden van het opdrachtteam van de toepassing van het van toepassing zijnde stelsel inzake financiële verslaggeving en de vat- baarheid van financiële overzichten van de entiteit voor afwijkingen van materieel belang; • Paragraaf 19 (b) en 20, die van de accountant vereisen dat de accountant inzicht heeft in de redenen voor eventuele wijzigingen in de grondslagen voor de financiële verslaggeving van de entiteit en om te evalueren of de grondslagen voor de financiële verslaggeving van de entiteit geschikt en consistent zijn met het van toepassing zijnde stelsel inzake financi- ele verslaggeving; • Paragrafen 21(b), 22(b), 23(b), 24(c), 25(c), 26(d) en 27, die vereisen dat de accountant evalueert, op basis van de vereiste verkregen inzichten, of de componenten van het sys- teem van interne beheersing van de entiteit passend zijn bij de omstandigheden van de en- titeit, gezien de aard en complexiteit van de entiteit en om te bepalen of een of meer tekort- komingen in de interne beheersing zijn geïdentificeerd; • Paragraaf 35, die vereist dat de accountant rekening houdt met alle controle-informatie ver- kregen uit de risico-inschattingswerkzaamheden, hetzij bevestigend of in tegenspraak met beweringen van management en om te evalueren of de controle-informatie verkregen uit de risico-

entity and its system of internal control, availability of information from the entity and the audit methodology and technology used in the course of the audit. It is not necessary to document the entirety of the auditor's understanding of the entity and matters related to it. Key elements67 of understanding documented by the auditor may include those on which the auditor based the assessment of the risks of material misstatement. However, the auditor is not required to document every inherent risk factor that was taken into account in identifying and assessing the risks of material misstatement at the assertion level.	inschattingswerkzaamheden een passende basis biedt voor de identificatie en in- schatting van de risico's op een afwijking van materieel belang; en • Paragraaf 36, die vereist dat de accountant, indien van toepassing, evalueert of bepaling van de accountant dat er geen risico's zijn op een afwijking van materieel belang zijn voor een materiële transactiestroom, rekeningsaldo of toelichting passend blijft. Schaalbaarheid A239 De accountant bepaalt met behulp van professionele oordeelsvorming de manier waarop de vereisten van paragraaf 38 zijn gedocumenteerd. A240 Meer gedetailleerde documentatie, die voldoende is om een ervaren accountant, die geen eer- dere ervaring heeft met de controle in staat te stellen om inzicht te krijgen in de aard, timing en omvang van de uitgevoerde controlewerkzaamheden, kan nodig zijn om de beweegreden voor moeilijke oordeelsvormingen te ondersteunen. A241 Voor de interne beheersingsmaatregelen van minder complexe entiteiten kan de vorm en om- vang van documentatie eenvoudig en relatief kort zijn. De vorm en omvang van de documenta- tie van de accountant wordt beïnvloed door de aard, omvang en complexiteit van de entiteit en het systeem van interne beheersing, beschikbaarheid van informatie van de entiteit en de con- trolemethodologie en -technologie die tijdens de controle is gebruikt. Het is niet nodig om het geheel van het inzicht van de accountant in de entiteit en aangelegenheden die daarmee ver- band houden te documenteren. Kernelementen68 van inzicht die door de accountant zijn gedo- cumenteerd, kunnen diegenen omvatten waarop de accountant de inschatting van de risico's op een afwijking van materieel belang heeft gebaseerd. De accountant is echter niet verplicht elke inherente risicofactor waarmee rekening is gehouden bij het identificeren en inschatten van de risico's op een afwijking van materieel belang op het niveau van beweringen te docu- menteren.

Bijlage 2 - Detailopmerkingen bijlage 5 en 6 bij Standaard 315

Appendix 5	
Entiti's mixAppendix 5 (Ref: Para. 25(a), 26(b)–(c), A94, A166–A172) Considerations for Understanding Information Technology (IT) This appendix provides further matters that the auditor may consider in understanding the entity's use of IT in its system of internal control. Understanding the Entity's Use of Information Technology in the Components of the Entity's System of Internal Control 1. An entity's system of internal control contains manual elements and automated elements (i.e., manual and automated controls and other resources used in the entity's system of internal control). An entity's mix of manual and automated elements varies with the nature and complexity of the entity's use of IT. An entity's use of IT affects the manner in which the information relevant to the preparation of the financial statements in accordance with the applicable financial reporting framework is processed, stored and communicated, and therefore affects the manner in which the entity's system of internal control is designed and implemented. Each component of the entity's system of internal control may use some extent of IT. Generally, IT benefits an entity's system of internal control by enabling an entity to: • Consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data; • Enhance the timeliness, availability and accuracy of information; • Facilitate the additional analysis of information; • Enhance the ability to monitor the performance of the entity's activities and its policies and procedures; • Reduce the risk that controls will be circumvented; and • Enhance the ability to achieve effective segregation of duties by implementing security controls in IT applications, databases and operating systems. 2. The characteristics of manual or automated elements are relevant to the auditor's identification and assessment of the risks of material misstatement, and further audit procedures based thereon. Automated controls may be more reliable than manual controls because they cannot be as easily bypassed, ignored, or overridden, and they are also less prone to simple errors and mistakes. Automated controls may be more effective than manual controls in the following circumstances: • High volume of recurring transactions, or in situations where errors that can be anticipated or predicted can be prevented, or detected and corrected, through automation. • Controls where the specific ways to perform the control can be adequately designed and automated. Understanding the Entity's Use of Information Technology in the Information System (Ref: Para. 25(a)) 3. The entity's information system may include the use of manual and automated elements, which also affect the manner in which transactions are initiated, recorded, processed, and reported. In particular, procedures to initiate, record, process and report transactions may be enforced through the IT applications used by the entity, and how the entity has configured those	Bijlage 5 (Zie Par. Zie Par. 25(a), 26(b)-(c), A94, A166 – A172) Overwegingen voor het verwerven van inzicht in informatietechnologie (IT) Deze bijlage geeft verdere aangelegenheden die de accountant kan overwegen bij het verwerven van inzicht in het gebruik van IT door de entiteit in het systeem van interne beheersing. Inzicht in het gebruik van informatietechnologie door de entiteit in de componenten van het systeem van interne beheersing van de entiteit 1 Het interne beheersingssysteem van een entiteit bevat handmatige elementen en geautomati- seerde elementen (dat wil zeggen, handmatige en geautomatiseerde interne beheersingsmaatre- gelen en andere middelen die worden gebruikt in het interne beheersingssysteem van de enti- teit). De combinatie van handmatige en geautomatiseerde elementen in een entiteit is afhankelijk van de aard en complexiteit van het gebruik van IT door de entiteit. Het gebruik van IT door een entiteit beïnvloedt de manier waarop de informatie die relevant is voor het opstellen van de finan- ciële overzichten in overeenstemming met het van toepassing zijnde stelsel inzake financiële ver- slaggeving, wordt verwerkt, opgeslagen en gecommuniceerd en beïnvloedt daarom de manier waarop het interne beheersingssysteem van de entiteit is opgezet en geïmplementeerd. Elke component van het interne beheersingssysteem van de entiteit kan een zekere mate van IT ge- bruiken. Over het algemeen komt IT het interne beheersingssysteem van een entiteit ten goede omdat het een entiteit in staat stelt om: • Vooraf gedefinieerde bedrijfsregels consistent toe te passen en complexe berekeningen uit te voeren bij de verwerking van grote hoeveelheden transacties of gegevens; • De tijdigheid, beschikbaarheid en nauwkeurigheid van informatie te verbeteren; • Aanvullende analyse van informatie te vergemakkelijken; • De uitvoering van de activiteiten en de beleidslijnen en procedures beter te monitoren; • Het risico te beperken dat interne beheersingsmaatregelen worden omzeild; en • De mogelijkheid te verbeteren om effectieve functiescheiding te bereiken door beveiligings-maatregelen te implementeren in IT-applicaties, databases en besturingssystemen. 2 De kenmerken van handmatige of geautomatiseerde elementen zijn relevant voor de identificatie en inschatting van de risico's op een afwijking van materieel belang door de accountant en ver- dere daarop gebaseerde controlewerkzaamheden. Geautomatiseerde interne beheersingsmaat- regelen kunnen betrouwbaarder zijn dan handmatige interne beheersingsmaatregelen omdat ze niet zo gemakkelijk kunnen worden omzeild, genegeerd of doorbroken en ze zijn ook minder ge- voelig voor eenvoudige fouten en vergissingen. Geautomatiseerde interne beheersingsmaatrege- len kunnen in de volgende omstandigheden effectiever zijn dan handmatige interne beheersings- maatregelen: • Grote aantallen van terugkerende transacties, of in situaties waarin te voorziene of te voor-spellen fouten kunnen worden voorkomen, of gedetecteerd en gecorrigeerd door automatise-ring; • Interne beheersingsmaatregelen waarbij de specifieke manieren voor de uitvoering daarvan adequaat kunnen worden opgezet en geautomatiseerd. Inzicht in het gebruik van informatietechnologie door de entiteit in het informatiesysteem (Zie Par. 25(a)) 3 Het informatiesysteem van de entiteit kan het gebruik van handmatige en geautomatiseerde ele- menten omvatten, die ook invloed hebben op de manier waarop transacties worden geïnitieerd, vastgelegd, verwerkt en gerapporteerd. Met name procedures voor

applications. In addition, records in the form of digital information may replace or supplement records in the form of paper documents.

4. In obtaining an understanding of the IT environment relevant to the flows of transactions and information processing in the information system, the auditor gathers information about the nature and characteristics of the IT applications used, as well as the supporting IT infrastructure and IT. The following table includes examples of matters that the auditor may consider in obtaining the understanding of the IT environment and includes examples of typical characteristics of IT environments based on the complexity of IT applications used in the entity's information system. However, such characteristics are directional and may differ depending on the nature of the specific IT applications in use by an entity.

het initiëren, registreren, ver- werken en rapporteren van transacties kunnen via de door de entiteit gebruikte IT-applicaties worden afgedwongen en de manier waarop de entiteit die applicaties heeft geconfigureerd. Daar- naast, kunnen digitale informatie vastleggingen papieren documenten vastleggingen vervangen of aanvullen.

4 Bij het verwerven van inzicht in de IT-omgeving die relevant is voor de transactiestromen en in- formatieverwerking in het informatiesysteem, verzamelt de accountant informatie over de aard en kenmerken van de gebruikte IT-applicaties, evenals de ondersteunende IT-infrastructuur. De vol- gende tabel bevat voorbeelden van aangelegenheden die de accountant kan overwegen bij het verwerven van inzicht in de IT-omgeving en bevat voorbeelden van typische kenmerken van IT- omgevingen op basis van de complexiteit van IT-applicaties die worden gebruikt in het informatie- systeem van de entiteit. Dergelijke kenmerken zijn echter richtinggevend en kunnen verschillen, afhankelijk van de aard van de specifieke IT-applicaties die door een entiteit worden gebruikt.

	Examples of typical characteristics of:		
	Non-complex commercial software	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g., ERP systems)
Matters related to extent of automation and use of data:			
• The extent of automated procedures for processing, and the complexity of those procedures, including, whether there is highly automated, paperless processing.	N/A	N/A	Extensive and often complex automated procedures
• The extent of the entity's reliance on system-generated reports in the processing of information.	Simple automated report logic	Simple relevant automated report logic	Complex automated report logic; Report-writer software
• How data is input (i.e., manual input, customer or vendor input, or file load).	Manual data inputs	Small number of data inputs or simple interfaces	Large number of data inputs or complex interfaces
	Examples of typical characteristics of:		
	Non-complex commercial software	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g., ERP systems)
• How IT facilitates communication between applications, databases or other aspects of the IT environment, internally and externally, as appropriate, through system interfaces.	No automated interfaces (manual inputs only)	Small number of data inputs or simple interfaces	Large number of data inputs or complex interfaces

Aangelegenheden die verband houden met de mate van automatisering en gebruik van gege- vens:

Niet complexe com- merciële software

Middelgrote en redelijk complexe commerciële software of IT- applicaties

Grote of complexe IT- applicaties (bijvoorbeeld ERP systemen)

• De mate van geauto- matiseerde procedu- res voor verwerking en de complexiteit van die procedures, inclusief of er sprake is van hoog geauto- matiseerde, papier- loze verwerking.

Nvt Nvt Uitgebreide en vaak com- plexe geautomatiseerde procedures

• De mate van steunen op systeem gegene- reerde rapporten door de entiteit in de ver- werking van informa- tie
• Hoe gegevens wor- den ingevoerd (d.w.z. handmatige invoer, klant- of leveranciers- invoer of het laden van bestanden).
• Hoe IT communicatie tussen applicaties, databases of andere aspecten van de IT- omgeving faciliteert, intern en extern, in- dien passend, door systeem interfaces.
• Het aantal en de com- plexiteit van gege- vens in digitale vorm verwerkt door het in- formatiesysteem, in- clusief of administra- tieve vastleggingen of andere informatie is opgeslagen in digitale vorm en de locatie van opgeslagen ge- gevens.

Aangelegenheden die verband houden met de IT-applicaties en IT infra- structuur:

Eenvoudige geautoma- tiseerde rapport logica

Handmatige gegevens- invoer

Geen geautomati- seerde interfaces (al- leen handmatige in- voer)

Kleine aantallen gege- vens of eenvoudige ge- gevens die handmatig kunnen worden geveri- fieerd; Gegevens lokaal beschikbaar

• The volume and complexity of data in digital form being processed by the information system, including whether accounting records or other information are stored in digital form and the location of stored data.	Low volume of data or simple data that is able to be verified manually; Data available locally	Low volume of data or simple data	Large volume of data or complex data; Data warehouses;[76] Use of internal or external IT service providers (e.g., third-party storage or hosting of data)
Matters related to the IT applications and IT infrastructure:			
• The type of application (e.g., a commercial application with little or no customization, or a highly-customized or highly-integrated application that may have been purchased	Purchased application with little or no customization	Purchased application or simple legacy or low-end ERP applications with little or no customization	Custom developed applications or more complex ERPs with significant customization
	Examples of typical characteristics of:		
	Non-complex commercial software	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g., ERP systems)
and customized, or developed in-house).			
• The complexity of the nature of the IT applications and the underlying IT infrastructure.	Small, simple laptop or client server-based solution	Mature and stable mainframe, small or simple client server, software as a service cloud	Complex mainframe, large or complex client server, web-facing, infrastructure as a service cloud
• Whether there is third-party hosting or outsourcing of IT.	If outsourced, competent, mature, proven provider (e.g., cloud provider)	If outsourced, competent, mature, proven provider (e.g., cloud provider)	Competent, mature proven provider for certain applications and new or start-up provider for others
• Whether the entity is using emerging technologies that affect its financial reporting.	No use of emerging technologies	Limited use of emerging technologies in some applications	Mixed use of emerging technologies across platforms

Eenvoudige relevante ge- automatiseerde rapport logica

Kleine aantallen gege- vensinvoer of eenvoudige interfaces

Kleine aantallen gege- vensinvoer of eenvoudige interfaces

Kleine aantallen gege- vens of eenvoudige gege- vens

Complexe geautomati- seerde rapport logica; rap- port generator software

Grote aantallen gegevens- invoer of complexe interfa- ces

Grote aantallen gegevens- invoer of complexe interfa- ces

Grote aantallen gegevens of complexe gegevens; Data warehouses;77 Ge- bruik van interne of ex- terne IT-service providers (bijv. opslag van derden of hosting van gegevens)

• Het type applicatie (bijv. een commerci- ele toepassing met weinig of geen maat- werk, of een sterk aangepaste of in hoge mate geïnte- greerde applicatie die mogelijk is gekocht en aangepast, of in eigen huis ontwikkeld).	Gekochte applicatie met weinig of geen maatwerk	Gekochte applicatie of eenvoudige verouderde of *low-end* ERP-applicaties met weinig of geen maatwerk	Op maat ontwikkelde ap- plicaties of complexere ERP's met significant maatwerk
• De complexiteit van de aard van de IT-applicaties en de on- derliggende IT infra- structuur.	Kleine, eenvoudige lap- top of client server ge- baseerde oplossing	Volwassen en stabiel mainframe, kleine of een- voudige client server, software als een service cloud	Complex mainframe, grote of complexe client server, web-gerichte, infrastruc- tuur als een service cloud
• Of er sprake is van *third party hosting* of uitbesteding van IT.	Indien uitbesteed, com- petente, volwassen, be- wezen leverancier (bijv. cloud provider)	Indien uitbesteed, compe- tente, volwassen, bewe- zen provider (bijv. cloud provider)	Competente, volwassen bewezen leverancier voor bepaalde applicaties en nieuwe of startup provider voor anderen
• Of de entiteit nieuwe technologieën ge- bruikt die invloed heb- ben op de financiële verslaggeving.	Geen gebruik van nieuwe technologieën	Beperkt gebruik van nieuwe technologieën in sommige applicaties	Gemengd gebruik van nieuwe technologieën over platforms heen

Matters related to IT processes:			
• The personnel involved in maintaining the IT environment (the number and skill level of the IT support resources that manage security and changes to the IT environment).	Few personnel with limited IT knowledge to process vendor upgrades and manage access	Limited personnel with IT skills / dedicated to IT	Dedicated IT departments with skilled personnel, including programming skills
• The complexity of processes to manage access rights.	Single individual with administrative access manages access rights	Few individuals with administrative access manage access rights	Complex processes managed by IT department for access rights
• The complexity of the security over the IT	Simple on-premise access with no	Some web-based applications with	Multiple platforms with web-based

Aangelegenheden gerelateerd aan IT processen:			
• Het personeel betrokken bij het onderhouden van de IT-omgeving (het aantal en vaardigheidsniveau van de IT ondersteunende middelen die de beveiliging beheren en veranderingen in de IT-omgeving).	Weinig personeel met beperkte IT-kennis om leveranciers upgrades te verwerken en toegang te beheren	Beperkt personeel met IT-vaardigheden / gewijd aan IT	Toegewijde IT afdelingen met bekwaam personeel, inclusief programmeervaardigheden
• De complexiteit van processen om toegangsrechten te beheren.	Een enkel persoon met beheerderstoegang beheert toegangsrechten	Beperkt aantal personen met beheerderstoegang beheren toegangsrechten	Complexe processen beheerd door IT afdeling voor toegangsrechten
• De complexiteit van de beveiliging over de IT-omgeving, inclusief kwetsbaarheid van de IT-applicaties, databases, en andere aspecten van de IT-omgeving voor cyberrisico's, vooral wanneer er web-gebaseerde transacties zijn of transacties waarbij externe interfaces betrokken zijn.	Eenvoudige toegang ter plaatse zonder externe web-gerichte elementen	Sommige web-gebaseerde applicaties met voornamelijk eenvoudige, rol-gebaseerde beveiliging	Meerdere platforms met web-gebaseerde toegang en complexe beveiligingsmodellen
• Of programma wijzigingen zijn gemaakt in de manier waarop informatie wordt verwerkt en de omvang van zulke veranderingen tijdens de verslagperiode.	Commerciële software zonder geïnstalleerde broncode	Enkele commerciële applicaties zonder broncode en andere volwassen applicaties met een klein aantal of eenvoudige veranderingen; traditionele levenscyclus van systeemontwikkeling	Nieuw of groot aantal of complexe veranderingen, verschillende ontwikkelingscycli elk jaar.
• De mate van wijziging binnen de IT-omgeving (bijvoorbeeld nieuwe aspecten van de IT-omgeving of significante wijzigingen in de IT-applicaties of de onderliggende IT infrastructuur).	Wijzigingen beperkt tot versie-upgrades van commerciële software	Wijzigingen bestaan uit commerciële software upgrades, ERP versie-upgrades, of verbeteringen aan verouderde systemen	Nieuwe, groot aantal of complexe veranderingen, verschillende ontwikkelingscycli elk jaar, forse ERP-aanpassing
• Of er een significante dataconversie was tijdens de verslagperiode en, indien dit het geval is, de aard en significantie van de aangebrachte wijzigingen en hoe de conversie was ondernomen.	Software-upgrades geleverd door de leverancier; Geen gegevensconversie kenmerken voor upgrade	Kleine versie upgrades voor commerciële software applicaties met beperkte gegevens conversie	Aanzienlijke versie upgrade, nieuwe release, platform verandering

	Examples of typical characteristics of:		
	Non-complex commercial software	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g., ERP systems)
environment, including vulnerability of the IT applications, databases, and other aspects of the IT environment to cyber risks, particularly when there are web-based transactions or transactions involving external interfaces.	external web-facing elements	primarily simple, role-based security	access and complex security models

	• Whether program changes have been made to the manner in which information is processed, and the extent of such changes during the period.	Commercial software with no source code installed	Some commercial applications with no source code and other mature applications with a small number or simple changes; traditional systems development lifecycle	New or large number or complex changes, several development cycles each year		
	• The extent of change within the IT environment (e.g., new aspects of the IT environment or significant changes in the IT applications or the underlying IT infrastructure).	Changes limited to version upgrades of commercial software	Changes consist of commercial software upgrades, ERP version upgrades, or legacy enhancements	New or large number or complex changes, several development cycles each year, heavy ERP customization		
	• Whether there was a major data conversion during the period and, if so, the nature and significance of the changes made, and how the conversion was undertaken.	Software upgrades provided by vendor; No data conversion features for upgrade	Minor version upgrades for commercial software applications with limited data being converted	Major version upgrade, new release, platform change		

Emerging Technologies 5. Entities may use emerging technologies (e.g., blockchain, robotics or artificial intelligence) because such technologies may present specific opportunities to increase operational efficiencies or enhance financial reporting. When emerging technologies are used in the entity's information system relevant to the preparation of the financial statements, the auditor may include such technologies in the identification of IT applications and other aspects of the IT environment that are subject to risks arising from the use of IT. While emerging technologies may be seen to be more sophisticated or more complex compared to existing technologies, the auditor's responsibilities in relation to IT applications and identified general IT controls in accordance with paragraph 26(b)–(c) remain unchanged. Scalability 6. Obtaining an understanding of the entity's IT environment may be more easily accomplished for a less complex entity that uses commercial software and when the entity does not have access to the source code to make any program changes. Such entities may not have dedicated IT resources but may have a person assigned in an administrator role for the purpose of granting employee access or installing vendor-provided updates to the IT applications. Specific matters that the auditor may consider in understanding the nature of a commercial accounting software package, which may be the single IT application used by a less complex entity in its information system, may include: • The extent to which the software is well established and has a reputation for reliability;	Nieuwe technologieën 5 Entiteiten kunnen nieuwe technologieën gebruiken (bijv. blockchain, robotica of kunstmatige intel- ligentie) omdat dergelijke technologieën specifieke kansen kunnen bieden om de operationele efficiëntie te verhogen of de financiële verslaggeving te verbeteren. Wanneer nieuwe technolo- gieën gebruikt worden in het informatiesysteem van de entiteit dat relevant is bij het opstellen van de financiële overzichten, kan de accountant dergelijke technologieën opnemen in de identificatie van IT-applicaties en andere aspecten van de IT-omgeving die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT. Terwijl nieuwe technologieën wellicht als geavanceerder of complexer worden beschouwd in vergelijking met bestaande technologieën, blijven de verant- woordelijkheden van de accountant met betrekking tot IT-applicaties en geïdentificeerde general IT controls in overeenstemming met paragraaf 26 (b) - (c) ongewijzigd. Schaalbaarheid 6 Het verwerven van inzicht in de IT-omgeving van de entiteit kan gemakkelijker worden bereikt voor een minder complexe entiteit die commerciële software gebruikt en wanneer de entiteit geen toegang heeft tot de broncode om programmawijzigingen aan te brengen. Dergelijke entiteiten hebben misschien geen specifieke IT-middelen, maar kan een persoon toegewezen hebben in een beheerdersrol met als doel het verlenen van toegang voor werknemers of installeren van door de leverancier geleverde updates voor de IT-applicaties. Specifieke aangelegenheden die de accountant kan overwegen om inzicht te verwerven in de aard van een commercieel boek- houdsoftwarepakket dat de enige IT-applicatie kan zijn die door een minder complexe entiteit in zijn informatiesysteem wordt gebruikt, kunnen omvatten: • De mate waarin de software goed ontwikkeld is is en een reputatie van betrouwbaarheid heeft;

• The extent to which it is possible for the entity to modify the source code of the software to include additional modules (i.e., add-ons) to the base software, or to make direct changes to data; • The nature and extent of modifications that have been made to the software. Although an entity may not be able to modify the source code of the software, many software packages allow for configuration (e.g., setting or amending reporting parameters). These do not usually involve modifications to source code; however, the auditor may consider the extent to which the entity is able to configure the software when considering the completeness and accuracy of information produced by the software that is used as audit evidence; and • The extent to which data related to the preparation of the financial statements can be directly accessed (i.e., direct access to the database without using the IT application) and the volume of data that is processed. The greater the volume of data, the more likely the entity may need controls that address maintaining the integrity of the data, which may include general IT controls over unauthorized access and changes to the data.	• De mate waarin het voor de entiteit mogelijk is om de broncode van de software te wijzigen om extra modules (bijv. add-ons) toe te voegen aan de basissoftware, of om directe wijzigin- gen aan gegevens aan te brengen; • De aard en omvang van wijzigingen die in de software zijn aangebracht. Hoewel een entiteit mogelijk niet in staat is om de broncode van de software te wijzigen, laten veel softwarepak- ketten configuratie toe (bijvoorbeeld het instellen of wijzigen van rapportageparameters). Meestal gaat het hier niet om wijzigingen in de broncode; de accountant kan echter overwe- gen in hoeverre de entiteit de software kan configureren wanneer de accountant de volledig- heid en nauwkeurigheid van informatie gegereerd door de software die wordt gebruikt als controle-informatie beschouwt; en • De mate waarin gegevens met betrekking tot het opstellen van de financiële overzichten di- rect kunnen zijn benaderd (d.w.z. directe toegang tot de database zonder de IT-applicatie te gebruiken) en het aantal gegevens dat worden verwerkt. Hoe groter het aantal gegevens, hoe groter de kans dat de entiteit interne beheersingsmaatregelen nodig heeft die betrekking hebben op het handhaven van de integriteit van de gegevens, waaronder general IT-controls met betrekking tot ongeautoriseerde toegang en wijzigingen in de gegevens.
7. Complex IT environments may include highly-customized or highly-integrated IT applications and may therefore require more effort to understand. Financial reporting processes or IT applications may be integrated with other IT applications. Such integration may involve IT applications that are used in the entity's business operations and that provide information to the IT applications relevant to the flows of transactions and information processing in the entity's information system. In such circumstances, certain IT applications used in the entity's business operations may also be relevant to the preparation of the financial statements. Complex IT environments also may require dedicated IT departments that have structured IT processes supported by personnel that have software development and IT environment maintenance skills. In other cases, an entity may use internal or external service providers to manage certain aspects of, or IT processes within, its IT environment (e.g., third-party hosting).	7 Complexe IT-omgevingen kunnen sterk aangepaste of in hoge mate geïntegreerde IT-applicaties omvatten en het kan daarom meer moeite vereisen om deze te begrijpen. Financiële verslagge- vingsprocessen of IT-applicaties kunnen worden geïntegreerd met andere IT-applicaties. Een dergelijke integratie kan betrekking hebben op IT-applicaties die worden gebruikt in de bedrijfsac- tiviteiten van de entiteit en die informatie verstrekken aan de IT-applicaties die relevant zijn voor de transactiestromen en informatieverwerking in het informatiesysteem van de entiteit. In zulke omstandigheden kunnen bepaalde IT-applicaties die worden gebruikt in de bedrijfsactiviteiten van de entiteit ook relevant zijn bij het opstellen van de financiële overzichten. Complexe IT- omgevingen vereisen mogelijk ook specifieke IT-afdelingen met gestructureerde IT-processen, ondersteund door personeel dat vaardigheden heeft op het gebied van software ontwikkeling en onderhoud van de IT-omgeving. In andere gevallen kan een entiteit interne of externe service providers gebruiken om bepaalde aspecten van, of IT-processen in, de IT-omgeving te beheren (bijvoorbeeld hosting door derden).
Identifying IT Applications that are Subject to Risks Arising from the use of IT	Het identificeren van IT-applicaties die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT
8. Through understanding the nature and complexity of the entity's IT environment, including the nature and extent of information processing controls, the auditor may determine which IT applications the entity is relying upon to accurately process and maintain the integrity of financial information. The identification of IT applications on which the entity relies may affect the auditor's decision to test the automated controls within such IT applications, assuming that such automated controls address identified risks of material misstatement. Conversely, if the entity is not relying on an IT application, the automated controls within such IT application are unlikely to be appropriate or sufficiently precise for purposes of operating effectiveness tests. Automated controls that may be identified in accordance with paragraph 26(b) may include, for example, automated calculations or input, processing and output controls, such as a three-way match of a purchase order, vendor shipping document, and vendor invoice. When automated controls are identified by the auditor and the auditor determines through the understanding of the IT environment that the entity is relying on the IT application that includes those automated controls, it may be more likely for the auditor to identify the IT application as one that is subject to risks arising from the use of IT.	8 Door inzicht in de aard en complexiteit van de IT-omgeving van de entiteit, inclusief de aard en omvang van interne beheersingsmaatregelen met betrekking tot informatieverwerking, kan de ac- countant bepalen op welke IT-applicaties de entiteit steunt om de integriteit van financiële infor- matie nauwkeurig te verwerken en te handhaven. De identificatie van IT-applicaties waarop de entiteit steunt, kan van invloed zijn op de beslissing van de accountant om de geautomatiseerde interne beheersingsmaatregelen binnen dergelijke IT-applicaties te toetsen, ervan uitgaande dat dergelijke geautomatiseerde interne beheersingsmaatregelen inspelen op geïdentificeerde risi- co's op een afwijking van materieel belang. Omgekeerd, als de entiteit niet steunt op een IT- applicatie, is het onwaarschijnlijk dat de geautomatiseerde interne beheersingsmaatregelen bin- nen een dergelijke IT-applicatie geschikt of voldoende nauwkeurig zijn ten behoeve van het toet- sen van de effectieve werking. Geautomatiseerde interne beheersingsmaatregelen die kunnen worden geïdentificeerd in overeenstemming met paragraaf 26(b) kunnen bijvoorbeeld geautoma- tiseerde berekeningen of interne beheersingsmaatregelen met betrekking tot invoer, verwerking en uitvoer omvatten, zoals een aansluiting tussen een inkooporder, verzending van een vervoers- document en een leveranciersfactuur. Wanneer geautomatiseerde interne beheersingsmaatrege- len door de accountant worden geïdentificeerd en de accountant bepaalt door het inzicht in de IT- omgeving dat de entiteit steunt op de IT-applicatie die deze geautomatiseerde interne beheer- singsmaatregelen bevat, is het waarschijnlijker dat de accountant de IT-applicatie identificeert als een die onderhevig is aan risico's die voortkomen uit het gebruik van IT.
9. In considering whether the IT applications for which the auditor has identified automated controls are subject to risks arising from the use of IT, the auditor is likely to consider whether,	9 Bij het overwegen of de IT-applicaties waarvoor de accountant geautomatiseerde interne beheer- singsmaatregelen heeft geïdentificeerd, onderhevig zijn aan risico's die voortkomen uit

and the extent to which, the entity may have access to source code that enables management to make program changes to such controls or the IT applications. The extent to which the entity makes program or configuration changes and the extent to which the IT processes over such changes are formalized may also be relevant considerations. The auditor is also likely to consider the risk of inappropriate access or changes to data.	het ge- bruik van IT, zal de accountant waarschijnlijk overwegen of en de mate waarin de entiteit mogelijk toegang heeft tot de broncode waarmee het management programma wijzigingen kan maken in dergelijke interne beheersingsmaatregelen of de IT-applicaties. De mate waarin de entiteit pro- gramma- of configuratiewijzigingen maakt en de mate waarin de IT-processen met betrekking tot dergelijke wijzigingen zijn geformaliseerd, kunnen ook relevante overwegingen zijn. De accoun- tant zal waarschijnlijk ook het risico op ongepaste toegang tot of wijzigingen in gegevens overwe- gen.
10. System-generated reports that the auditor may intend to use as audit evidence may include, for example, a trade receivable aging report or an inventory valuation report. For such reports, the auditor may obtain audit evidence about the completeness and accuracy of the reports by substantively testing the inputs and outputs of the report. In other cases, the auditor may plan to test the operating effectiveness of the controls over the preparation and maintenance of the report, in which case the IT application from which it is produced is likely to be subject to risks arising from the use of IT. In addition to testing the completeness and accuracy of the report, the auditor may plan to test the operating effectiveness of general IT controls that address risks related to inappropriate or unauthorized program changes to, or data changes in, the report.	10 Door het systeem gegenereerde rapporten die de accountant voornemens is te gebruiken als controle-informatie, kunnen bijvoorbeeld een rapport over de ouderdom van debiteuren of een rapport over de waardering van voorraden omvatten. Voor dergelijke rapporten kan de accoun- tant controle-informatie verkrijgen over de volledigheid en nauwkeurigheid van de rapporten door gegevensgerichte werkzaamheden op de inputs en outputs van het rapport. In andere gevallen kan de accountant van plan zijn de effectieve werking van de interne beheersingsmaatregelen met betrekking tot het opstellen en het onderhoud van het rapport te toetsen, in welk geval de IT- applicatie waaruit het is gegeneerd, waarschijnlijk onderhevig is aan risico's die voortkomen uit het gebruik van IT. Naast het toetsen van de volledigheid en nauwkeurigheid van het rapport, kan de accountant van plan zijn om de effectieve werking van general IT controls die inspelen op risi- co's die verband houden met ongepaste of ongeautoriseerde programmawijzigingen of gege- venswijzigingen in het rapport, te toetsen.
11. Some IT applications may include report-writing functionality within them while some entities may also utilize separate report-writing applications (i.e., report-writers). In such cases, the auditor may need to determine the sources of system-generated reports (i.e., the application that prepares the report and the data sources used by the report) to determine the IT applications subject to risks arising from the use of IT.	11 Sommige IT-applicaties kunnen een functie voor het schrijven van rapporten bevatten, terwijl sommige entiteiten ook afzonderlijke applicaties voor het schrijven van rapporten (d.w.z. rapport- generators) kunnen gebruiken. In dergelijke gevallen kan het nodig zijn dat de accountant de bronnen van door het systeem gegenereerde rapporten bepaalt (d.w.z. de applicatie die het rap- port opstelt en de gegevensbronnen die door het rapport worden gebruikt) om de IT-applicaties te bepalen die aan risico's onderhevig zijn die voortkomen uit het gebruik van IT.
12. The data sources used by IT applications may be databases that, for example, can only be accessed through the IT application or by IT personnel with database administration privileges. In other cases, the data source may be a data warehouse that may itself be considered to be an IT application subject to risks arising from the use of IT.	12 De gegevensbronnen die door IT-applicaties worden gebruikt, kunnen databases zijn die bijvoor- beeld alleen toegankelijk zijn via de IT-applicatie of door IT-personeel met database beheerrech- ten. In andere gevallen kan de gegevensbron een datawarehouse zijn dat zelf kan worden be- schouwd als een IT-applicatie onderhevig aan risico's die voortkomen uit het gebruik van IT.
13. The auditor may have identified a risk for which substantive procedures alone are not sufficient because of the entity's use of highly-automated and paperless processing of transactions, which may involve multiple integrated IT applications. In such circumstances, the controls identified by the auditor are likely to include automated controls. Further, the entity may be relying on general IT controls to maintain the integrity of the transactions processed and other information used in processing. In such cases, the IT applications involved in the processing and the storage of the information are likely subject to risks arising from the use of IT.	13 De accountant kan een risico geïdentificeerd hebben waarvoor gegevensgerichte werkzaamhe- den alleen niet voldoende zijn vanwege het gebruik van in hoge mate geautomatiseerde en pa- pierloze verwerking van transacties door de entiteit, wat betrekking kan hebben op meerdere ge- integreerde IT-applicaties. In dergelijke omstandigheden omvatten de door de accountant ge- identificeerde interne beheersingsmaatregelen waarschijnlijk geautomatiseerde interne beheer- singsmaatregelen. Verder kan de entiteit steunen op general IT-controls om de integriteit van de verwerkte transacties en andere informatie die gebruikt is in de verwerking, te handhaven. In der- gelijke gevallen zijn de IT-applicaties die betrokken zijn bij de verwerking en de opslag van de in- formatie waarschijnlijk onderhevig aan risico's die voortkomen uit het gebruik van IT.
End-User Computing	Computergebruik door eindgebruikers
14. Although audit evidence may also come in the form of system-generated output that is used in a calculation performed in an end-user computing tool (e.g., spreadsheet software or simple databases), such tools are not typically identified as IT applications in the context of paragraph 26(b). Designing and implementing controls around access and change to end-user computing tools may be challenging, and such controls are rarely equivalent to, or as effective as, general IT controls. Rather, the auditor may consider a combination of information processing controls, taking into account the purpose and complexity of the end-user computing involved, such as:	14 Hoewel controle-informatie ook kan bestaan uit door het systeem gegenereerde output die wordt gebruikt in een berekening uitgevoerd in een computerhulpmiddel voor eindgebruikers (bijv. spreadsheetsoftware of eenvoudige databases), worden dergelijke hulpmiddelen doorgaans niet geïdentificeerd als IT-applicaties in de context van paragraaf 26(b). Het opzetten en implemente- ren van interne beheersingsmaatregelen rond toegang en wijziging van computerhulpmiddelen voor eindgebruikers kan uitdagend zijn en dergelijke interne beheersingsmaatregelen zijn zelden gelijk aan of even effectief als general IT controls. In plaats daarvan kan de accountant een com- binatie van beheersingsmaatregelen met betrekking tot

• Information processing controls over the initiation and processing of the source data, including relevant automated or interface controls to the point from which the data is extracted (i.e., the data warehouse); • Controls to check that the logic is functioning as intended, for example, controls which 'prove' the extraction of data, such as reconciling the report to the data from which it was derived, comparing the individual data from the report to the source and vice versa, and controls which check the formulas or macros; or • Use of validation software tools, which systematically check formulas or macros, such as spreadsheet integrity tools.	informatieverwerking overwegen, reke- ning houdend met het doel en de complexiteit van het betreffende computergebruik door eindge- bruikers, zoals: • Interne beheersingsmaatregelen met betrekking tot informatieverwerking inzake de initiatie en verwerking van de brongegevens, inclusief relevante geautomatiseerde interne beheer- singsmaatregelen of via interfaces tot het punt van waaruit de gegevens worden geëxtra- heerd (dat wil zeggen het datawarehouse); • Interne beheersingsmaatregelen om te controleren of de logica werkt zoals bedoeld, bijvoor- beeld interne beheersingsmaatregelen die het extraheren van gegevens 'bewijzen', zoals het aansluiten van het rapport op de gegevens waarvan het is afgeleid, het vergelijken van de individuele gegevens uit het rapport met de bron en vice versa, en interne beheersingsmaat- regelen die de formules of macro's controleren; of • Gebruik van validatie softwarehulpmiddelen, die formules of macro's controleren, zoals spreadsheet integriteitshulpmiddelen.
Scalability 15. The entity's ability to maintain the integrity of information stored and processed in the information system may vary based on the complexity and volume of the related transactions and other information. The greater the complexity and volume of data that supports a significant class of transactions, account balance or disclosure, the less likely it may become for the entity to maintain integrity of that information through information processing controls alone (e.g., input and output controls or review controls). It also becomes less likely that the auditor will be able to obtain audit evidence about the completeness and accuracy of such information through substantive testing alone when such information is used as audit evidence. In some circumstances, when volume and complexity of transactions are lower, management may have an information processing control that is sufficient to verify the accuracy and completeness of the data (e.g., individual sales orders processed and billed may be reconciled to the hard copy originally entered into the IT application). When the entity relies on general IT controls to maintain the integrity of certain information used by IT applications, the auditor may determine that the IT applications that maintain that information are subject to risks arising from the use of IT.	Schaalbaarheid 15 De mogelijkheid van de entiteit om de integriteit te handhaven van de informatie die in het infor- matiesysteem is opgeslagen en verwerkt, kan variëren op basis van de complexiteit en het aantal gerelateerde transacties en andere informatie. Hoe groter de complexiteit en het aantal gegevens dat een significante transactiestroom, rekeningsaldo of toelichting ondersteunt, hoe minder waar- schijnlijk het wordt dat de entiteit de integriteit van die informatie handhaaft via interne beheer- singsmaatregelen met betrekking tot informatieverwerking alleen (bijvoorbeeld interne beheer- singsmaatregelen met betrekking tot input en output of interne beheersingsmaatregelen voor be- oordeling). Het wordt ook minder waarschijnlijk dat de accountant controle-informatie zal kunnen verkrijgen over de volledigheid en nauwkeurigheid van dergelijke informatie door gegevensge- richte werkzaamheden alleen wanneer dergelijke informatie wordt gebruikt als controle-informa- tie. In sommige omstandigheden, wanneer het aantal en de complexiteit van transacties lager is, kan het management een interne beheersingsmaatregel met betrekking tot informatieverwerking hebben die voldoende is om de nauwkeurigheid en volledigheid van de gegevens te verifiëren (bijv. individueel verwerkte en gefactureerde verkooporders kunnen worden aangesloten met de hard copy die oorspronkelijk in de IT-applicatie is ingevoerd). Wanneer de entiteit steunt op gene- ral IT-controls om de integriteit van bepaalde informatie die door IT-applicaties wordt gebruikt, te handhaven, kan de accountant bepalen dat de IT-applicaties die die informatie onderhouden, on- derhevig zijn aan risico's die voortkomen uit het gebruik van IT.

Example characteristics of an IT application that is likely not subject to risks arising from IT	Example characteristics of an IT application that is likely subject to risks arising from IT
• Standalone applications. • The volume of data (transactions) is not significant. • The application's functionality is not complex. • Each transaction is supported by original hard copy documentation.	• Applications are interfaced. • The volume of data (transactions) is significant. • The application's functionality is complex as: – The application automatically initiates transactions; and – There are a variety of complex calculations underlying automated entries.

Voorbeeldkenmerken van een IT-applicatie die waarschijnlijk niet onderhevig is aan risico's die voortkomen uit IT	**Voorbeeldkenmerken van een IT-applicatie die waarschijnlijk onderhevig is aan risico's die voortkomen uit IT**
• Zelfstandige applicaties; • De hoeveelheid gegevens (transacties) is niet sig- nificant; • De functionaliteit van de applicatie is niet complex; • Elke transactie wordt ondersteund door originele *hard copy* documentatie.	• Applicaties zijn gekoppeld; • De hoeveelheid gegevens (transacties) is signifi- cant; • De functionaliteit van de applicatie is complex zo- als: o de toepassing initieert automatisch transac- ties; en o er zijn verschillende complexe berekeningen met onderliggende geautomatiseerde invoer.

	IT application is likely not subject to risks arising from IT because: • The volume of data is not significant and therefore management is not relying upon general IT controls to process or maintain the data. • Management does not rely on automated controls or other automated functionality. The auditor has not identified automated controls in accordance with paragraph 26(a). • Although management uses system-generated reports in their controls, it does not rely on these reports. Instead, it reconciles the reports back to the hard copy documentation and verifies the calculations in the reports. • The auditor will directly test information produced by the entity used as audit evidence.	IT application is likely subject to risks arising from IT because: • Management relies on an application system to process or maintain data as the volume of data is significant. • Management relies upon the application system to perform certain automated controls that the auditor has also identified.		De IT-applicatie is waarschijnlijk niet onderhevig aan risico's op IT omdat: • De hoeveelheid gegevens niet significant is en het management daarom niet steunt op *general IT controls* om de gegevens te verwerken of te onderhouden; • Het management niet op geautomatiseerde interne beheersingsmaatregelen of een andere geautomatiseerde functionaliteit steunt. De accountant heeft geen geautomatiseerde interne beheersingsmaatregelen geïdentificeerd in overeenstemming met paragraaf 26(a); • Hoewel het management systeem-gegenereerde rapporten gebruikt in hun interne beheersingsmaatregelen, het niet op deze rapporten steunt. In plaats daarvan, sluit het de rapporten aan met de *hard copy* documentatie en verifieert het de berekeningen in de rapporten; • De accountant informatie die wordt gegenereerd door de entiteit die als controle-informatie wordt gebruikt direct zal toetsen.	De IT-applicatie is waarschijnlijk onderhevig aan risico's op IT omdat: • Het management steunt op een applicatie systeem om gegevens te verwerken of te onderhouden als de hoeveelheid gegevens significant is; • Het management steunt op het applicatie systeem om bepaalde geautomatiseerde interne beheersingsmaatregelen uit te voeren die de accountant ook heeft geïdentificeerd.
Other Aspects of the IT Environment that Are Subject to Risks Arising from the Use of IT 16. When the auditor identifies IT applications that are subject to risks arising from the use of IT, other aspects of the IT environment are also typically subject to risks arising from the use of IT. The IT infrastructure includes the databases, operating system, and network. Databases store the data used by IT applications and may consist of many interrelated data tables. Data in databases may also be accessed directly through database management systems by IT or other personnel with database administration privileges. The operating system is responsible for managing communications between hardware, IT applications, and other software used in the network. As such, IT applications and databases may be directly accessed through the operating system. A network is used in the IT infrastructure to transmit data and to share information, resources and services through a common communications link. The network also typically establishes a layer of logical security (enabled through the operating system) for access to the underlying resources. 17. When IT applications are identified by the auditor to be subject to risks arising from IT, the database(s) that stores the data processed by an identified IT application is typically also identified. Similarly, because an IT application's ability to operate is often dependent on the operating system and IT applications and databases may be directly accessed from the operating system, the operating system is typically subject to risks arising from the use of IT. The network may be identified when it is a central point of access to the identified IT applications and related databases or when an IT application interacts with vendors or external parties through the internet, or when web-facing IT applications are identified by the auditor. Identifying Risks Arising from the Use of IT and General IT Controls 18. Examples of risks arising from the use of IT include risks related to inappropriate reliance on IT applications that are inaccurately processing data, processing inaccurate data, or both, such as			Andere aspecten van de IT-omgeving die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT 16 Wanneer de accountant IT-applicaties identificeert die onderhevig zijn aan risico's die voortko- men uit het gebruik van IT, zijn andere aspecten van de IT-omgeving doorgaans ook onderhevig aan risico's die voortkomen uit het gebruik van IT. De IT infrastructuur omvat de databases, het besturingssysteem en het netwerk. Databases slaan de gegevens die gebruikt worden door IT- applicaties op en kunnen bestaan uit vele onderling verbonden gegevenstabellen. Gegevens in databases kunnen ook rechtstreeks toegankelijk zijn via database managementsystemen door IT of ander personeel met database beheerrechten. Het besturingssysteem is verantwoordelijk voor het beheer van de communicatie tussen hardware, IT-applicaties en andere software die in het netwerk wordt gebruikt. Als zodanig kunnen IT-applicaties en databases direct toegankelijk zijn via het besturingssysteem. Een netwerk wordt gebruikt in de IT infrastructuur om gegevens te verzenden en informatie, middelen en diensten te delen via een gemeenschappelijke communi- catielink. Het netwerk brengt doorgaans ook een logische beveiligingslaag tot stand (ingescha- keld via het besturingssysteem) voor toegang tot de onderliggende middelen. 17 Wanneer IT-applicaties door de accountant worden geïdentificeerd als onderhevig aan risico's die voortkomen uit IT, word(t)(en) de database(s) die de gegevens opslaat(n) die worden verwerkt door een geïdentificeerde IT-applicatie, meestal ook geïdentificeerd. Omdat de mogelijkheid voor de werking van een IT-applicatie vaak afhankelijk is van het besturingssysteem en de IT- applicaties en databases direct toegankelijk kunnen zijn vanuit het besturingssysteem, is het be- sturingssysteem op een gelijke manier meestal onderhevig aan risico's die voortkomen uit het ge- bruik van IT. Het netwerk kan worden geïdentificeerd wanneer het een centraal toegangspunt is voor de geïdentificeerde IT-applicaties en gerelateerde databases of wanneer een IT applicatie interactie heeft met leveranciers of externe partijen via het internet, of wanneer web-gerichte IT- applicaties worden geïdentificeerd door de accountant. Identificeren van risico's die voortkomen uit het gebruik van IT en general IT-controls 18 Voorbeelden van risico's die voortkomen uit het gebruik van IT omvatten risico's die verband hou- den met een ongepast steunen op IT-applicaties die onnauwkeurig gegevens verwerken, on- nauwkeurige gegevens verwerken, of beide, zoals:		

• Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions, or inaccurate recording of transactions. Particular risks may arise where multiple users access a common database. • The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties. • Unauthorized changes to data in master files. • Unauthorized changes to IT applications or other aspects of the IT environment. • Failure to make necessary changes to IT applications or other aspects of the IT environment. • Inappropriate manual intervention. • Potential loss of data or inability to access data as required.	• Onbevoegde toegang tot gegevens die kan leiden tot vernietiging van gegevens of onge- paste wijzigingen in gegevens, inclusief het opnemen van ongeautoriseerde of niet-be- staande transacties of het onjuist vastleggen van transacties. Bijzondere risico's kunnen ont- staan wanneer meerdere gebruikers toegang hebben tot een gemeenschappelijke database; • De mogelijkheid voor IT-personeel om toegangsrechten te verkrijgen die verder gaan dan no- dig is om hun toegewezen taken uit te voeren waardoor functiescheiding wordt doorbroken. • Onbevoegde wijzigingen in gegevens in hoofdbestanden; • Onbevoegde wijzigingen in IT-applicaties of andere aspecten van de IT-omgeving; • Het niet aanbrengen van noodzakelijke wijzigingen in IT-applicaties of andere aspecten van de IT-omgeving; • Ongepaste handmatige interventie; • Potentieel verlies van gegevens of onmogelijkheid om toegang te krijgen tot gegevens zoals vereist.
19. The auditor’s consideration of unauthorized access may include risks related to unauthorized access by internal or external parties (often referred to as cybersecurity risks). Such risks may not necessarily affect financial reporting, as an entity’s IT environment may also include IT applications and related data that address operational or compliance needs. It is important to note that cyber incidents usually first occur through the perimeter and internal network layers, which tend to be further removed from the IT application, database and operating systems that affect the preparation of the financial statements. Accordingly, if information about a security breach has been identified, the auditor ordinarily considers the extent to which such a breach had the potential to affect financial reporting. If financial reporting may be affected, the auditor may decide to understand, and test the related controls to determine the possible impact or scope of potential misstatements in the financial statements or may determine that the entity has provided adequate disclosures in relation to such security breach.	19 De overweging van de accountant van onbevoegde toegang kan risico's met betrekking tot onbe- voegde toegang omvatten door interne of externe partijen (vaak aangeduid als cybersecurity-risi- co's). Dergelijke risico's hoeven niet noodzakelijkerwijs invloed te hebben op de financiële ver- slaggeving, aangezien de IT-omgeving van een entiteit ook IT-applicaties en aanverwante gege- vens kan omvatten die betrekking hebben op operationele of nalevingsbehoeften. Het is belang- rijk op te merken dat cyberincidenten meestal eerst voorkomen via het datacenter en interne net- werklagen, die de neiging hebben verder verwijderd te zijn van de IT-applicatie, database en be- sturingssystemen die van invloed zijn op het opstellen van de financiële overzichten. Dienover- eenkomstig, als informatie over een inbreuk op de beveiliging is geïdentificeerd, overweegt de accountant gewoonlijk in hoeverre een dergelijke inbreuk op de beveiliging de financiële verslag- geving zou kunnen beïnvloeden. Als de financiële verslaggeving hierdoor kan worden beïnvloed, kan de accountant besluiten inzicht te verwerven in de interne beheersingsmaatregelen en deze te toetsen om de mogelijke impact of reikwijdte van mogelijke afwijkingen in de financiële over- zichten te bepalen of kan de accountant bepalen dat de entiteit voldoende toelichting heeft ver- strekt over een dergelijke inbreuk op de beveiliging.
20. In addition, laws and regulations that may have a direct or indirect effect on the entity’s financial statements may include data protection legislation. Considering an entity’s compliance with such laws or regulations, in accordance with ISA 250 (Revised),77 may involve understanding the entity’s IT processes and general IT controls that the entity has implemented to address the relevant laws or regulations.	20 Wet- en regelgeving die een direct of indirect effect op de financiële overzichten van de entiteit heeft, kan bovendien gegevensbeschermingswetgeving omvatten. Overweging van de naleving van dergelijke wet- of regelgeving door een entiteit, in overeenstemming met Standaard 250 ,78 kan inzicht in de IT processen van de entiteit en general IT controls die de entiteit heeft geïmple- menteerd om de relevante wet- of regelgeving te adresseren, omvatten.
21. General IT controls are implemented to address risks arising from the use of IT. Accordingly, the auditor uses the understanding obtained about the identified IT applications and other aspects of the IT environment and the applicable risks arising from the use of IT in determining the general IT controls to identify. In some cases, an entity may use common IT processes across its IT environment or across certain IT applications, in which case common risks arising from the use of IT and common general IT controls may be identified.	21 General IT-controls worden geïmplementeerd om in te spelen op risico's die voortkomen uit het gebruik van IT. Dienovereenkomstig gebruikt de accountant het verkregen inzicht in de geïdentifi- ceerde IT-applicaties en andere aspecten van de IT-omgeving en de van toepassing zijnde risi- co's die voortkomen uit het gebruik van IT bij het bepalen van de te identificeren general IT con- trols. In sommige gevallen kan een entiteit gemeenschappelijke IT-processen rondom de IT- omgeving of tussen bepaalde IT-applicaties gebruiken, in welk geval gemeenschappelijke risico's die voortkomen uit het gebruik van IT en gemeenschappelijke general IT controls kunnen worden geïdentificeerd.
22. In general, a greater number of general IT controls related to IT applications and databases are likely to be identified than for other aspects of the IT environment. This is because these aspects are the most closely concerned with the information processing and storage of information in the entity’s information system. In identifying general IT controls, the auditor may consider controls over actions of both end users and of the entity’s IT personnel or IT service providers.	22 In het algemeen kan waarschijnlijk een groter aantal general IT controls met betrekking tot IT- applicaties en databases worden geïdentificeerd dan voor andere aspecten van de IT-omgeving. Dit komt omdat deze aspecten het meest betrokken zijn bij de informatieverwerking en opslag van informatie in het informatiesysteem van de entiteit. Bij het identificeren van general IT con- trols kan de accountant de interne beheersing van handelingen van zowel eindgebruikers als van het IT-personeel van de entiteit of IT-serviceproviders overwegen.
23. Appendix 6 provides further explanation of the nature of the general IT controls typically implemented for different aspects of the IT environment. In addition, examples of general IT controls for different IT processes are provided.	23 Bijlage 6 geeft een nadere toelichting op de aard van de general IT controls doorgaans geïmple- menteerd voor verschillende aspecten van de IT-omgeving. Daarnaast worden voorbeelden van general IT controls voor verschillende IT-processen gegeven.

Appendix 6 (Ref: Para. 25(c)(ii), A173–A174) This appendix provides further matters that the auditor may consider in understanding general IT controls. 1. The nature of the general IT controls typically implemented for each of the aspects of the IT environment: (a) Applications General IT controls at the IT application layer will correlate to the nature and extent of application functionality and the access paths allowed in the technology. For example, more controls will be relevant for highly-integrated IT applications with complex security options than a legacy IT application supporting a small number of account balances with access methods only through transactions. (b) Database General IT controls at the database layer typically address risks arising from the use of IT related to unauthorized updates to financial reporting information in the database through direct database access or execution of a script or program. (c) Operating system General IT controls at the operating system layer typically address risks arising from the use of IT related to administrative access, which can facilitate the override of other controls. This includes actions such as compromising other user's credentials, adding new, unauthorized users, loading malware or executing scripts or other unauthorized programs. (d) Network General IT controls at the network layer typically address risks arising from the use of IT related to network segmentation, remote access, and authentication. Network controls may be relevant when an entity has web-facing applications used in financial reporting. Network controls are also may be relevant when the entity has significant business partner relationships or third-party outsourcing, which may increase data transmissions and the need for remote access. 2. Examples of general IT controls that may exist, organized by IT process include: (a) Process to manage access: o Authentication Controls that ensure a user accessing the IT application or other aspect of the IT environment is using the user's own log-in credentials (i.e., the user is not using another user's credentials). o Authorization Controls that allow users to access the information necessary for their job responsibilities and nothing further, which facilitates appropriate segregation of duties. o Provisioning Controls to authorize new users and modifications to existing users' access privileges. o Deprovisioning Controls to remove user access upon termination or transfer. o Privileged access Controls over administrative or powerful users' access. o User access reviews Controls to recertify or evaluate user access for ongoing authorization over time. o Security configuration controls Each technology generally has key configuration settings that help restrict access to the environment. o Physical access	Bijlage 6 (Zie Par. 25(c)(ii), A173 – A174) Overwegingen voor het verwerven van inzicht in general IT controls Deze bijlage bevat verdere aangelegenheden die de accountant kan overwegen bij het verwerven van inzicht in general IT controls. 1 De aard van de general IT controls die doorgaans worden geïmplementeerd voor elk aspect van de IT-omgeving: a Applicaties General IT-controls op de IT-applicatielaag hangen samen met de aard en omvang van appli- catiefunctionaliteit en de toegangspaden die zijn toegestaan in de technologie. Bijvoorbeeld meer interne beheersingsmaatregelen zullen relevant zijn voor in hoge mate geïntegreerde IT-applicaties met complexe beveiligingsopties dan een verouderde IT-applicatie die een klein aantal rekeningsaldi ondersteunt met uitsluitend wachtwoordbeveiliging. b Database General IT-controls op de databaselaag spelen normaliter in op de risico's die voortkomen uit het gebruik van IT gerelateerd aan ongeautoriseerde updates van financiële verslaggevings-informatie in de database via directe toegang tot de database of uitvoering van een script of programma. c Besturingssysteem General IT-controls op de laag van het besturingssysteem spelen doorgaans in op risico's die voortkomen uit het gebruik van IT met betrekking tot beheerderstoegang, dat het doorbreken van andere interne beheersingsmaatregelen mogelijk kan maken. Dit omvat handelingen zo- als het in gevaar brengen van de inloggegevens van andere gebruikers, het toevoegen van nieuwe, ongeautoriseerde gebruikers, laden van malware of uitvoeren van scripts of andere ongeautoriseerde programma's. d Netwerk General IT-controls op de netwerklaag spelen doorgaans in op risico's die voortkomen uit het gebruik van IT gerelateerd aan netwerksegmentatie, toegang op afstand en authenticatie. Netwerk beheersmaatregelen kunnen relevant zijn wanneer een entiteit web-gerichte applica- ties heeft die worden gebruikt voor financiële verslaggeving. Netwerk beheersmaatregelen kunnen ook relevant zijn wanneer de entiteit significante relaties met zakenpartners heeft of gebruik maakt van serviceorganisaties, waardoor gegevensoverdracht en de noodzaak van toegang op afstand kunnen toenemen. 2 Voorbeelden van general IT-controls die kunnen bestaan, georganiseerd door IT-processen, om- vatten: a Proces om toegang te beheren: • Authenticatie Interne beheersingsmaatregelen die ervoor zorgen dat een gebruiker die toegang heeft tot de IT-applicatie of een ander aspect van de IT-omgeving, de eigen inloggegevens van de gebruiker gebruikt (dat wil zeggen, de gebruiker geen inloggegevens van andere ge- bruikers gebruikt). • Autorisatie Interne beheersingsmaatregelen die gebruikers toestaan om toegang te hebben tot de informatie die nodig is voor hun taakverantwoordelijkheden en verder niet, wat een pas- sende functiescheiding mogelijk maakt. • Toegang verlenen Interne beheersingsmaatregelen om nieuwe gebruikers en wijzigingen in de toegangs- rechten van bestaande gebruikers te autoriseren. • Toegang opheffen Interne beheersingsmaatregelen om gebruikerstoegang te verwijderen bij beëindiging dienstverband of functieverandering. • Toegangsprivileges Interne beheersingsmaatregelen met betrekking tot de toegang van beheerders of krach- tige gebruikers.

Controls over physical access to the data center and hardware, as such access may be used to override other controls.

(b) Process to manage program or other changes to the IT environment:

o Change management process

Controls over the process to design, program, test and migrate changes to a production (i.e., end user) environment.

o Segregation of duties over change migration

Controls that segregate access to make and migrate changes to a production environment.

o Systems development or acquisition or implementation

Controls over initial IT application development or implementation (or in relation to other aspects of the IT environment).

o Data conversion

Controls over the conversion of data during development, implementation or upgrades to the IT environment.

(c) Process to manage IT operations

o Job scheduling

Controls over access to schedule and initiate jobs or programs that may affect financial reporting.

o Job monitoring

Controls to monitor financial reporting jobs or programs for successful execution.

o Backup and recovery

Controls to ensure backups of financial reporting data occur as planned and that such data is available and able to be accessed for timely recovery in the event of an outage or attack.

o Intrusion detection

Controls to monitor for vulnerabilities and or intrusions in the IT environment.

The table below illustrates examples of general IT controls to address examples of risks arising from the use of IT, including for different IT applications based on their nature.

Process	Risks	Controls	IT Applications		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
Manage Access	User-access privileges:	Management approves the nature	Yes – instead of user access	Yes	Yes

• Beoordelingen van gebruikerstoegang

Interne beheersingsmaatregelen om gebruikerstoegang opnieuw te certificeren of te eva- lueren voor doorlopende autorisatie in de loop van de tijd.

• Interne beheersingsmaatregelen met betrekking tot beveiligingsconfiguratie

Elke technologie heeft over het algemeen belangrijke configuratie-instellingen die helpen de toegang tot haar omgeving te beperken.

• Fysieke toegang

Interne beheersingsmaatregelen met betrekking tot fysieke toegang tot het datacenter en hardware, omdat dergelijke toegang gebruikt kan worden om andere interne beheer- singsmaatregelen te doorbreken.

b Proces om programma- of andere wijzigingen in de IT-omgeving te beheren:

• Change management proces

Interne beheersingsmaatregelen met betrekking tot het ontwikkelen, testen en doorvoe- ren van wijzigingen naar een productie omgeving (d.w.z. eindgebruiker).

• Functiescheiding over wijzigingsmigratie

Interne beheersingsmaatregelen die toegang scheiden om wijzigingen in een productie- omgeving aan te brengen.

• Systeemontwikkeling of acquisitie of implementatie

Interne beheersingsmaatregelen met betrekking tot de initiële ontwikkeling of implemen- tatie van IT-applicaties (of in relatie tot andere aspecten van de IT-omgeving).

• Data conversie

Interne beheersingsmaatregelen met betrekking tot de conversie van gegevens tijdens ontwikkeling, implementatie of upgrades naar de IT-omgeving.

c Proces om IT-activiteiten te beheren

• Taakplanning

Interne beheersingsmaatregelen met betrekking tot de toegang om taken of programma's te plannen en te initiëren die gevolgen kunnen hebben voor de financiële verslaggeving.

• Taakmonitoring

Interne beheersingsmaatregelen om financiële verslaggevingstaken of -programma's te monitoren voor succesvolle uitvoering.

• Back-up en herstel

Interne beheersingsmaatregelen om ervoor te zorgen dat back-ups van financiële ver- slaggevingsgegevens plaatsvinden zoals gepland, zodat gegevens beschikbaar zijn en kunnen worden geraadpleegd voor tijdig herstel in geval van een storing of aanval.

• Indringersdetectie

Interne beheersingsmaatregelen om te monitoren op kwetsbaarheden en/of inbraken in de IT-omgeving.

De onderstaande tabel illustreert voorbeelden van general IT controls om in te spelen op voorbeelden van risico's die voortkomen uit het gebruik van IT, inclusief verschillende IT-applicaties op basis van hun aard.

Proces	Risico's	Interne beheersings-maatregelen	IT-applicaties		
IT proces	Voorbeeld-risico's die voortkomen uit het gebruik van IT	Voorbeeld gene- ral IT-controls	Niet-complexe commerciële soft- ware - Van toe- passing (Ja/ nee)	Middelgrote en matig complexe commerciële soft- ware of IT- applicaties - Van toepassing (Ja/ nee)	Grote of com- plexe IT- applicaties (bij- voorbeeld ERP systemen) - Van toepassing (Ja/ nee)

	Users have access privileges beyond those necessary to perform their assigned duties, which may create	and extent of user-access privileges for new and modified user access, including standard application profiles/roles, critical financial reporting transactions, and	reviews noted below		
Process	**Risks**	**Controls**	**IT Applications**		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
	improper segregation of duties.	segregation of duties			
		Access for terminated or transferred users is removed or modified in a timely manner	Yes – instead of user access reviews below	Yes	Yes
		User access is periodically reviewed	Yes – instead of provisioning/ Deprovisioning controls above	Yes – for certain applications	Yes
		Segregation of duties is monitored and conflicting access is either removed or mapped to mitigating controls, which are documented and tested	N/A – no system enabled segregation	Yes – for certain applications	Yes
		Privileged-level access (e.g., configuration, data and security administrators) is authorized and	Yes – likely at IT application layer only	Yes – at IT application and certain layers of IT environment for platform	Yes – at all layers of IT environment for platform

Toegang beheren	Gebruikers-toegangs- privileges: Gebruikers hebben toegangs-privileges die verder gaan dan nodig om hun toegewezen taken uit te voeren, hetgeen ongepaste functiescheiding kan creëren.	Management keurt de aard en omvang van gebruikers toegangs-privileges voor nieuwe en aangepaste gebruikers-toegang goed, inclusief standaard applicatie profielen / rollen, kritische financiële verslag-	Ja - in plaats van beoordelingen van gebruikers-toegang hieronder	Ja	Ja
		gevings- transacties, en functie-scheiding			
		Toegang voor beeindigde of overgedragen gebruikers is tijdig verwijderd of gewijzigd	Ja - in plaats van beoordelingen van gebruikers-toegang hieronder	Ja	Ja
		Gebruikers-toegang wordt periodiek beoordeeld	Ja - in plaats van interne beheersingsmaat-regelen over toegang verlenen/opheffen hierboven	Ja voor bepaalde applicaties	Ja
		Functiescheiding wordt gemonitord en conflicterende toegang wordt verwijderd of toegewezen aan mitigerende interne beheersingsmaat-regelen, die zijn gedocumenteerd en getoetst	Nvt – geen systeem ingeschakelde scheiding	Ja voor bepaalde applicaties	Ja
		Toegang op Privilege-niveau (bijv. configuratie, gegevens en veiligheids- beheerders) is geautoriseerd en op gepaste wijze beperkt	Ja - waarschijnlijk alleen bij IT-applicatie-laag	Ja - bij IT applicatie en bepaalde lagen van IT-omgeving voor een platform	Ja bij alle lagen van IT-omgeving voor een platform
Toegang beheren	Directe gegevens toegang: Ongepaste veranderingen zijn rechtstreeks gemaakt in financiële data door andere middelen dan applicatie transacties.	Toegang tot applicatie gegevens-bestanden of database objecten / tabellen / gegevens is beperkt tot geautoriseerd personeel op basis van hun taak-verantwoordelijkheden en toegewezen rol, en dergelijke toegang is goedgekeurd door het management	Nvt	Ja voor bepaalde applicaties en databases	Ja

			Toegang beheren	Systeem instellingen: Systemen zijn niet voldoende geconfigureerd of bijgewerkt om systeemtoegang te beperken tot naar behoren geautoriseerde en geschikte gebruikers.	Toegang is geverifieerd door unieke gebruikers-ID's en wachtwoorden of andere methoden zoals een mechanisme voor het valideren dat gebruikers geautoriseerd zijn om toegang te krijgen tot het systeem. Wachtwoord parameters voldoen aan de bedrijfs- of sector normen (bijv. minimum lengte wachtwoord en complexiteit, vervaldatum, account-vergrendeling)	Ja – alleen wachtwoord authenticatie	Ja - mix van wachtwoord en multi-factor authenticatie	Ja

Process	Risks	Controls	IT Applications		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
		appropriately restricted			
Manage Access	Direct data access: Inappropriate changes are made directly to financial data through means other than application transactions.	Access to application data files or database objects/tables/data is limited to authorized personnel, based on their job responsibilities and assigned role, and such access is approved by management	N/A	Yes – for certain applications and databases	Yes
Manage Access	System settings: Systems are not adequately configured or updated to restrict system access to properly authorized and	Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system. Password	Yes – password authentication only	Yes – mix of password and multi-factor authentication	Yes

		De belangrijkste kenmerken van de bewakings-configuratie zijn op gepaste wijze geïmplementeerd	Nvt – er bestaan geen technische veiligheids- configuraties	Ja voor bepaalde applicaties en databases	Ja
Wijzigingen beheren	Applicatie wijzigingen: Ongepaste wijzigingen zijn doorgevoerd aan applicatie-systemen of programma's die relevante geautomatiseerde interne beheersingsmaat-regelen (d.w.z. configureerbare instellingen, geautomatiseerde algoritmen, geautomatiseerde berekeningen en geautomatiseerde data-extractie) of rapport logica bevatten.	Applicatie wijzigingen zijn op gepaste wijze getest en goedgekeurd voordat ze doorgevoerd worden naar de productie omgeving	Nvt – zou verifieren dat er geen broncode is geïnstalleerd	Ja - voor niet-commerciële software	Ja
		Toegang tot het doorvoeren van wijzigingen in de applicatie productie omgeving is op gepaste wijze beperkt en gescheiden van de ontwikkel-omgeving	Nvt	Ja voor niet-commerciële software	Ja
Wijziging beheren	Database wijzigingen: Ongepaste wijzigingen zijn doorgevoerd in de database structuur en relaties tussen de gegevens.	Database wijzigingen zijn op gepaste wijze getoetst en goedgekeurd voordat ze verplaatst worden naar de productie omgeving	Nvt – geen database veranderingen gemaakt bij de entiteit	Ja - voor niet-commerciële software	Ja
Wijzigingen beheren	Systeem software wijzigingen: Ongepaste wijzigingen zijn gemaakt in systeem software (bijv. besturings- systeem, netwerk, *change management* software, toegangscontrole software).	Systeem software wijzigingen zijn op gepaste wijze getest en goedgekeurd voordat ze worden doorgevoerd naar de productie	Nvt – geen systeem software wijzigingen zijn gemaakt bij entiteit	Ja	Ja

		appropriate users.	parameters meet company or industry standards (e.g., password minimum length and				Wijzigingen beheren	Gegevens conversie: Gegevens geconverteerd uit verouderde systemen of voorgaande versies introduceren fouten in gegevens als de conversie incomplete, overtollige, verouderde, of onnauwkeurige gegevens overbrengt.	Management keurt de resultaten van de conversie van gegevens goed (bijvoorbeeld balansopmakende en aansluitings- activiteiten) van het oude applicatie systeem of de gegevens structuur naar het nieuwe applicatiesysteem of de gegevensstructuur en monitort dat de conversie is uitgevoerd in overeenstemming met vastgestelde conversie- beleidslijnen en procedures	Nvt – behandeld door handmatige interne beheersingsmaat-regelen	Ja	Ja

Process	Risks	Controls	IT Applications		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
		complexity, expiration, account lockout)			
		The key attributes of the security configuration are appropriately implemented	N/A – no technical security configurations exist	Yes – for certain applications and databases	Yes
Manage Change	Application changes: Inappropriate changes are made to application systems or	Application changes are appropriately tested and approved before being moved into the production environment	N/A – would verify no source code installed	Yes – for non-commercial software	Yes

IT activiteiten	Netwerk: het netwerk voorkomt onvoldoende dat onbevoegde gebruikers ongepast toegang verkrijgen tot informatie systemen.	Toegangsauthenticatie door unieke gebruikers-ID's en wachtwoorden of andere methoden zoals een mechanisme voor het valideren dat gebruikers geautoriseerd zijn om toegang te krijgen tot het systeem. Wachtwoord parameters voldoen aan bedrijfs- of professionele beleidslijnen en normen (bijv. minimum lengte wachtwoord en complexiteit, vervaldatum, account-vergrendeling)	Nvt – er bestaat geen aparte netwerk authenticatie methode	Ja	Ja
		Het netwerk is zodanig gesegmenteerd dat web-gerichte applicaties gescheiden zijn van het interne netwerk	Nvt – geen netwerk segmentatie toegepast	Ja – met oordeelsvorming	Ja – met oordeelsvorming
		Kwetsbaarheids-scans van de netwerk omgeving worden periodiek uitgevoerd door het netwerk management team (beveiligingscentrum), dat ook potentiële kwetsbaarheden onderzoekt	Nvt	Ja – met oordeelsvorming	Ja – met oordeelsvorming

	programs that contain relevant automated controls (i.e., configurable settings, automated algorithms, automated calculations, and automated data extraction) or report logic.	Access to implement changes into the application production environment is appropriately restricted and segregated from the development environment	N/A	Yes for non-commercial software	Yes

		Waarschuwingen worden periodiek gegenereerd om bedreigingen die zijn geïdentifi-ceerd door de in-breuk detectie-systemen te com-municeren. Deze bedreigingen zijn onderzocht door het netwerk ma-nagement team (beveiligingscen-trum)	Nvt	Ja – met oor-deelsvorming	Ja – met oor-deelsvorming
		Interne beheer-singsmaat-rege-len zijn geïmple-menteerd om toe-gang tot *Virtual Private Network* (VPN) te beper-ken tot geautori-seerde en ge-schikte gebruikers	Nvt - geen VPN	Ja – met oor-deelsvorming	Ja – met oor-deelsvorming
IT Activiteiten	Gegevens back-up en herstel: Fi-nanciële gege-vens kunnen niet tijdig worden her-steld of benaderd bij een verlies van gegevens.	Er wordt regelma-tig een back-up gemaakt van fi-nanciële gege-vens volgens een vastgesteld schema en fre-quentie	Nvt – steunend op handmatige back-ups door het financiële team	Ja	Ja
IT Activiteiten	Taakplanning: Productie sys-temen, program-ma's, of taken re-sulteren in on-nauwkeurig, on-volledig, of onge-autoriseerd ver-werken van gege-vens.	Alleen geautori-seerde gebruikers hebben toegang om de batch ta-ken bij te werken (inclusief inter-face-taken) in de taakplannings-software	Nvt - geen batch taken	Ja voor bepaalde applicaties	Ja
		Kritische sys-temen, program-ma's of taken worden gemoni-tord en verwer-kings-fouten wor-den gecorrigeerd om te zorgen voor succesvolle im-plementatie.	Nvt - geen taak-monitoring	Ja voor bepaalde applicaties	Ja

Process	Risks	Controls	IT Applications		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
Manage Change	Database changes: Inappropriate changes are made to the database structure and relationships between the data.	Database changes are appropriately tested and approved before being moved into the production environment	N/A – no database changes made at entity	Yes – for non-commercial software	Yes
Manage Change	System software changes: Inappropriate changes are made to system software (e.g., operating system, network,	System software changes are appropriately tested and approved before being moved to production	N/A – no system software changes are made at entity	Yes	Yes

		change-management software, access-control software).						
	Process	**Risks**	**Controls**	**IT Applications**				
	IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**		
	Manage Change	Data conversion: Data converted from legacy systems or previous versions introduces data errors if the conversion transfers incomplete, redundant, obsolete, or inaccurate data.	Management approves the results of the conversion of data (e.g., balancing and reconciliation activities) from the old application system or data structure to the new application system or data structure and monitors that the conversion is performed in accordance with established conversion policies and procedures	N/A – Addressed through manual controls	Yes	Yes		
	IT Operations	Network: The network does not adequately prevent unauthorized users from gaining inappropriate access to information systems.	Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company or	N/A – no separate network authentication method exists	Yes	Yes		
	Process	**Risks**	**Controls**	**IT Applications**				

IT Process	Example Risks Arising from the Use of IT	Example General IT Controls	Non-complex commercial software – Applicable (yes / no)	Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)	Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)
		professional policies and standards (e.g., password minimum length and complexity, expiration, account lockout)			
		Network is architected to segment web-facing applications from the internal network, where ICFR relevant applications are accessed	N/A – no network segmentation employed	Yes – with judgment	Yes – with judgment
		On a periodic basis, vulnerability scans of the network perimeter are performed by the network management team, which also investigates potential vulnerabilities	N/A	Yes – with judgment	Yes – with judgment
		On a periodic basis, alerts are generated to provide	N/A	Yes – with judgment	Yes – with judgment

Process	Risks	Controls	IT Applications		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
		notification of			

			threats identified by the intrusion detection systems. These threats are investigated by the network management team			
			Controls are implemented to restrict Virtual Private Network (VPN) access to authorized and appropriate users	N/A – no VPN	Yes – with judgment	Yes – with judgment
	IT Operations	Data backup and recovery: Financial data cannot be recovered or accessed in a timely manner when there is a loss of data.	Financial data is backed up on a regular basis according to an established schedule and frequency	N/A – relying on manual backups by finance team	Yes	Yes
	IT Operations	Job scheduling: Production systems, programs, or	Only authorized users have access to update the batch jobs (including	N/A – no batch jobs	Yes – for certain applications	Yes

Process	**Risks**	**Controls**	**IT Applications**		
IT Process	**Example Risks Arising from the Use of IT**	**Example General IT Controls**	**Non-complex commercial software – Applicable (yes / no)**	**Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)**	**Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)**
	jobs result in inaccurate, incomplete, or unauthorized processing of data.	interface jobs) in the job scheduling software			
		Critical systems, programs, or jobs are monitored, and processing errors are corrected to ensure successful completion.	N/A – no job monitoring	Yes – for certain applications	Yes
