Volwassenheidsmodel informatiebeveiliging

Jurgen Pertijs,
werkgroep volwassenheidsmodel informatiebeveiliging

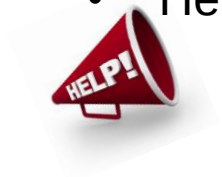
NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Vragen in de boardroom

- Op welke wijze bepaalt mijn organisatie haar risicobereidheid voor informatiebeveiliging?
- Hoe weet mijn organisatie en haar stakeholders dat informatiebeveiliging volwassen genoeg is?
- Hoe weerbaar is mijn organisatie met betrekking tot cyber security incidenten?
- Hoe hebben mijn “lines of defense” hun check & balances opgezet om de effectiviteit van de beveiligingsmaatregelen te toetsen?

- Is mijn informatievoorziening aangaande beveiliging toereikend om op basis hiervan te kunnen (bij)sturen?
- Hoe vergewist mijn organisatie zich ervan dat mijn leveranciers en ketenpartners hun beveiliging goed hebben geregeld?
- Hoe presteert mijn organisatie ten opzichte van andere organisatieonderdelen?
- Wat moet mijn organisatie regelen om het vereiste niveau te bereiken?
- Heb ik waar voor mijn geld?



Opdracht werkgroep

De opdracht was:

1. Up to date maken van het model van 2016 met de laatste inzichten ten aanzien van het beheersen van cyberrisico;
2. De bekendheid van het model vergroten.

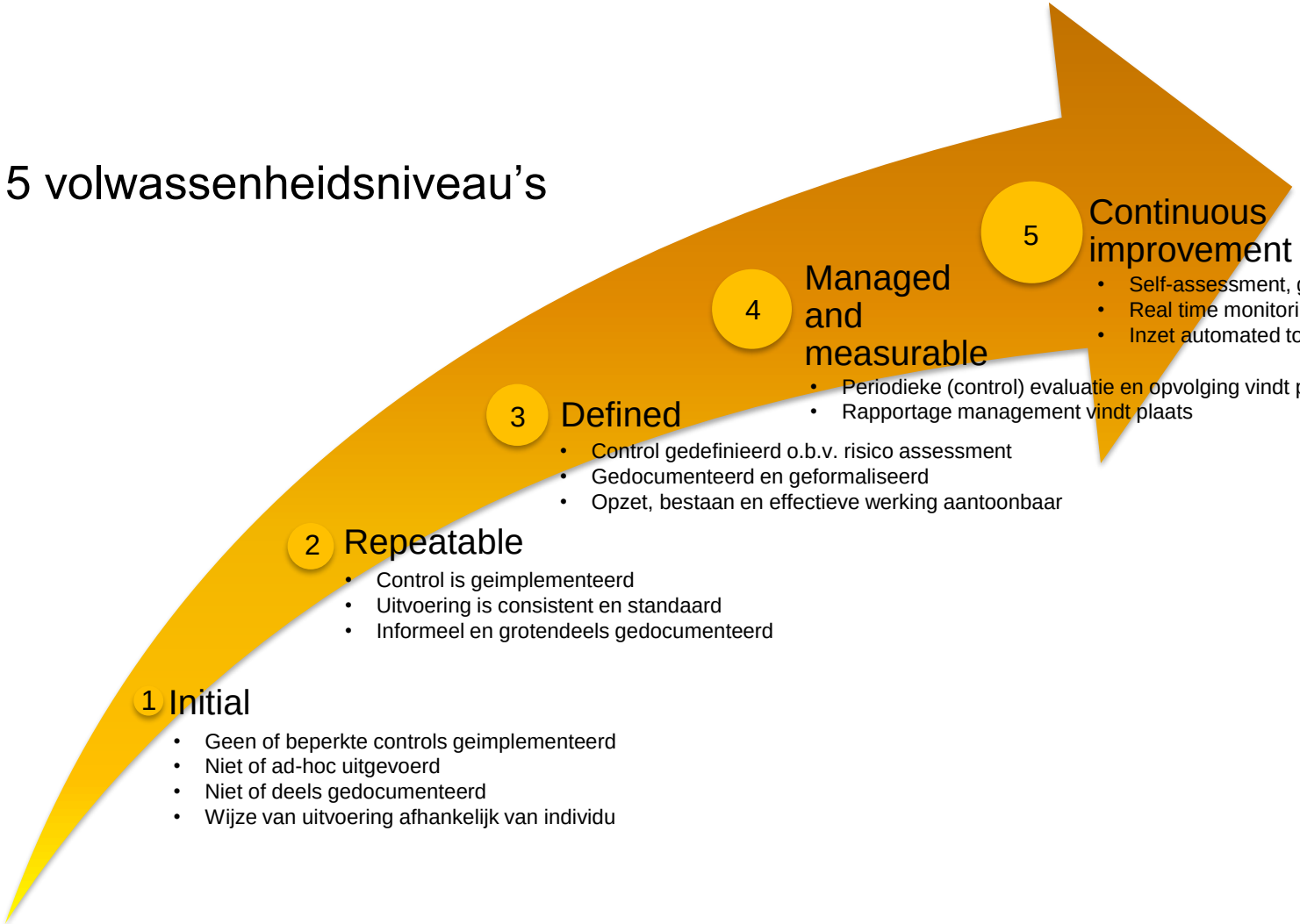
Het ontwerp

- Model is gebaseerd op “good practices”
- Referenties naar CobIT, ISO27K, BIO, DNB, NIST
- Engelstalig
- Gebieden:
  - Governance
  - Organisation
  - Risk Management
  - Human Resources
  - Configuration Management
  - Incident & Problem Management
  - Change Management
  - System Development
  - Data Management
  - Identity & Access Management
  - Security Management
  - Physical Security
  - Computer Operations
  - Business Continuity Management
  - Supply Chain Management

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

- 5 volwassenheidsniveau’s



1 Initial
- Geen of beperkte controls geimplementeerd
- Niet of ad-hoc uitgevoerd
- Niet of deels gedocumenteerd
- Wijze van uitvoering afhankelijk van individu

2 Repeatable
- Control is geimplementeerd
- Uitvoering is consistent en standaard
- Informeel en grotendeels gedocumenteerd

3 Defined
- Control gedefinieerd o.b.v. risico assessment
- Gedocumenteerd en geformaliseerd
- Opzet, bestaan en effectieve werking aantoonbaar

4 Managed and measurable
- Periodieke (control) evaluatie en opvolging vindt plaats
- Rapportage management vindt plaats

5 Continuous improvement
- Self-assessment, gap en root cause analyses
- Real time monitoring
- Inzet automated tooling

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Een kijkje in het model…

GENERAL INFORMATION

Organization			
Name:	<name>		
Country:	<country>		
Industry:	00 - None		

Facts & Figures			
1	Annual business turnover	€ -	in Euro
2	Number of employees	0	in FTEs
3	Total budget of ICT operations and ICT development, including	€ -	in Euro
4	Budget of Information Security in Business	€ -	in Euro
5	Budget of Information Security in ICT Departments	€ -	in Euro
6	% of ICT security services outsourced to third parties compared to total of ICT security services delivered	0	%
7	% audit capacity spent on IT audit compared to total audit capacity (last year)	0	%
8	Total number of FTEs in the Information Security Departments & number of vacant positions in the	total	vacant positions
		0	0

Remark(s)
<remarks>

Approval & Preparation	
Approval date	<dd-mm-yy>
Maturity assessment approved by:	<name>
Job Function / Owner:	<job function>
Maturity assessment prepared by:	<name>
Job Function:	<job function>

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Totaaloverzicht

Area	ID	Control name	Risk description	Indicative maturity level based on inherent risk estimation	Control Objective	Maturity Indication Level 1 Initial "Initial Controls are not, or only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Maturity Indication Level 2 Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.	Maturity Indication Level 3 Defined Controls are documented and executed in a structured and formal manner. Execution of control can be proved, is tested and effective.	Maturity Indication Level 4 Managed and measurable The effectiveness of the control is periodically assessed an improved when necessary. This assessment is documented.	Maturity Indication Level 5 Continuous improvement An enterprisewide risk and control programme provides continuous and effective control and risk issues resolution.	Actual Maturity Indication Level	References COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2017	BIO 2019	NIST Cybersecurity Framework
Governance	**GO.01**	**Strategy**	An absence of strategy can lead to poor business and security decisions or inappropriate response to changes in the business environment.	3	An information and cyber security strategy and vision is leading for all activities and measures concerning information security	- Information and/or cyber security activities or measures are implemented and/or executed on an ad-hoc basis.	- A strategy and vision has been defined, but has not been formally accepted.	- Strategy and vision has been approved by senior management. - Strategy and mission is actively communicated to employees, contractors and business partners.	- Strategy and vision are acknowledged as leading for all activities and measures regarding information and cyber security. - Alignment with strategy and vision is documented where applicable. - The validity and feasibility of the strategy and vision is periodically verified.	- Strategy also addresses how IT will help business objectives to be realized. - If necessary, the strategy or vision is adjusted to keep pace with business objectives and external developments.	1	PO1.4 ME4.2	APO02.01 APO02.02 APO02.03, APO02.04, APO02.05	5.1, A5.1.1	1.2	5.1.1 5.1.1.1	ID.GV-3
	GO.02	**Policy**	Inability to comply with legislative, regulatory and/or internal information security requirements due to an ineffective policy framework which supports the IT strategy and information security.	3	The organization has adopted a (information) security policy which is communicated to employees (and contractors) via a written policy document or intranet. If applicable, the policy is also actively communicated to suppliers/vendors. The policy is regularly updated, reviewed and approved by senior management.	- No policy defined. - Some policy statements drafted.	- A (information) security policy has been defined and covers most relevant aspects of information security.	- Policy has been approved by senior management. - Policy is actively communicated to employees, contractors and business partners (suppliers) and is made available as hard copy or digital document via intranet. - Policy is part of the security awareness program. - Compliance with policy is assessed on ad-hoc basis.	- The (information) security policy has been embedded into / adopted by the organization and translated into underlying procedures, baselines and instructions. - Policy is evaluated, updated and reapproved by senior management on a periodic basis.	- Compliance with (information) security policy is periodically reported to senior management.	2	PO6.3, PO6.4, PO6.5	APO01.03, APO01.04, APO01.06 APO01.07 APO01.08	5.2, A5.1.1, A5.1.2, A6.1.1, A7.2.2, A18.2.2	1.2	5.1.1 5.1.1.1 5.1.2 5.1.2.1 6.1.1.1 6.1.1.2 6.1.1.3 6.1.1.4	ID.GV-3
	GO.03	**Plan / Roadmap**	Guidance and support for information security in accordance with business objectives, risks and compliance requirements is not provided by the organization.	3	Business objectives, risks and compliance requirements are translated into an overall information and/or cyber security plan, taking into consideration IT infrastructure and the security culture.	- No information or cyber security plan or roadmap defined. - A few individual IT security projects have been defined and/or in progress.	- An information and/or cyber security plan or roadmap has been defined and covers all relevant business objectives, risks and compliance requirements.	- The plan or roadmap has been approved by senior management. - The plan has been translated into required (information) security policies and procedures together with appropriate investments in services, personnel, software and hardware. - Related policies and procedures are communicated to stakeholders and users.	- The information and/or cyber security plan is implemented and supported via enforced (information) security policies, procedures, required services, personnel, software and hardware. - There is a process for periodically evaluating and updating the information and/or cyber security plan and for forcing appropriate levels of management review and approval of changes.	- The information and/or cyber security plan versus related project portfolio are periodically monitored for e.g. progress, threats, feasibility and extent to which business requirements are met, including benefit tracking. - Reports submitted to senior management.	3	DS5.2	APO02.05 APO13.02	5.2, A5.1.1, A5.1.2, A6.2.1, A6.2.2, A7.2.2, A9.1.1, A10.1.1, A13.2.1, A18.1.1, A18.1.2, A18.1.3 A18.1.4 A18.1.5	1.1	5.1.1 5.1.1.1 5.1.2 5.1.2.1 6.2.1 6.2.1.1 6.2.1.2 6.2.2 7.2.2 7.2.2.1 7.2.2.2 7.2.2.3 9.1.1 10.1.1 10.1.1.1 10.1.1.2 13.2.1 18.1.1 18.1.2 18.1.3 18.1.3.1 18.1.4 18.1.5	ID.BE-1 ID.GV-1 ID.GV-2 ID.GV-3

Area	ID	Control name	Risk description	Indicative maturity level based on inherent risk estimation	Control Objective	Maturity Indication Level 1 Initial "Initial Controls are not, or only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Maturity Indication Level 2 Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.	Maturity Indication Level 3 Defined Controls are documented and executed in a structured and formal manner. Execution of control can be proved, is tested and effective.	Maturity Indication Level 4 Managed and measurable The effectiveness of the control is periodically assessed an improved when necessary. This assessment is documented.	Maturity Indication Level 5 Continuous improvement An enterprisewide risk and control programme provides continuous and effective control and risk issues resolution.	Actual Maturity Indication Level	References COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2017	BIO 2019	NIST Cybersecurity Framework
Change Management	**CH.01**	**Change standards and procedures**	The lack of a formal IT change management process, which ensures that proposed changes are reviewed, authorized, tested, implemented, documented and released in a controlled manner, could lead to business disruptions and/or loss of confidential data.	3	Formal change management procedures have been set up to handle all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms, in a standardized manner.	- Absence of change management policy and change management procedure. - Changes and requests for changes are not handled in a standardized or consistent manner. - Roles and responsibilities are not defined. - Formal approval (authorization) of changes does not take place. - There is poor or nonexistent documentation of changes.	- A change management policy has been defined to cover critical aspects. - A consistent change management process is in place and most changes are executed in accordance with this process. - Roles and responsibilities are partially defined. - The process is informal and unauthorized changes may occur. - Version control is implemented for critical system parameters.	- The change management policy and working practices are documented, standardized and communicated. - A formal change management process is in place for changes to applications, procedures, processes, system and service parameters and the underlying platforms. - The process includes all elements from promotion to production, including change authorization, impact analysis, release management, tracking of changes and roll back procedures. - Roles and responsibilities are defined and	In addition: - The change management policy has been fully embedded into the organization and implemented consistently for all changes. - The quality and effectiveness of the change management process is periodically evaluated. - Reports are sent to senior management for review. - Tools are used to detect unauthorized changes.	In addition: - The change management policy is regularly reviewed and updated. - Roles and responsibilities are reviewed on an ongoing basis. - Exception analysis is performed and exceptions are investigated. - Management receives regular reports on shortcomings and trends, which lead to improvement plans. - Reporting requirements are regularly reviewed and updated.	3	AI6.1, AI6.4, AI6.5	BAI06.01, BAI06.02, BAI06.03, BAI06.04	8.1, A12.1.2, A14.2.2, A14.2.4	10.1	12.1.2 12.1.2.1 14.2.2 14.2.2.1	
	CH.02	**Impact assessment, prioritization and authorization**	Inadequate impact assessment, prioritization or authorization could lead to business disruptions, corruption and/or loss of confidential data.	4	All change requests are assessed in a structured manner to determine impact on the operational system and its functionality. All changes are categorized, prioritized and authorized.	- There is no procedure for the assessment, prioritization and authorization of changes. - Roles and responsibilities are not defined. - Impact assessments for change requests are executed on an ad hoc basis and unauthorized changes can take place. - The process for categorizing and prioritizing changes is not standardized.	- Analysis is carried out into the impact of IT changes on business operations. - Criteria for the analysis are being developed. - An informal process is in place to categorize, prioritize and authorize changes. - Roles and responsibilities are partially defined. - Business process owners are mainly involved in the approval process.	- A formal procedure for the assessment, categorization, prioritization and authorization of changes has been formalized and communicated. - Impact assessments take place prior to a change. (Cyber) security, legal, contractual and compliance implications are considered in the assessment process. - There is a formal procedure for the authorization of changes (Change	- The procedure for the assessment, categorization, prioritization and authorization of changes is implemented consistently. - All changes are subject to thorough planning and impact assessment to minimize the likelihood and impact of post-production problems. - The number of disruptions or data errors caused by inaccurate specifications and/or an incomplete impact assessment is kept	- The assessment procedure is regularly reviewed and updated. - The measurement criteria are regularly reviewed. - Management receives regular reports which lead to improvement plans. - Reporting requirements are regularly reviewed and updated.	2	AI6.2	BAI06.01	8.1, A12.1.2, A12.6.1, A14.2.2, A14.2.4	10.2	12.1.2 12.1.2.1 12.6.1 14.2.2 14.2.2.1	

Risico analyse & control objective

Area	ID	Control name	Risk description	Indicative maturity level based on inherent risk estimation	Control Objective
Governance	GO.01	Strategy	An absence of strategy can lead to poor business and security decisions or inappropriate response to changes in the business environment.	3	An information and cyber security strategy and vision is leading for all activities and measures concerning information security
	GO.02	Policy	Inability to comply with legislative, regulatory and/or internal information security requirements due to an ineffective policy framework which supports the IT strategy and information security.	3	The organization has adopted a (information) security policy which is communicated to employees (and contractors) via a written policy document or intranet. If applicable, the policy is also actively communicated to suppliers/vendors. The policy is regularly updated, reviewed and approved by senior management.
	GO.03	Plan / Roadmap	Guidance and support for information security in accordance with business objectives, risks and compliance requirements is not provided by the organization.	3	Business objectives, risks and compliance requirements are translated into an overal information and/or cyber security plan, taking into consideration IT infrastructure and the security culture.

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Volwassenheidsmeting

Maturity Indication Level 1 **Initial** "Initial Controls are not, or only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Maturity Indication Level 2 **Repeatable** Controls are in place and executed in a structured and consistent, but informal, manner.	Maturity Indication Level 3 **Defined** Controls are documented and executed in a structured and formal manner. Execution of control can be proved, is tested and effective.	Maturity Indication Level 4 **Managed and measurable** The effectiveness of the control is periodically assessed and improved when necessary. This assessment is documented.	Maturity Indication Level 5 **Continuous improvement** An enterprisewide risk and control programme provides continuous and effective control and risk issues resolution.	Actual Maturity Indication Level
- Information and/or cyber security activities or measures are implemented and/or executed on an ad-hoc basis.	- A strategy and vision has been defined, but has not been formally accepted.	- Strategy and vision has been approved by senior management. - Strategy and mission is actively communicated to employees, contractors and business partners.	- Strategy and vision are acknowledged as leading for all activities and measures regarding information and cyber security. - Alignment with strategy and vision is documented where applicable. - The validity and feasibility of the strategy and vision is periodically verified.	- Strategy also addresses how IT will help business objectives to be realized. - If necessary, the strategy or vision is adjusted to keep pace with business objectives and external developments.	2
- No policy defined. - Some policy statements drafted.	- A (information) security policy has been defined and covers most relevant aspects of information security.	- Policy has been approved by senior management. - Policy is actively communicated to employees, contractors and business partners (suppliers) and is made available as hard copy or digital document via intranet. - Policy is part of the security awareness program. - Compliance with policy is assessed on ad-hoc basis.	- The (information) security policy has been embedded into / adopted by the organization and translated into underlying procedures, baselines and instructions. - Policy is evaluated, updated and reapproved by senior management on a periodic basis.	- Compliance with (information) security policy is periodically reported to senior management.	2
- No information or cyber security plan or roadmap defined. - A few individual IT security projects have been defined and/or in progress.	- An information and/or cyber security plan or roadmap has been defined and covers all relevant business objectives, risks and compliance requirements.	- The plan or roadmap has been approved by senior management. - The plan has been translated into required (information) security policies and procedures together with appropriate investments in services, personnel, software and hardware. - Related policies and procedures are communicated to stakeholders and users.	- The information and/or cyber security plan is implemented and supported via enforced (information) security policies, procedures, required services, personnel, software and hardware. - There is a process for periodically evaluating and updating the information and/or cyber security plan and for forcing appropriate levels of management review and approval of changes.	- The information and/or cyber security plan versus related project portfolio are periodically monitored for e.g. progress, threats, feasibility and extent to which business requirements are met, including benefit tracking. - Reports submitted to senior management.	3

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

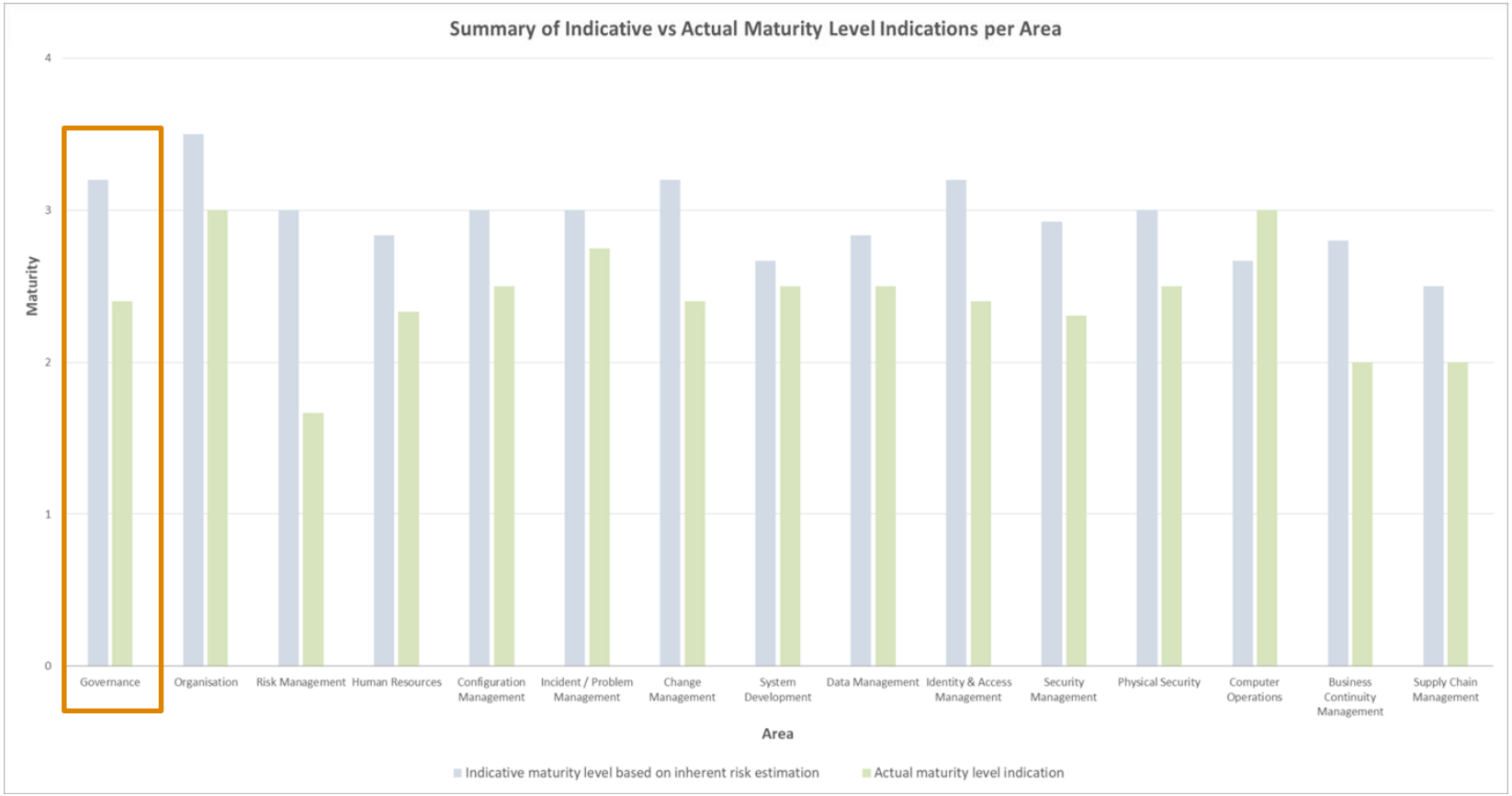
Referenties naar good practices

Area	ID	Control name	References					
			COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2017	BIO 2019	NIST Cybersecurity Framework
Governance	**GO.01**	**Strategy**	PO1.4, ME4.2	APO02.01 APO02.02 APO02.03, APO02.04, APO02.05	5.1, A.5.1.1	1.2	5.1.1 5.1.1.1	ID.GV-3
	GO.02	**Policy**	PO6.3, PO6.4, PO6.5	APO01.03, APO01.04, APO01.06 APO01.07 APO01.08	5.2, A.5.1.1, A.5.1.2, A.6.1.1, A.7.2.2, A.18.2.2	1.2	5.1.1 5.1.1.1 5.1.2 5.1.2.1 6.1.1.1 6.1.1.2 6.1.1.3 6.1.1.4	ID.GV-3
	GO.03	**Plan / Roadmap**	DS5.2	APO02.05 APO13.02	5.2, A.5.1.1, A.5.1.2, A.6.2.1, A.6.2.2, A.7.2.2, A.9.1.1, A.10.1.1, A.13.2.1, A.18.1.1, A.18.1.2,	1.1	5.1.1 5.1.1.1 5.1.2 5.1.2.1 6.2.1 6.2.1.1 6.2.1.2 6.2.2 7.2.2 7.2.2.1 7.2.2.2	ID.BE-1 ID.GV-1 ID.GV-2 ID.GV-3

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Voorbeeldrapportages - Maturity level indications



NBA

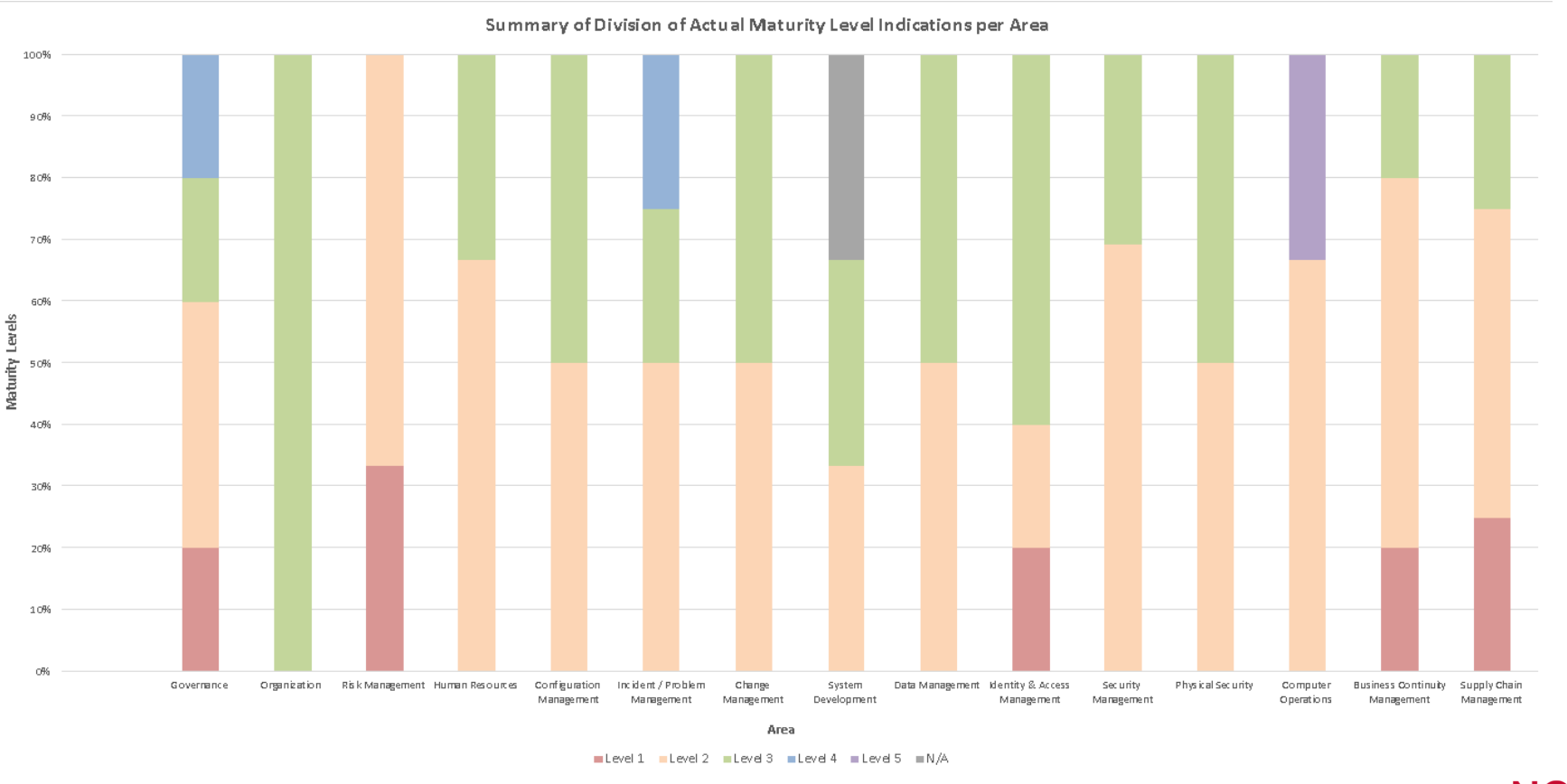
NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Voorbeeldrapportages - Governance

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Voorbeeldrapportages - Maturity level indications per area



NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Toepassing van het model

- Context zelf meewegen: maak risico indicatie organisatiespecifiek
  - aard van business en informatievoorziening
  - IT landschap
  - afhankelijkheid van informatievoorziening en derden in “waardeketen”
  - wet & regelgeving
  - risicobereidheid

- Rapportages: toegevoegde waarde door periodieke dialoog met stakeholders
  - kwetsbaarheden, impact en risico’s
  - prioritering en opvolging mitigerende acties
  - “challenge” sessie met verantwoordelijke directie

- Evalueer periodiek (het gebruik van) het model, en vertel het ons

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Vragen?

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Dank voor uw aandacht.

Koninklijke Nederlandse Beroepsorganisatie van Accountants

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS