Security (in) architecture

v1.0

ISACA Round Table
Monday, September 1, 2014

Ing. Renato Kuiper, CISA, CISSP, TOGAF. CSF

VERDONCK
KLOOSTER&
ASSOCIATES

Focus on:
Security, Risk Management, IAM, Cloud and Architecture

2013 CSA NL: Cloud Security Alliance/ board member

2013 CSA: Cyber Security Academy, program group/ teacher

2011 Haagse Hoge School: teacher security architecture and cloud.

2000 Several PvIB rolls and publications

2010 Management consultant/ Architect VKA

1997 Principal security consultant - CMG

1986 Teacher HTS, systems programmer/ security specialist

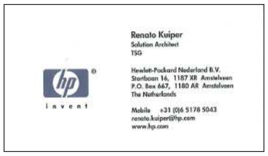
Renato Kuiper

ISC

Renato Kuiper
RIVIT

Zeisterweg 1 • 3594 NH Odijk • Postbus 230 • 3970 AE Driebergen
T (0343) 53 47 82 • F (0343) 53 47 99 • M 06 51 28 95 55

renato.kuiper@isc.nl • www.isc.nl
privé • renato.kuiper@chello.nl



Renato Kuiper
Solution Architect
TSG

Hewlett-Packard Nederland B.V.
Startbaan 16, 1187 XR Amstelveen
P.O. Box 667, 1180 AR Amstelveen
The Netherlands

Mobile   +31 (0)6 5178 5043
renato.kuiper@hp.com
www.hp.com

POLITIE
• Npol Organisatie

Renato Kuiper

Industrieweg 12
Postbus 150
7940 AD MEPPEL

Werk:
Servicedesk +31(0)522 722 000
Algemeen +31(0)522 722 222
Fax +31(0)522 722 223

Mobiel:
Telefoon +31(0)6

renato.kuiper@npol.politie.nl

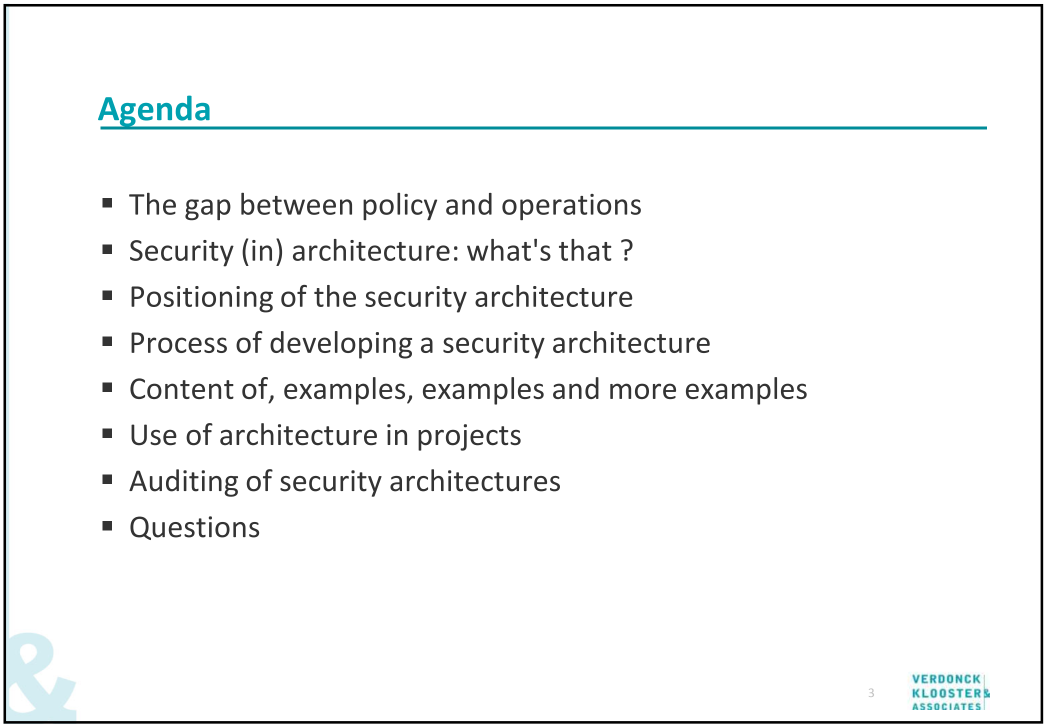
VERDONCK
KLOOSTER&
ASSOCIATES

ING. RENATO KUIPER CISA CISSP
MANAGEMENT CONSULTANT

06-53609963
RENATO.KUIPER@VKA.NL

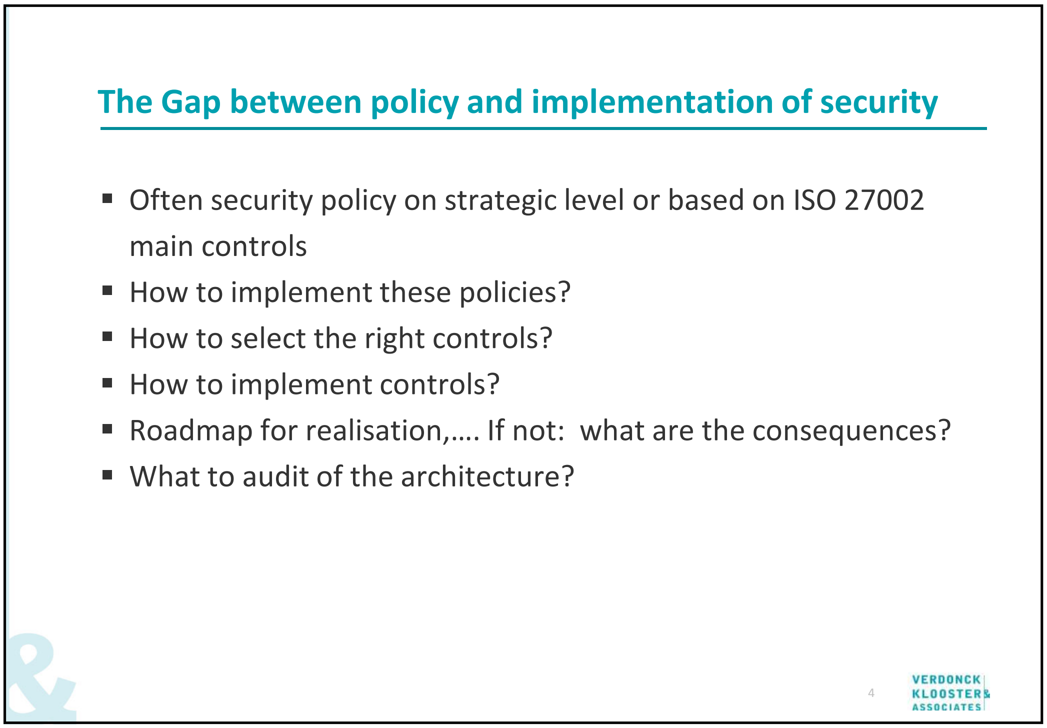
BARON DE COUBERTINLAAN 1
2719 EN ZOETERMEER
TEL 079 368 10 00
INFO@VKA.NL
WWW.VKA.NL

VERDONCK
KLOOSTER&
ASSOCIATES



Agenda

- The gap between policy and operations
- Security (in) architecture: what's that ?
- Positioning of the security architecture
- Process of developing a security architecture
- Content of, examples, examples and more examples
- Use of architecture in projects
- Auditing of security architectures
- Questions

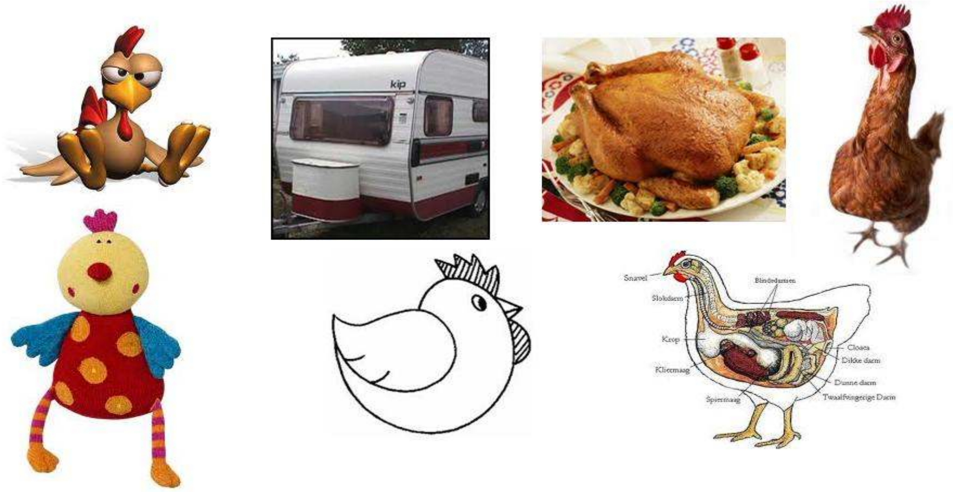


The Gap between policy and implementation of security

- Often security policy on strategic level or based on ISO 27002 main controls
- How to implement these policies?
- How to select the right controls?
- How to implement controls?
- Roadmap for realisation,…. If not: what are the consequences?
- What to audit of the architecture?

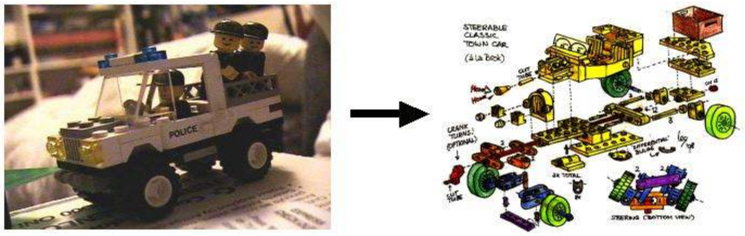
What is a security architecture?

Architecture is like a chicken, everyone has their own interpretation



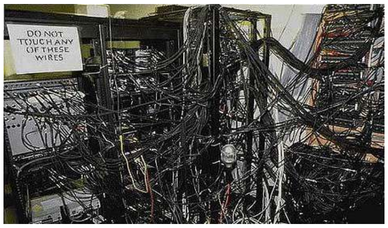
What’s a security architecture (1)?

- A Security Architecture is a **prescriptive document** that uses a set of coherent models and principles efficiently and flexibly **to guide the implementation** of the **information security policy** of an organization.



What’s a security architecture (2)?

- A security architecture consists of a transparent and **coherent overview** of **models**, **principles**, starting points and conditions that give **a concrete interpretation of the information security policy**, usually without speaking in terms of specific solutions.
- A security architecture **reduces a complex problem** into models, principles and sub problems that can be understood, mainly on the basis of the well-known what, where, when, how, with what and who questions.
- The models and principles show **where you take which type of measures**, when the principles **are applicable**, and how they **connect with** other principles.



Security (in) architecture, gives

- Consistency and understanding

  Understanding the business requirements and the assets of the organization and consistency with the measures to be taken in order to secure and protect that

- Transparency and balance

  Visible relevant security requirements and principles for all assets within the organization, goal of general and specific measures is clear and transparent

- Overall picture and clarity

  A clear and consistent overall design, the consistency of the measures is clear, there are no exceptions incomprehensible or additional measures

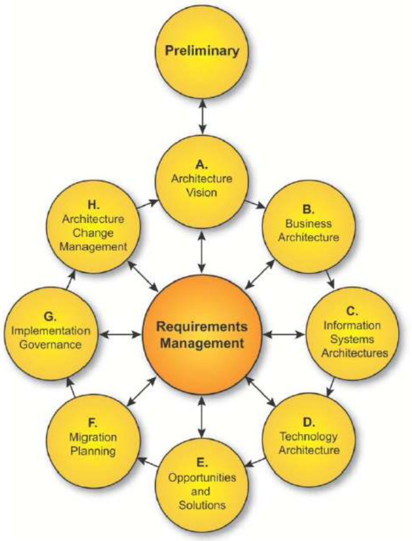
VERDONCK KLOOSTERS ASSOCIATES

Different kinds of architectures

- **Reference architecture:** model architecture for a specific domain: examples: NORA, MARIJ etc.
- **Domain architecture:** architecture for a specific domain within an organization; example Business unit production or logistics
- **Project Start Architecture** (PSA- conform DYA): architecture as a steering instrument for a project
- **IST**/ Current State architecture: describes the current situation.
- **SOLL**/ Future State architecture: describes the end situation, the targeted goals
- **MIGRATION**/ Target State architecture: specific plateau of implementation toward the end state
- ....

VERDONCK KLOOSTERS ASSOCIATES

TOGAF


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

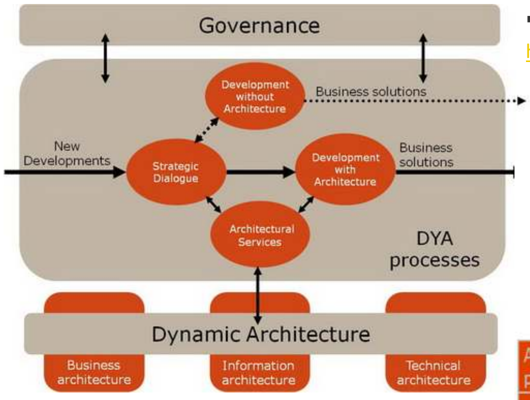
Developed by The Opengroup
Started as a technical architecture, in the latest version also Business architecture (not yet mature!)

It has a methodology the ADM: The Architecture Development Methodology.

Besides defining the architecture it also realizes the architecture through implementation and a governance process.

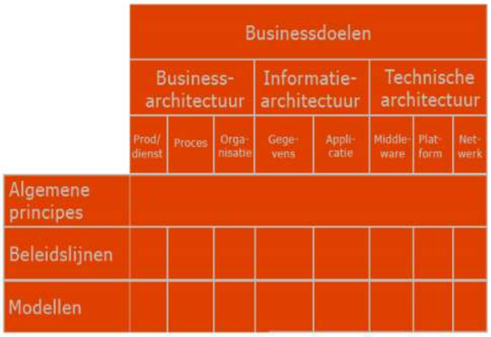
http://www.opengroup.org/togaf

DYA: Dynamic Architecture

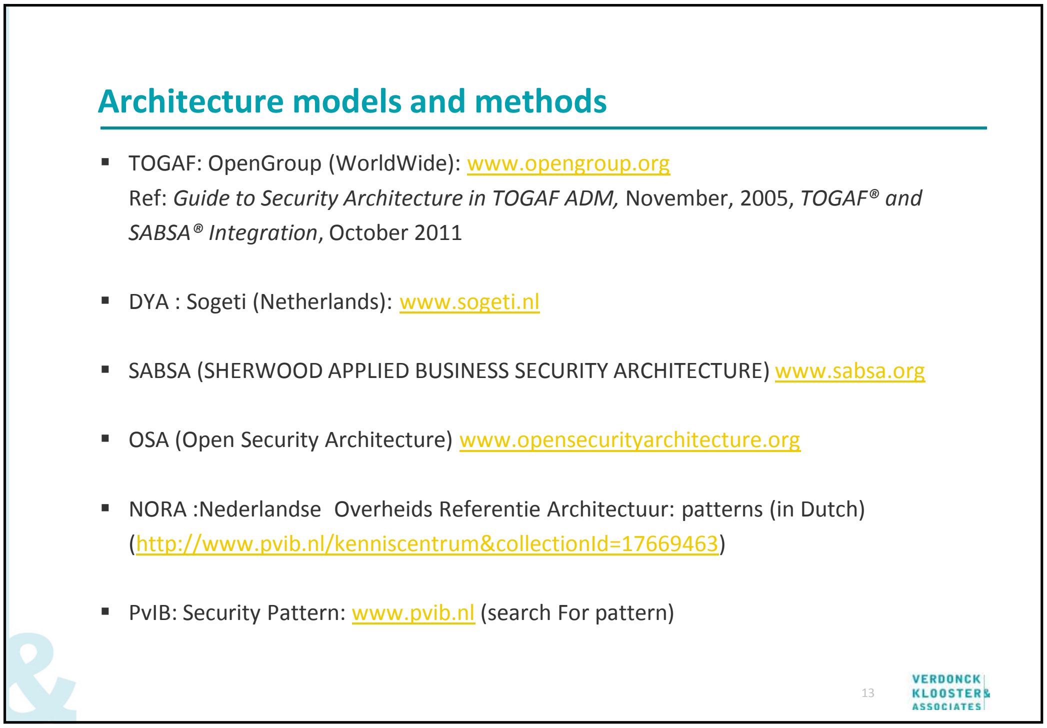


- Developed by Sogeti (Netherlands)

http://www.dya.info

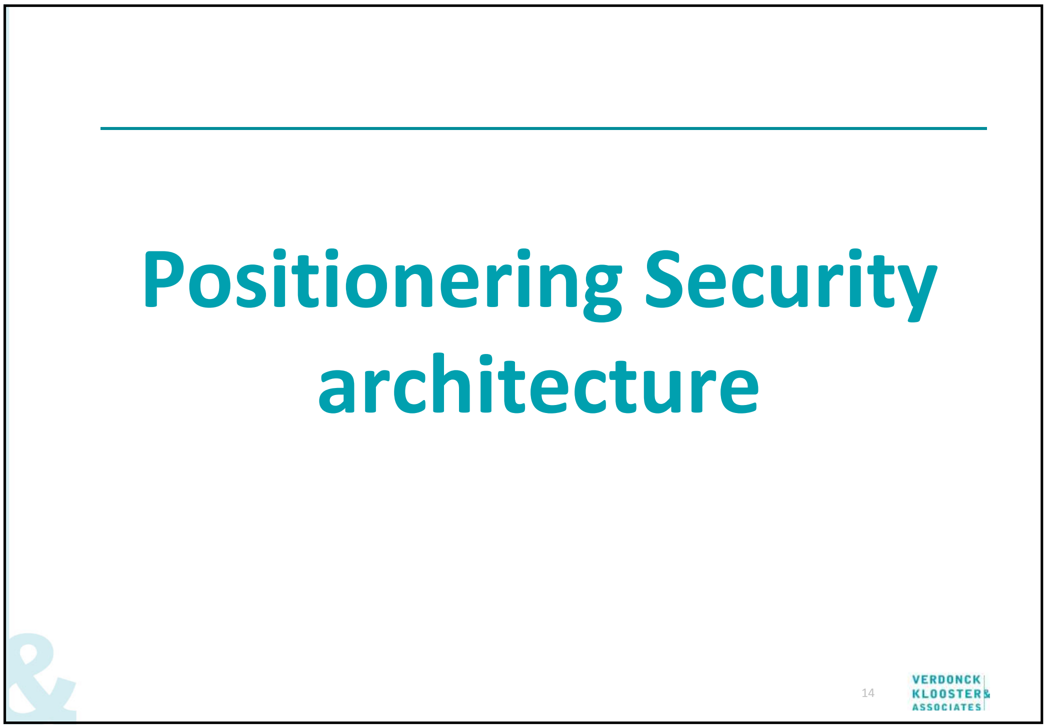


	Businessdoelen							
	Business-architectuur			Informatie-architectuur		Technische architectuur		
	Prod/dienst	Proces	Organisatie	Gegevens	Applicatie	Middleware	Platform	Netwerk
Algemene principes								
Beleidslijnen								
Modellen								

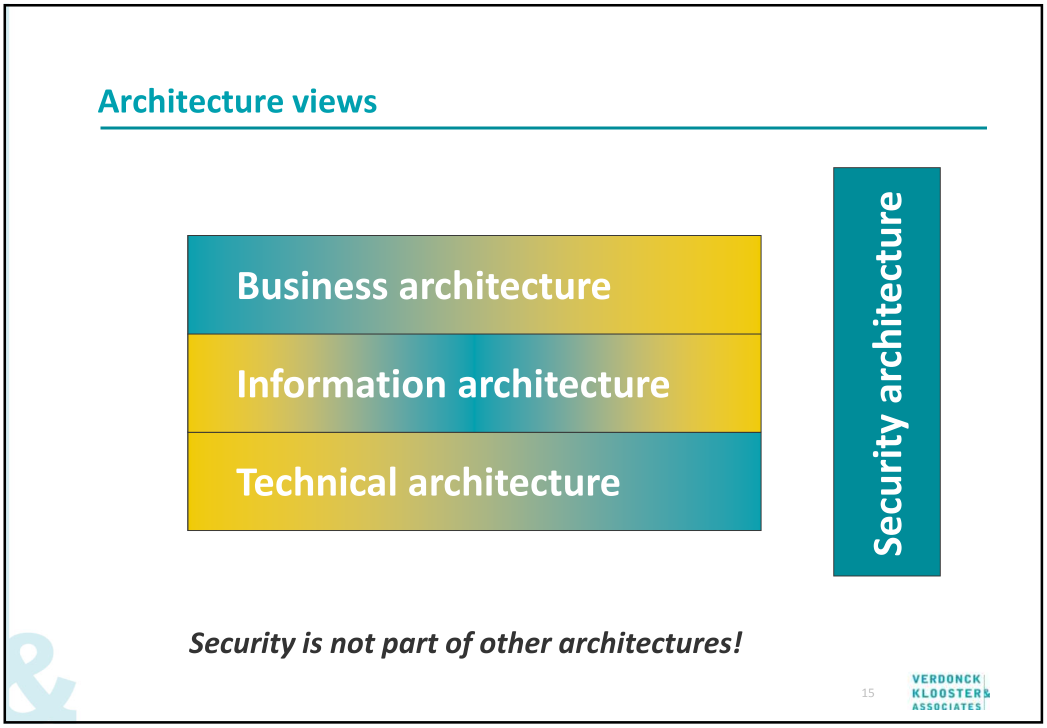


Architecture models and methods

- TOGAF: OpenGroup (WorldWide): www.opengroup.org
  Ref: *Guide to Security Architecture in TOGAF ADM,* November, 2005, *TOGAF® and SABSA® Integration*, October 2011
- DYA : Sogeti (Netherlands): www.sogeti.nl
- SABSA (SHERWOOD APPLIED BUSINESS SECURITY ARCHITECTURE) www.sabsa.org
- OSA (Open Security Architecture) www.opensecurityarchitecture.org
- NORA :Nederlandse Overheids Referentie Architectuur: patterns (in Dutch) (http://www.pvib.nl/kenniscentrum&collectionId=17669463)
- PvIB: Security Pattern: www.pvib.nl (search For pattern)



Positionering Security architecture



Architecture views

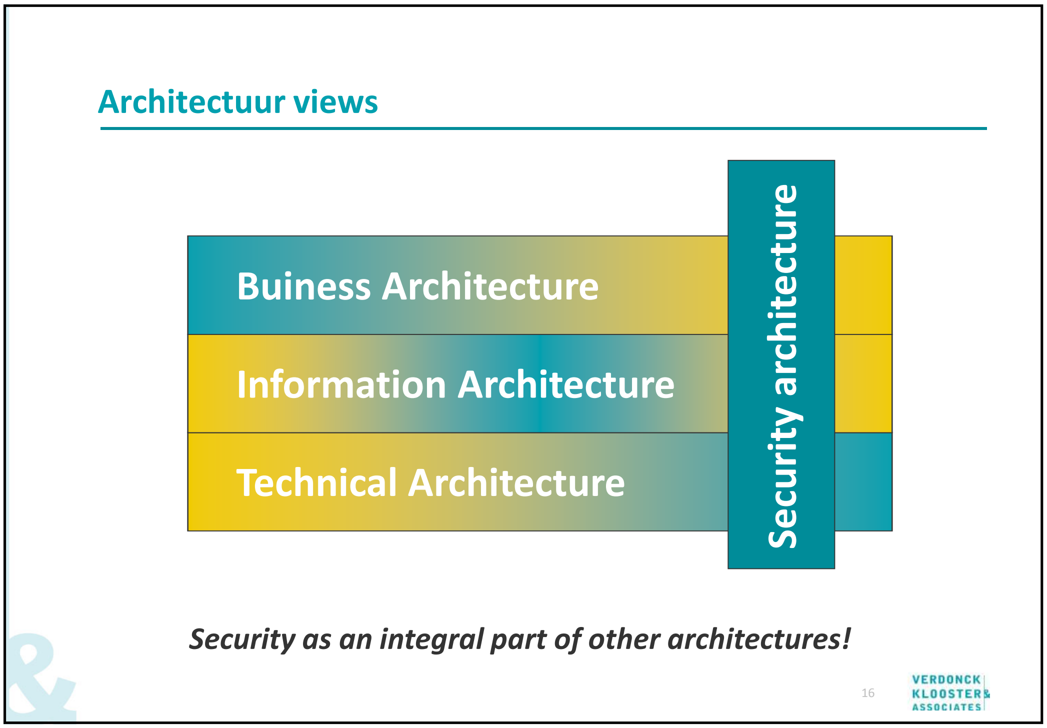
Business architecture

Information architecture

Technical architecture

Security architecture

Security is not part of other architectures!



Architectuur views

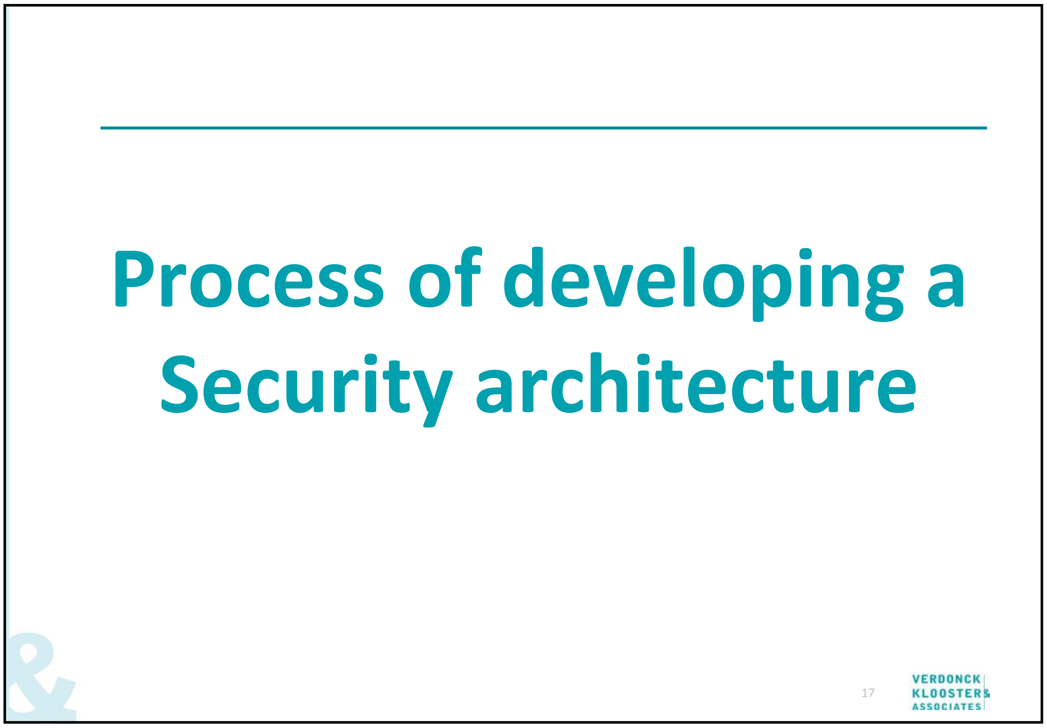
Buiness Architecture

Information Architecture

Technical Architecture

Security architecture

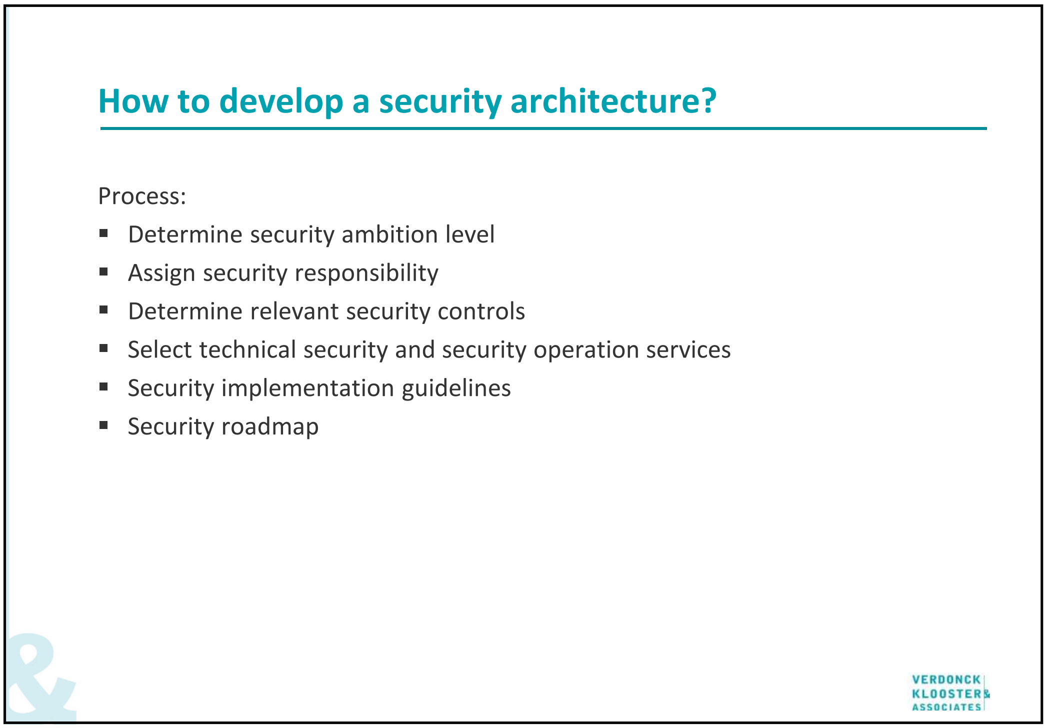
Security as an integral part of other architectures!



Process of developing a Security architecture

17

VERDONCK KLOOSTER & ASSOCIATES



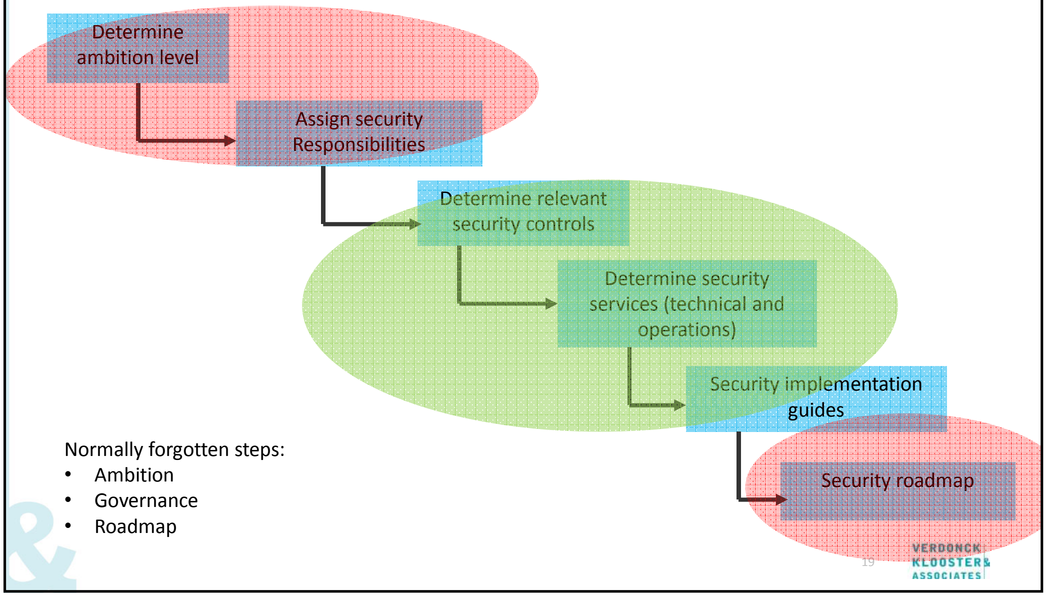
How to develop a security architecture?

Process:

- Determine security ambition level
- Assign security responsibility
- Determine relevant security controls
- Select technical security and security operation services
- Security implementation guidelines
- Security roadmap

VERDONCK KLOOSTER & ASSOCIATES

Process of developing a security architecture



Determine ambition level

Assign security Responsibilities

Determine relevant security controls

Determine security services (technical and operations)

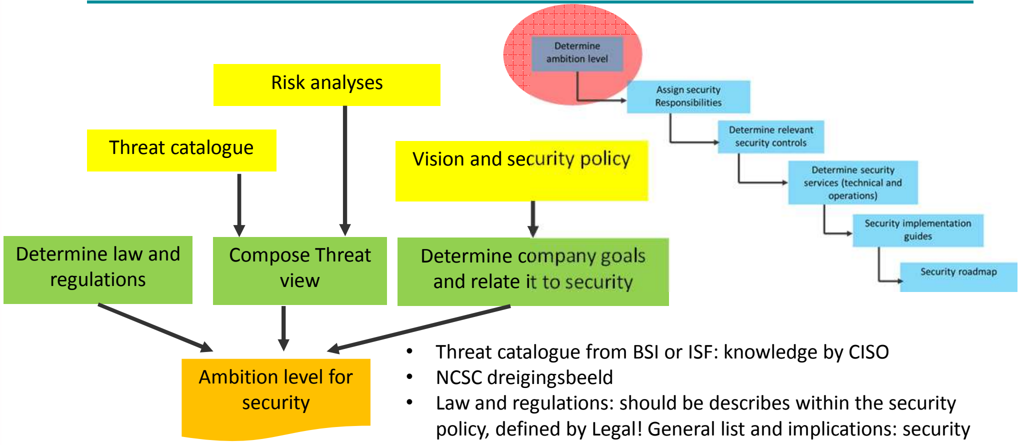
Security implementation guides

Security roadmap

Normally forgotten steps:

- Ambition
- Governance
- Roadmap

Determine ambition level



Risk analyses

Threat catalogue

Vision and security policy

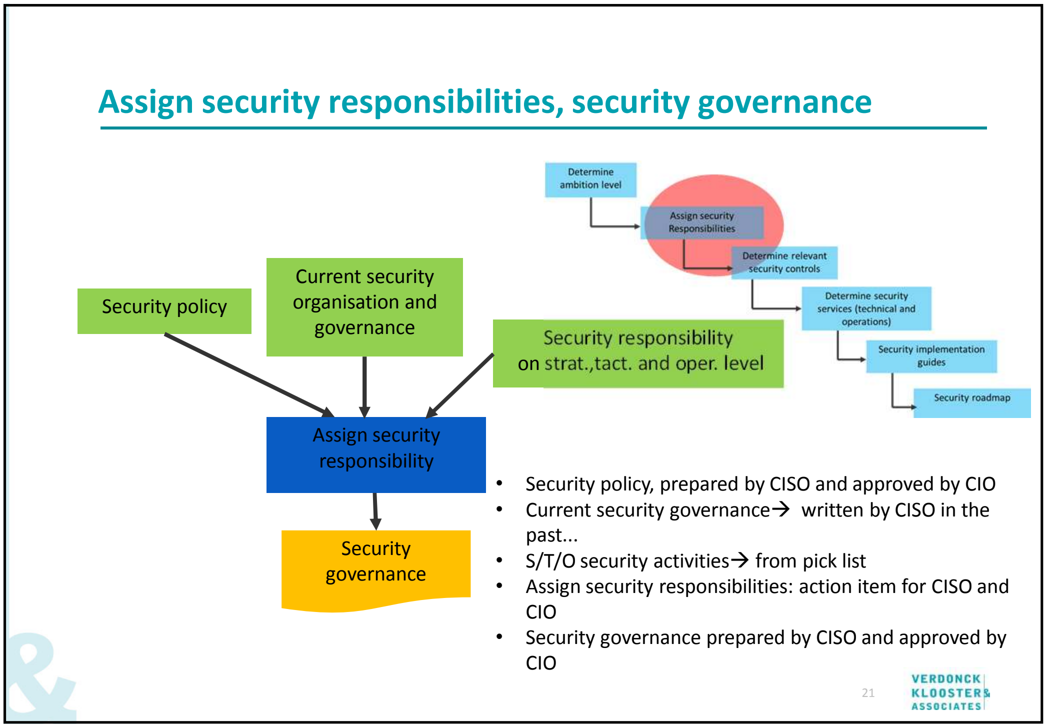
Determine law and regulations

Compose Threat view

Determine company goals and relate it to security

Ambition level for security

- Threat catalogue from BSI or ISF: knowledge by CISO
- NCSC dreigingsbeeld
- Law and regulations: should be describes within the security policy, defined by Legal! General list and implications: security architect
- Risk analyses: method selected by CISO, execution by CEO, CFO, supported by CISO: determine risk tolerance/ risk appetite, acceptance of results by Cxx level
- Threat view composed by CISO and security architect based op RA
- Ambition level, prepared by CIO and CISO, approval by CFO



Assign security responsibilities, security governance

Determine ambition level

Assign security Responsibilities

Determine relevant security controls

Determine security services (technical and operations)

Security implementation guides

Security roadmap

Security policy

Current security organisation and governance

Security responsibility on strat.,tact. and oper. level

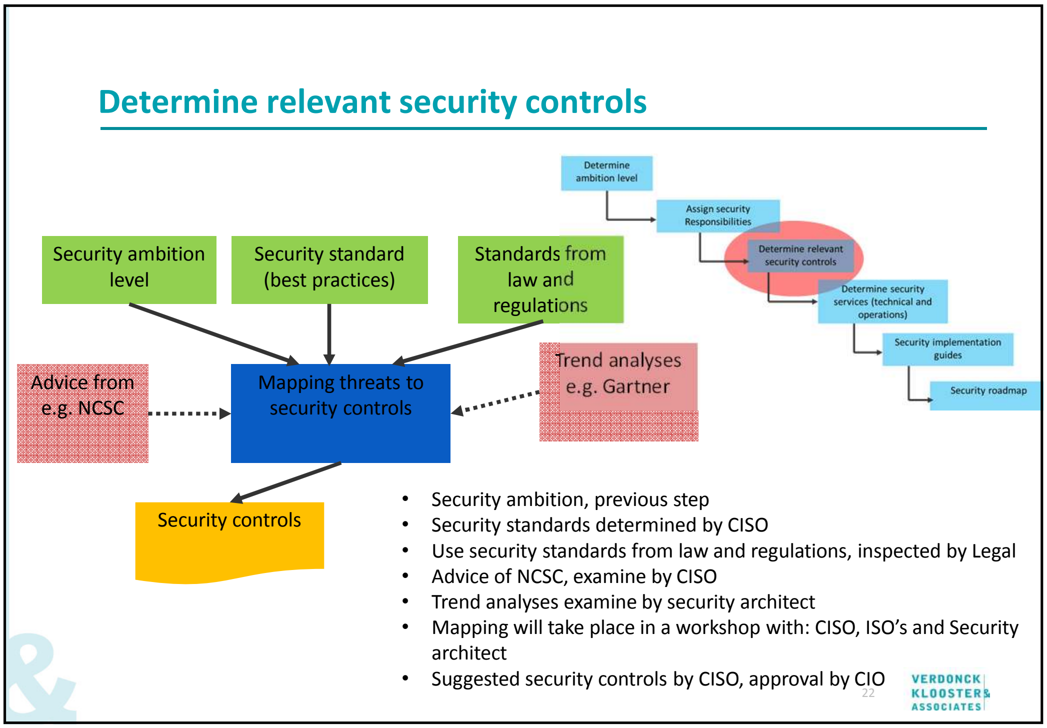
Assign security responsibility

Security governance

- Security policy, prepared by CISO and approved by CIO
- Current security governance→ written by CISO in the past...
- S/T/O security activities→ from pick list
- Assign security responsibilities: action item for CISO and CIO
- Security governance prepared by CISO and approved by CIO

21

VERDONCK KLOOSTERS & ASSOCIATES



Determine relevant security controls

Determine ambition level

Assign security Responsibilities

Determine relevant security controls

Determine security services (technical and operations)

Security implementation guides

Security roadmap

Security ambition level

Security standard (best practices)

Standards from law and regulations

Advice from e.g. NCSC

Mapping threats to security controls

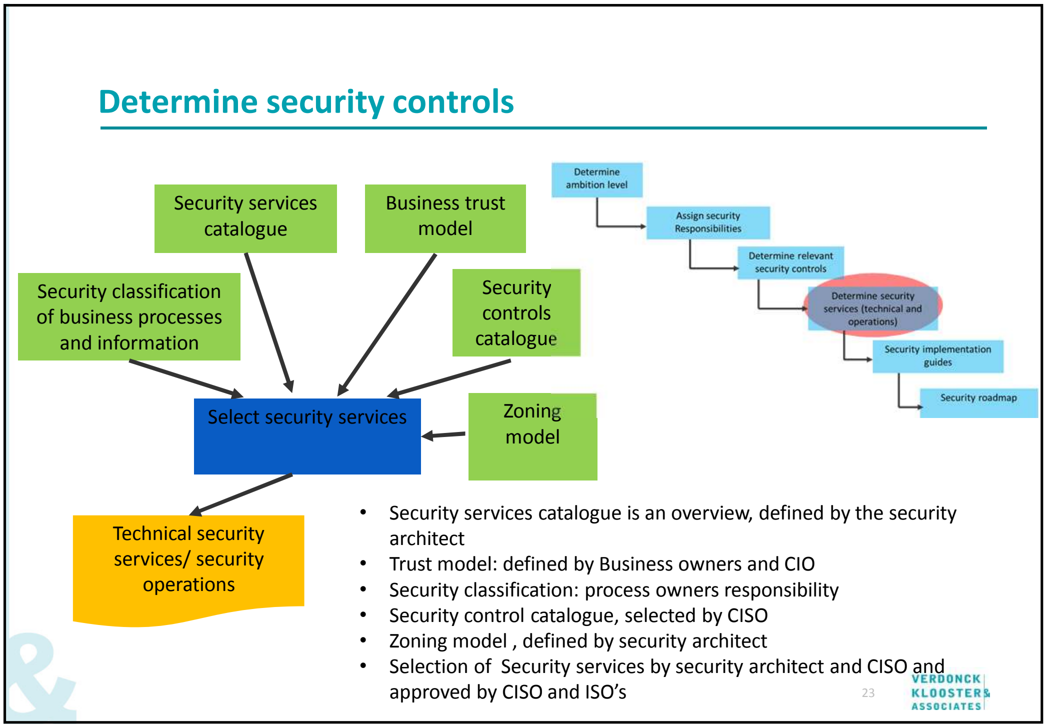
Trend analyses e.g. Gartner

Security controls

- Security ambition, previous step
- Security standards determined by CISO
- Use security standards from law and regulations, inspected by Legal
- Advice of NCSC, examine by CISO
- Trend analyses examine by security architect
- Mapping will take place in a workshop with: CISO, ISO's and Security architect
- Suggested security controls by CISO, approval by CIO

22

VERDONCK KLOOSTERS & ASSOCIATES



Determine security controls

Security services catalogue

Business trust model

Security classification of business processes and information

Security controls catalogue

Select security services

Zoning model

Technical security services/ security operations

Determine ambition level

Assign security Responsibilities

Determine relevant security controls

Determine security services (technical and operations)

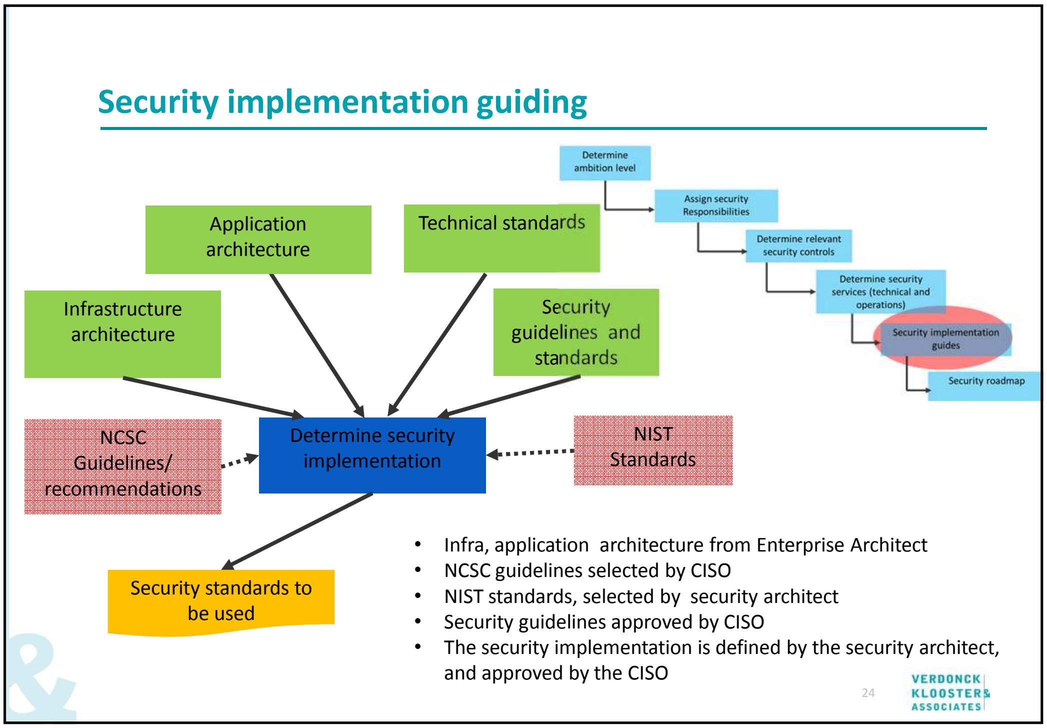
Security implementation guides

Security roadmap

- Security services catalogue is an overview, defined by the security architect
- Trust model: defined by Business owners and CIO
- Security classification: process owners responsibility
- Security control catalogue, selected by CISO
- Zoning model , defined by security architect
- Selection of Security services by security architect and CISO and approved by CISO and ISO's

23

VERDONCK KLOOSTER & ASSOCIATES



Security implementation guiding

Application architecture

Technical standards

Infrastructure architecture

Security guidelines and standards

NCSC Guidelines/ recommendations

Determine security implementation

NIST Standards

Security standards to be used

Determine ambition level

Assign security Responsibilities

Determine relevant security controls

Determine security services (technical and operations)

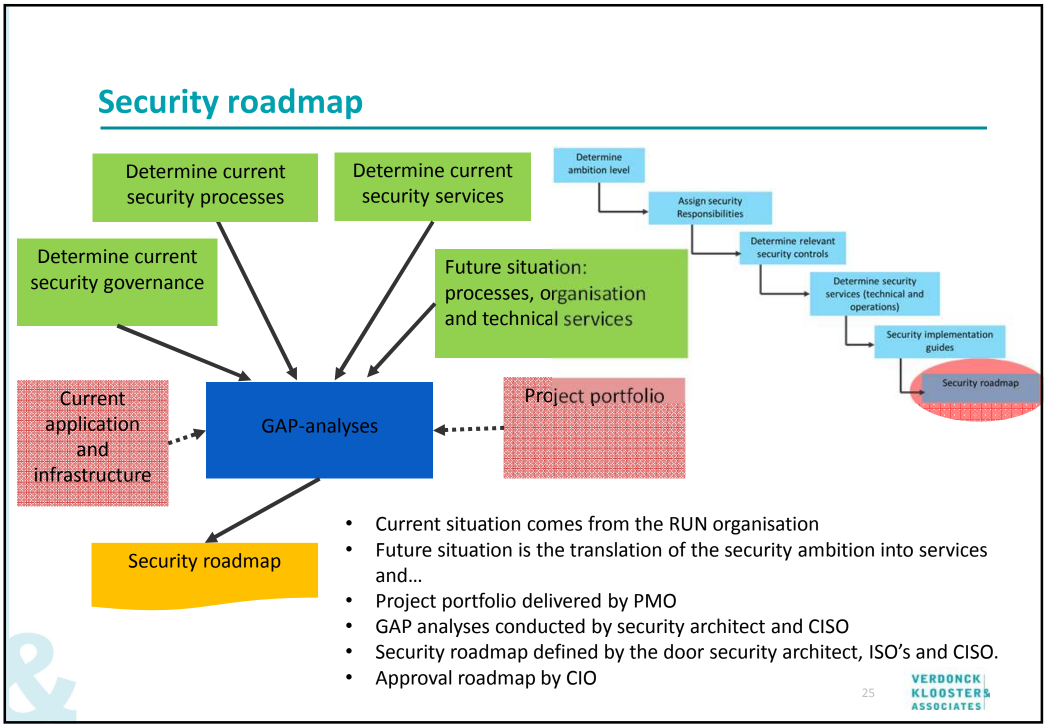
Security implementation guides

Security roadmap

- Infra, application architecture from Enterprise Architect
- NCSC guidelines selected by CISO
- NIST standards, selected by security architect
- Security guidelines approved by CISO
- The security implementation is defined by the security architect, and approved by the CISO

24

VERDONCK KLOOSTER & ASSOCIATES



Security roadmap

Determine current security processes

Determine current security services

Determine current security governance

Future situation: processes, organisation and technical services

Determine ambition level

Assign security Responsibilities

Determine relevant security controls

Determine security services (technical and operations)

Security implementation guides

Security roadmap

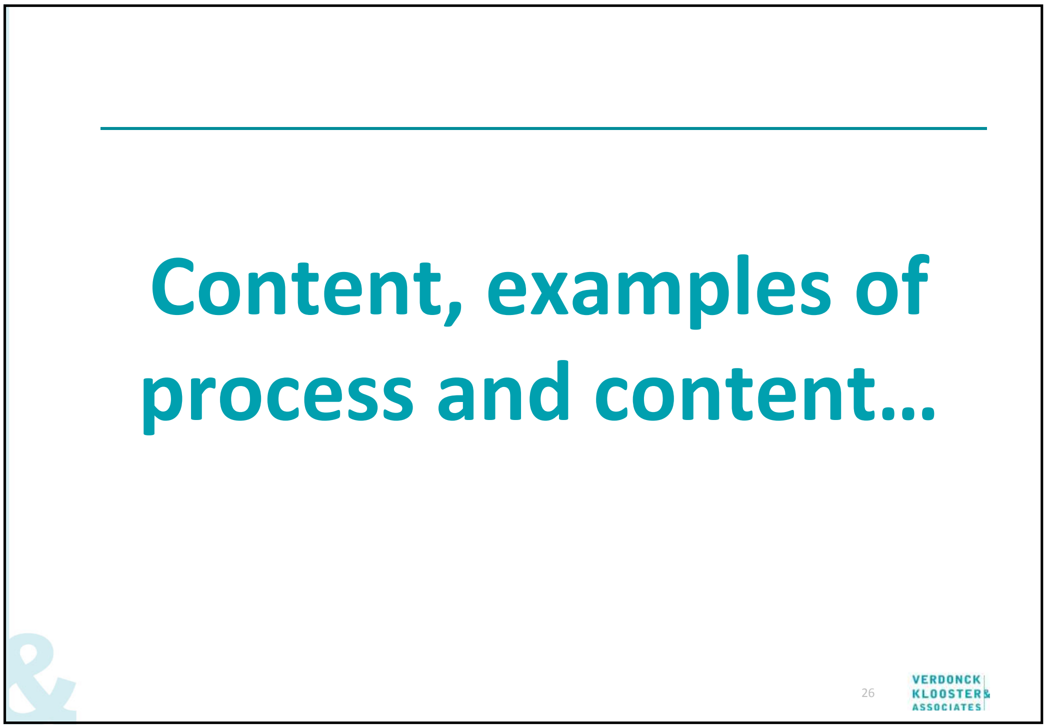
Current application and infrastructure

GAP-analyses

Project portfolio

Security roadmap

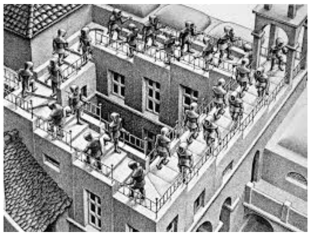
- Current situation comes from the RUN organisation
- Future situation is the translation of the security ambition into services and…
- Project portfolio delivered by PMO
- GAP analyses conducted by security architect and CISO
- Security roadmap defined by the door security architect, ISO's and CISO.
- Approval roadmap by CIO



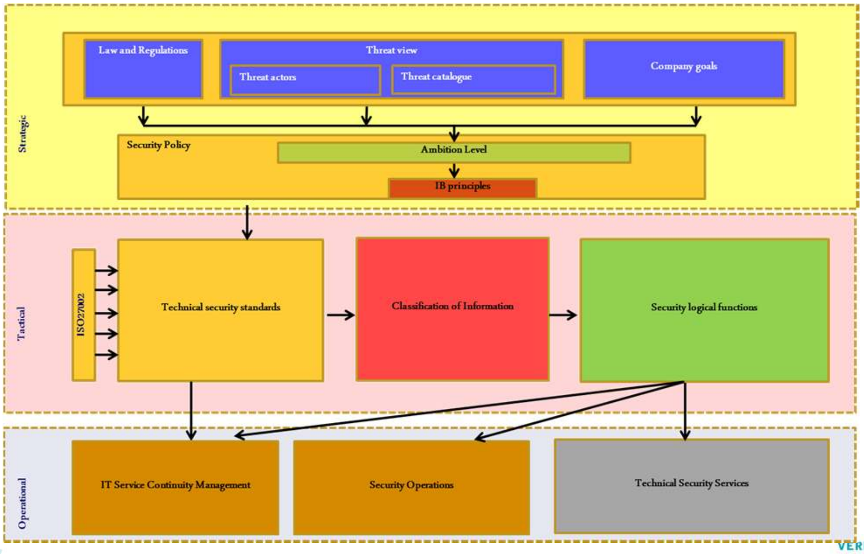
Content, examples of process and content…

Content

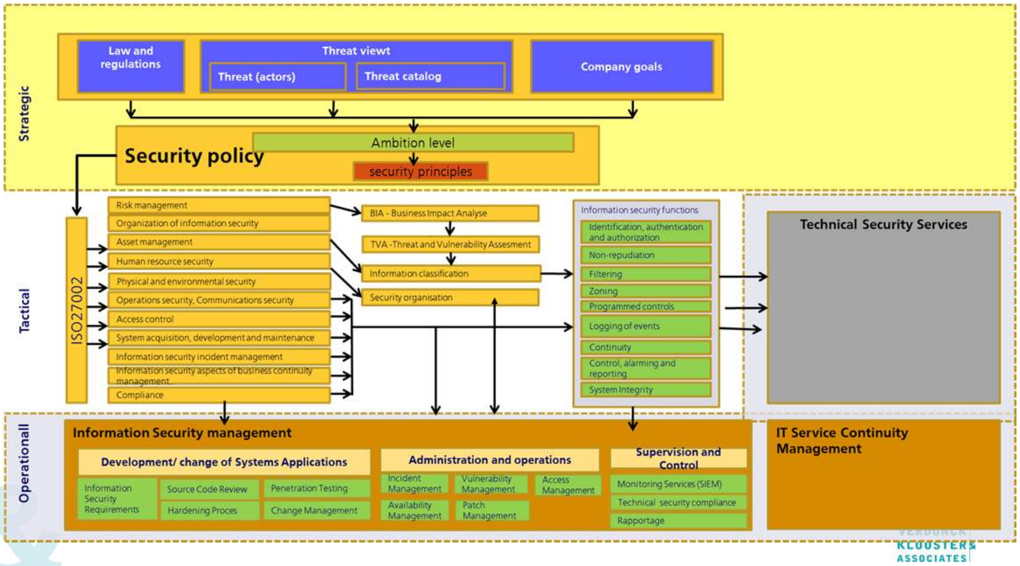
It is all about principles, models, standards, guidelines



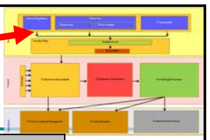
Content of a security architecture (high level)



In detail…


Strategic
Law and regulations
Threat viewt
Threat (actors)
Threat catalog
Company goals
Security policy
Ambition level
security principles
Tactical
ISO27002
Risk management
Organization of information security
Asset management
Human resource security
Physical and environmental security
Operations security, Communications security
Access control
System acquisition, development and maintenance
Information security incident management
Information security aspects of business continuity management
Compliance
BIA - Business Impact Analyse
TVA -Threat and Vulnerability Assesment
Information classification
Security organisation
Information security functions
Identification, authentication and authorization
Non-repudiation
Filtering
Zoning
Programmed controls
Logging of events
Continuity
Control, alarming and reporting
System Integrity
Technical Security Services
Operationall
Information Security management
Development/ change of Systems Applications
Information Security Requirements
Source Code Review
Penetration Testing
Hardening Proces
Change Management
Administration and operations
Incident Management
Vulnerability Management
Access Management
Availability Management
Patch Management
Supervision and Control
Monitoring Services (SIEM)
Technical security compliance
Rapportage
IT Service Continuity Management

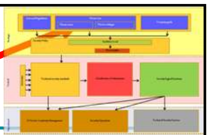
Law and regulations

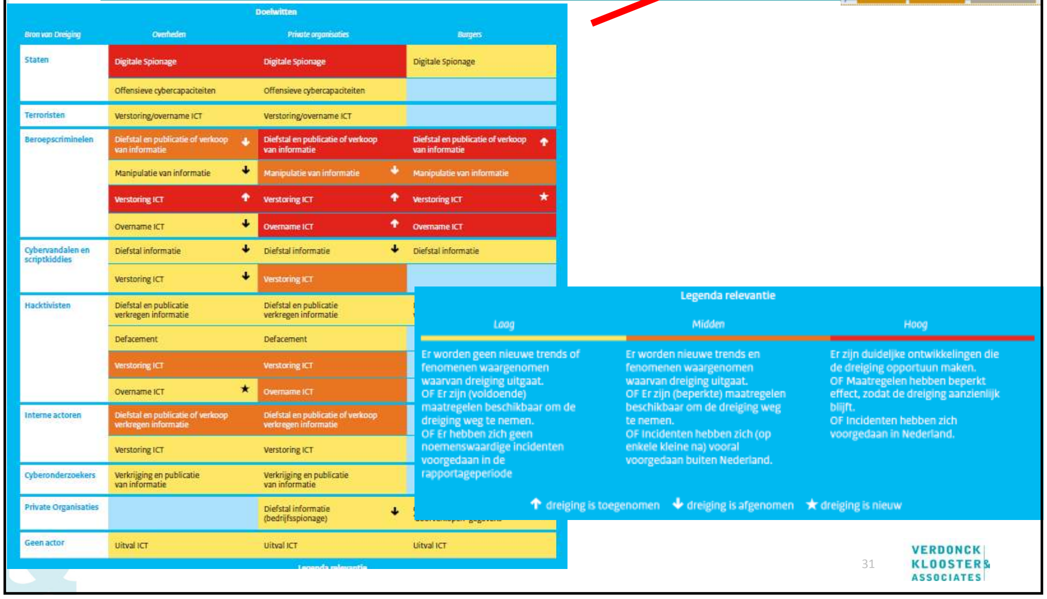


Law and regulations	Focus area	Implications	Principles/ solutions
Wbp : Privacy law	• Privacy aspects of data of customers and own staff. • The obligation to treat information carefully • Data leakage when information is compromised.	Level of security based on risk classification of the privacy information	Security is based on AV23.
WCC (I993) Law computer criminalities -I	• Computer intrusion. • Computer fraud • Computer terrorr	Tracability iof actions of personel should be described in HRM.	All personell actions must be tracebale to an individual person..
Law computer criminaliteit - II.	• E-Mail secret • SPAM • Organisational coorpreration in investigavtions	Disclaimer in e-mail of company so it is a formal statement.	All messages of teh company will be guided with covered juristriction.
PCI-DSS	• Credit card (CC) use, tranist and storga of CC information. • Use of Debitcards.	Comply to PCI-DSS requirements..	Security of PAN relatetd information and requirements for hardware and software uder for processen CC transactions. Active PCI monitoring.
Copyright law	• Software licences.	• Controle on use of illegal software. • Check on use of paid software.	The organisation will only allow formal licences of software.
Law on archiving	• Formulate CIA rating in recordmanagement.	• Preserve integrity on informatio during lifetime	Data will be protected during the whol elife cycle duet o the periods defined within the law.
Telecomwet	The organisatio as ISP for WIFI	Liability for WIFI services for customers!	• Compartiment for guest wifi use. • Logging of user activities.
Recordmanagement policy	Period of preserving information	Long-time storage and retrieval of information	Implement archiving function within the organisation

30

Dreigingsbeeld Nederland NCSC (2014)
Dutch threat report (1)





Doelwitten

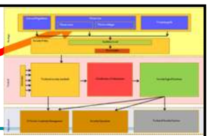
Bron van Dreiging	Overheden	Private organisaties	Burgers
Staten	Digitale Spionage	Digitale Spionage	Digitale Spionage
	Offensieve cybercapaciteiten	Offensieve cybercapaciteiten	
Terroristen	Verstoring/overname ICT	Verstoring/overname ICT	
Beroepscriminelen	Diefstal en publicatie of verkoop van informatie ↓	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie ↑
	Manipulatie van informatie ↓	Manipulatie van informatie ↓	Manipulatie van informatie
	Verstoring ICT ↑	Verstoring ICT ↑	Verstoring ICT ★
	Overname ICT ↓	Overname ICT ↑	Overname ICT
Cybervandalen en scriptkiddies	Diefstal informatie ↓	Diefstal informatie ↓	Diefstal informatie
	Verstoring ICT ↓	Verstoring ICT	
Hacktivisten	Diefstal en publicatie verkregen informatie	Diefstal en publicatie verkregen informatie	
	Defacement	Defacement	
	Verstoring ICT	Verstoring ICT	
	Overname ICT ★	Overname ICT	
Interne actoren	Diefstal en publicatie of verkoop verkregen informatie	Diefstal en publicatie of verkoop verkregen informatie	
	Verstoring ICT	Verstoring ICT	
Cyberonderzoekers	Verkrijging en publicatie van informatie	Verkrijging en publicatie van informatie	
Private Organisaties		Diefstal informatie (bedrijfsspionage) ↓	'doorverkopen' gegevens
Geen actor	Uitval ICT	Uitval ICT	Uitval ICT

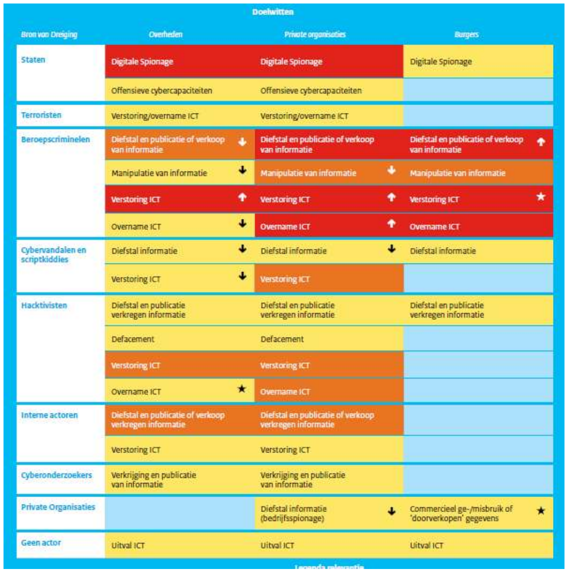
Legenda relevantie

Laag	Midden	Hoog
Er worden geen nieuwe trends of fenomenen waargenomen waarvan dreiging uitgaat. OF Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen. OF Er hebben zich geen noemenswaardige incidenten voorgedaan in de rapportageperiode	Er worden nieuwe trends en fenomenen waargenomen waarvan dreiging uitgaat. OF Er zijn (beperkte) maatregelen beschikbaar om de dreiging weg te nemen. OF Incidenten hebben zich (op enkele kleine na) vooral voorgedaan buiten Nederland.	Er zijn duidelijke ontwikkelingen die de dreiging opportuun maken. OF Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft. OF Incidenten hebben zich voorgedaan in Nederland.

↑ dreiging is toegenomen ↓ dreiging is afgenomen ★ dreiging is nieuw

Dreigingsbeeld Nederland NCSC (2014)
Dutch threat report (2)





Doelwitten

Bron van Dreiging	Overheden	Private organisaties	Burgers
Staten	Digitale Spionage	Digitale Spionage	Digitale Spionage
	Offensieve cybercapaciteiten	Offensieve cybercapaciteiten	
Terroristen	Verstoring/overname ICT	Verstoring/overname ICT	
Beroepscriminelen	Diefstal en publicatie of verkoop van informatie ↓	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie ↑
	Manipulatie van informatie ↓	Manipulatie van informatie ↓	Manipulatie van informatie
	Verstoring ICT ↑	Verstoring ICT ↑	Verstoring ICT ★
	Overname ICT ↓	Overname ICT ↑	Overname ICT
Cybervandalen en scriptkiddies	Diefstal informatie ↓	Diefstal informatie ↓	Diefstal informatie
	Verstoring ICT ↓	Verstoring ICT	
Hacktivisten	Diefstal en publicatie verkregen informatie	Diefstal en publicatie verkregen informatie	Diefstal en publicatie verkregen informatie
	Defacement	Defacement	
	Verstoring ICT	Verstoring ICT	
	Overname ICT ★	Overname ICT	
Interne actoren	Diefstal en publicatie of verkoop verkregen informatie	Diefstal en publicatie of verkoop verkregen informatie	
	Verstoring ICT	Verstoring ICT	
Cyberonderzoekers	Verkrijging en publicatie van informatie	Verkrijging en publicatie van informatie	
Private Organisaties		Diefstal informatie (bedrijfsspionage) ↓	Commercieel ge-/misbruik of 'doorverkopen' gegevens ★
Geen actor	Uitval ICT	Uitval ICT	Uitval ICT

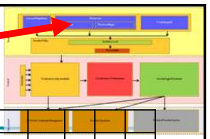
Legenda relevantie

Specifiek maken voor de organsiatie

Wel of niet tegen beveiligen? Basis of add-on?

Threat catalogs:
BSI www.bsi.de or ISF: www.securityforum.org

Threats and actors



	Threat type	Description										
Threat Category – External attack			Staten	Private Organsiaties	(Beroeps) criminelen	Terroristen	Hacktivisten	Scriptkiddies	Cyberonderz oekers	Interne factoren	Falen van IT	Geen Actor
T1	Carrying out denial of service attacks	Deliberately overloading systems and network devices or re-directing network traffic.	X	X	X	X	X	X				
T2	Hacking	Gaining unauthorised access to systems and networks.	X	X	X	X	X	X	X			
T3	Undertaking malicious probes or scans	Probes or scans of network devices and systems to gather information that could be used to undertake an attack.	X	X	X	X	X	X	X			
T4	Cracking passwords	Determining the plaintext version of an encrypted password.	X	X	X	X	X	X	X			
T5	Cracking keys	Determining the plaintext version of an encrypted key (eg WEP keys in wireless networks).	X	X	X	X	X	X	X			
T6	Defacing web sites	Unauthorised modification of web site content.	X	X	X	X	X	X				
T7	Spoofing web sites	The creation of a bogus web site that masquerades as a genuine web site to which users are directed.	X	X	X	X	X		X			
T8	Spoofing user identities	The unauthorised use of valid user identity information by a malicious external party to gain access to a system (typically as a result of 'identity theft').	X	X	X	X	X		X			
T9	Modifying network traffic	Falsifying the source or destination address of network traffic or modifying the content of network traffic in transit.	X	X	X	X			X			
T10	Eavesdropping	The unauthorised interception of information in transit.	X	X	X	X	X		X			
T11	Distributing computer viruses (including worms)	Self-replicating programs that propagate between systems and carry out an unauthorised action or set of actions (typically referred to as the payload).	X	X	X	X	X		X			
T12	Introducing Trojan horses	Computer code that masquerades as an authorised program but which carries out an unauthorised action (or set of actions).	X	X	X	X	X		X			
T13	Introducing malicious code	The introduction of malicious code (eg rootkits), malicious mobile code (eg unauthorised active content), spyware or adware.	X	X	X	X	X		X			
T14	Carrying out social engineering	The deliberate manipulation of staff to elicit information	X	X	X	X	X		X			

Security principles (1)

Benefit — **Ad principles for information security practitioners will help an organization**

Support the business

- Integrate information security into essential business activities
- Derive value from information security, helping to meet business requirements
- Meet statutory obligations, stakeholder expectations and avoid civil or criminal penalties
- Support business requirements and manage information risks
- Analyze and assess emerging information security threats
- Reduce costs, improve efficiency and enhance effectiveness

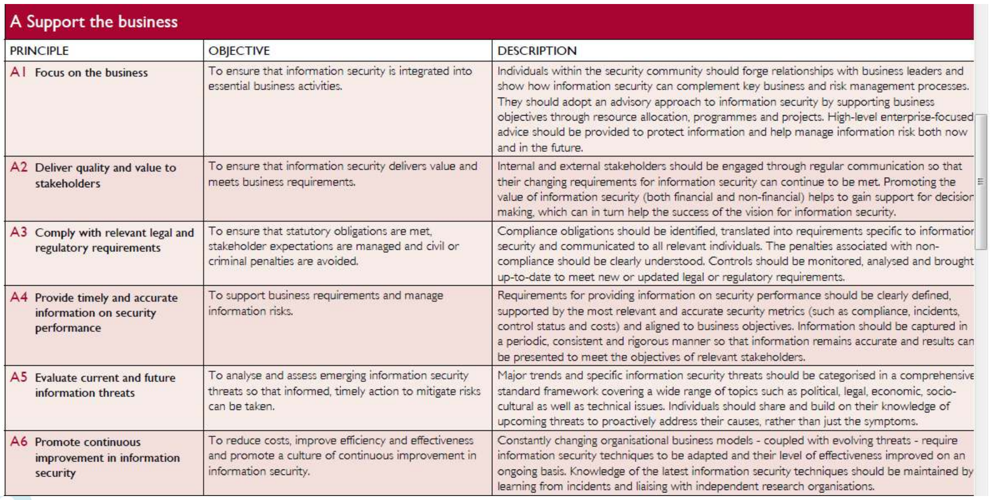
Defend the business

- Treat risks in a consistent and effective manner
- Prevent classified information (eg confidential or sensitive) being disclosed to unauthorized individuals
- Prioritize scarce information security resources by protecting those business applications where a security incident would have the greatest business impact
- Build quality, cost-effective systems upon which business people can rely (eg that are consistently robust, accurate and reliable)

Promote responsible security behaviour

- Perform information security-related activities in a reliable, responsible and effective manner
- Provide a positive security influence on the behavior of end users, reduce the likelihood of security incidents occurring, and limit their potential business impact.

Security principles (2)



A Support the business

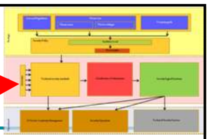
PRINCIPLE	OBJECTIVE	DESCRIPTION
A1 Focus on the business	To ensure that information security is integrated into essential business activities.	Individuals within the security community should forge relationships with business leaders and show how information security can complement key business and risk management processes. They should adopt an advisory approach to information security by supporting business objectives through resource allocation, programmes and projects. High-level enterprise-focused advice should be provided to protect information and help manage information risk both now and in the future.
A2 Deliver quality and value to stakeholders	To ensure that information security delivers value and meets business requirements.	Internal and external stakeholders should be engaged through regular communication so that their changing requirements for information security can continue to be met. Promoting the value of information security (both financial and non-financial) helps to gain support for decision making, which can in turn help the success of the vision for information security.
A3 Comply with relevant legal and regulatory requirements	To ensure that statutory obligations are met, stakeholder expectations are managed and civil or criminal penalties are avoided.	Compliance obligations should be identified, translated into requirements specific to information security and communicated to all relevant individuals. The penalties associated with non-compliance should be clearly understood. Controls should be monitored, analysed and brought up-to-date to meet new or updated legal or regulatory requirements.
A4 Provide timely and accurate information on security performance	To support business requirements and manage information risks.	Requirements for providing information on security performance should be clearly defined, supported by the most relevant and accurate security metrics (such as compliance, incidents, control status and costs) and aligned to business objectives. Information should be captured in a periodic, consistent and rigorous manner so that information remains accurate and results can be presented to meet the objectives of relevant stakeholders.
A5 Evaluate current and future information threats	To analyse and assess emerging information security threats so that informed, timely action to mitigate risks can be taken.	Major trends and specific information security threats should be categorised in a comprehensive standard framework covering a wide range of topics such as political, legal, economic, socio-cultural as well as technical issues. Individuals should share and build on their knowledge of upcoming threats to proactively address their causes, rather than just the symptoms.
A6 Promote continuous improvement in information security	To reduce costs, improve efficiency and effectiveness and promote a culture of continuous improvement in information security.	Constantly changing organisational business models - coupled with evolving threats - require information security techniques to be adapted and their level of effectiveness improved on an ongoing basis. Knowledge of the latest information security techniques should be maintained by learning from incidents and liaising with independent research organisations.

Make them organizational specific.....

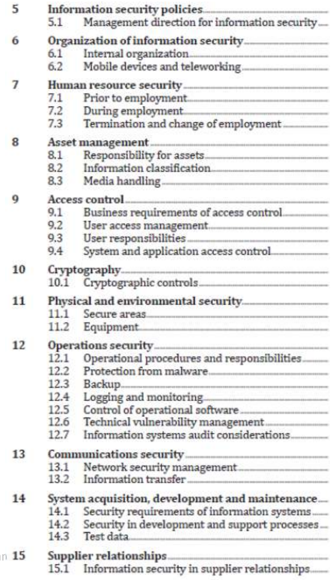
Security principles (3)

Security architecture principle	Explanation
Security by design	The security requirements of a system or application should be considered as part of its overall requirements (and not as an afterthought), to avoid wasting unnecessary time, money and effort.
Simplicity	By reducing the complexity and diversity of security controls, less mistakes and errors should occur. Simplicity of security controls should result in better understanding and management of security controls, and the prompt resolution of security-related issues.
Defence in depth	Using layers of security increases the level of effort required by an attacker to gain unauthorised access to a system or application. In the event one security control fails or is compromised, another security control should prevent the exposure of information or an information system.

Related principes linked to top 12 principles...



Controls: examples



5 **Information security policies**
5.1 Management direction for information security

6 **Organization of information security**
6.1 Internal organization
6.2 Mobile devices and teleworking

7 **Human resource security**
7.1 Prior to employment
7.2 During employment
7.3 Termination and change of employment

8 **Asset management**
8.1 Responsibility for assets
8.2 Information classification
8.3 Media handling

9 **Access control**
9.1 Business requirements of access control
9.2 User access management
9.3 User responsibilities
9.4 System and application access control

10 **Cryptography**
10.1 Cryptographic controls

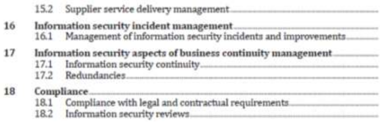
11 **Physical and environmental security**
11.1 Secure areas
11.2 Equipment

12 **Operations security**
12.1 Operational procedures and responsibilities
12.2 Protection from malware
12.3 Backup
12.4 Logging and monitoring
12.5 Control of operational software
12.6 Technical vulnerability management
12.7 Information systems audit considerations

13 **Communications security**
13.1 Network security management
13.2 Information transfer

14 **System acquisition, development and maintenance**
14.1 Security requirements of information systems
14.2 Security in development and support processes
14.3 Test data

15 **Supplier relationships**
15.1 Information security in supplier relationships



15.2 Supplier service delivery management

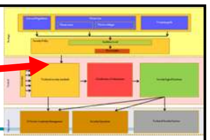
16 **Information security incident management**
16.1 Management of information security incidents and improvements

17 **Information security aspects of business continuity management**
17.1 Information security continuity
17.2 Redundancies

18 **Compliance**
18.1 Compliance with legal and contractual requirements
18.2 Information security reviews

- ISO 27001/2: www.iso.ch
- BSI: www.bsi.de
- ISF SoGP: www.securityforum.org
- CSA: CCM www.cloudsecurityalliance.org/ccm

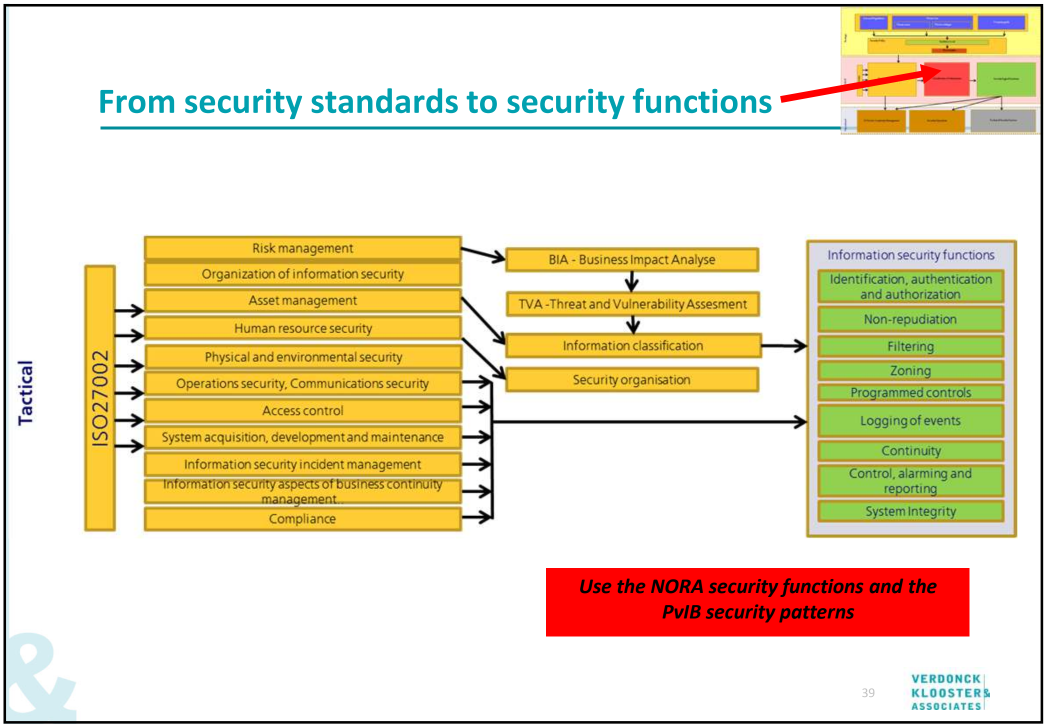
VERDONCK KLOOSTER & ASSOCIATES



Threats to controls?

Threats/ controls EXAMPLES….. ISO27002:2013 (about 133 contrl)	Digital espionage	Intrusions (malware/ spam)	Digital (identity) fraud	Disruption online services	Disruption critical infrastructure	black male	Sabotage	Publication of information	Acts of God	Hardware or software failures
9.1 Business requirements of access control	v		v					v		
9.2 User access management			v					v		
9.3 User responsibilities		v				v		v		
9.4 System and application access control			v					v		
12.1 Operational procedures and responsibilities			v					v		
12.2 Protection from malware		v								
12.3 Backup				v					v	v
12.4 Logging and monitoring	V		V							v
12.5 Control of operational software		v								
12.6 Technical vulnerability Management	V	v		v						
12.7 Information systems audit considerations					v					
17.1 Information security continuity					v				v	v
17.2 Redundancies					v				v	v

VERDONCK KLOOSTER & ASSOCIATES



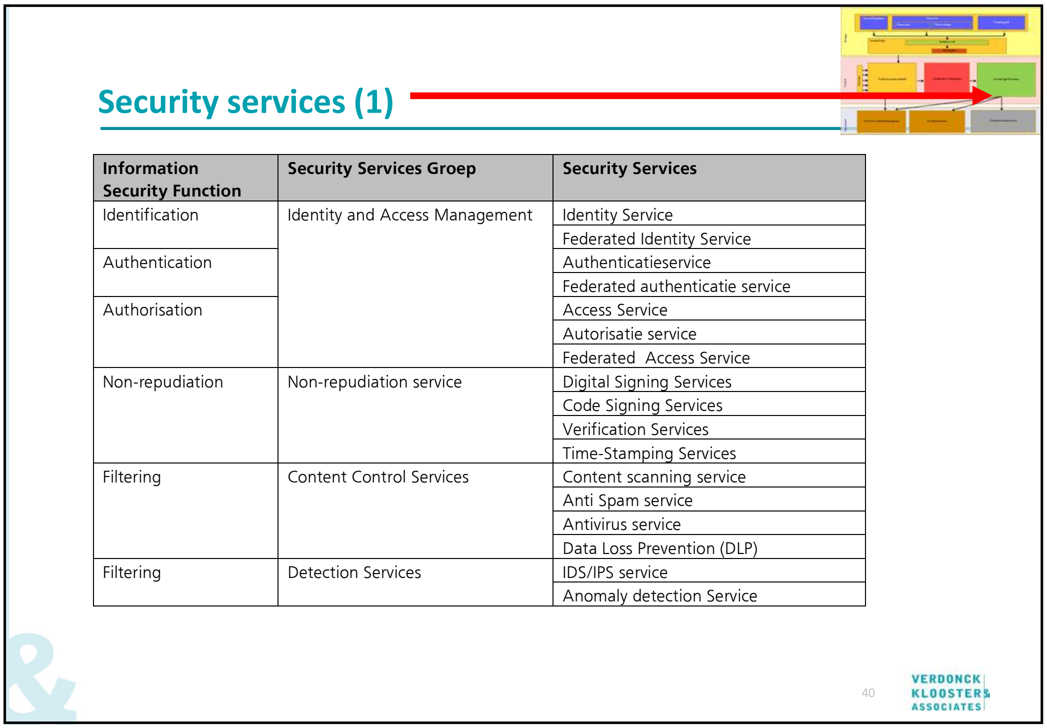
From security standards to security functions

Tactical
ISO27002
Risk management
Organization of information security
Asset management
Human resource security
Physical and environmental security
Operations security, Communications security
Access control
System acquisition, development and maintenance
Information security incident management
Information security aspects of business continuity management
Compliance
BIA - Business Impact Analyse
TVA -Threat and Vulnerability Assesment
Information classification
Security organisation
Information security functions
Identification, authentication and authorization
Non-repudiation
Filtering
Zoning
Programmed controls
Logging of events
Continuity
Control, alarming and reporting
System Integrity

Use the NORA security functions and the PvIB security patterns

39

VERDONCK KLOOSTERS & ASSOCIATES



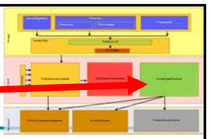
Security services (1)

Information Security Function	Security Services Groep	Security Services
Identification	Identity and Access Management	Identity Service
		Federated Identity Service
Authentication		Authenticatieservice
		Federated authenticatie service
Authorisation		Access Service
		Autorisatie service
		Federated Access Service
Non-repudiation	Non-repudiation service	Digital Signing Services
		Code Signing Services
		Verification Services
		Time-Stamping Services
Filtering	Content Control Services	Content scanning service
		Anti Spam service
		Antivirus service
		Data Loss Prevention (DLP)
Filtering	Detection Services	IDS/IPS service
		Anomaly detection Service

40

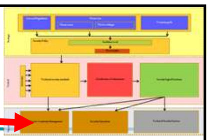
VERDONCK KLOOSTERS & ASSOCIATES

Security services (2)

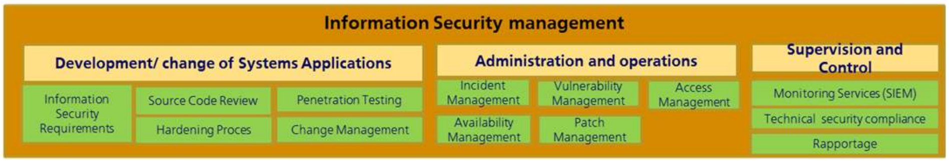


Information Security Function	Security Services Groep	Security Services
Zoning	Boundary Protection Services	Packet Filtering Service
		Proxy/ reverse proxy service
		Web Application Firewall Service
	Crypto Services	Crypto Service (in transit)
		Crypto Service (in use)
		Crypto service (in storage)
		Crypto key management Service
		PKI services
		DRM services
		Secure Erase (storage)
		Secure Zone Services
Programmed application controls	Tbd	Tbd (geprog. controles)
Control Alarming and reporting	Monitoring Services	Audit service
		Reporting Service
		SIEM Service
Logging of events		Loging service
System integrity	System Integrity Services	OS-code integrity check
Continuity	Availability Services	Backup-restore service
		Data replicatie service
		Redundancy Service
		Load balancing Service
		DRP service

Security Services (3)



Operationall



Information Security management

Development/ change of Systems Applications
- Information Security Requirements
- Source Code Review
- Penetration Testing
- Hardening Proces
- Change Management

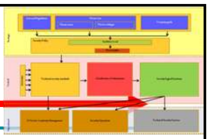
Administration and operations
- Incident Management
- Vulnerability Management
- Access Management
- Availability Management
- Patch Management

Supervision and Control
- Monitoring Services (SIEM)
- Technical security compliance
- Rapportage

Are you doing it yourself, or through an outsourced ICT supplier or a specific Security Operations Center (SOC)?

Keep it simple: ITIL v3 security mangement is not yet compleet!

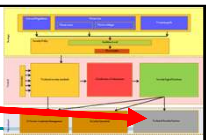
ISO 27002 standard /security services



				Identity Services (directory services)	Authentication Services	Authorization Services	Federation Services	Access Co
10.9.3	Openbaar beschikbare informatie		x					
10.10	Controle							
10.10.1	Aanmaken audit logbestanden		x	X	X	X		X
10.10.2	Contole van systeemgebruik		x			X		
10.10.3	Bescherming van informatie in logbestanden		x					
10.10.4	Logbestanden van administrators en operators		x			X		X
10.10.5	Registratie van storingen		x					
10.10.6	Synchronisatie van systeemklokken		x					
11	Toegangsbeveiliging							
11.1	Bedrijfseisen ten aanzien van toegangsbeheersing							
11.1.1	Toegangsbeleid	x	x					
11.2	Beheer van toegangsrechten van gebruikers							
11.2.1	Registratie van gebruikers	x	x	X	X	X		X
11.2.2	Beheer van speciale bevoegdheden	x	x	X	X	X		X
11.2.3	Beheer van gebruikerswachtwoorden		x		X			
11.2.4	Beoordeling van toegangsrechten van gebruikers	x	x			X		
11.3	Verantwoordelijkheden van gebruikers							
11.3.1	Gebruik van wachtwoorden	x	x		X			
11.3.2	Onbeheerde gebruikersapparatuur	x	x		X			
11.3.3	Clear desk en clear screen beleid	x	x		X			
11.4	Toegangsbeheersing voor netwerken							
11.4.1	Beleid ten aanzien van het gebruik van netwerkdiensten	X	x					
11.4.2	Authenticatie van gebruikers bij externe verbindingen		x		X		X	
11.4.3	Identificatie van netwerkapparatuur		x	X				

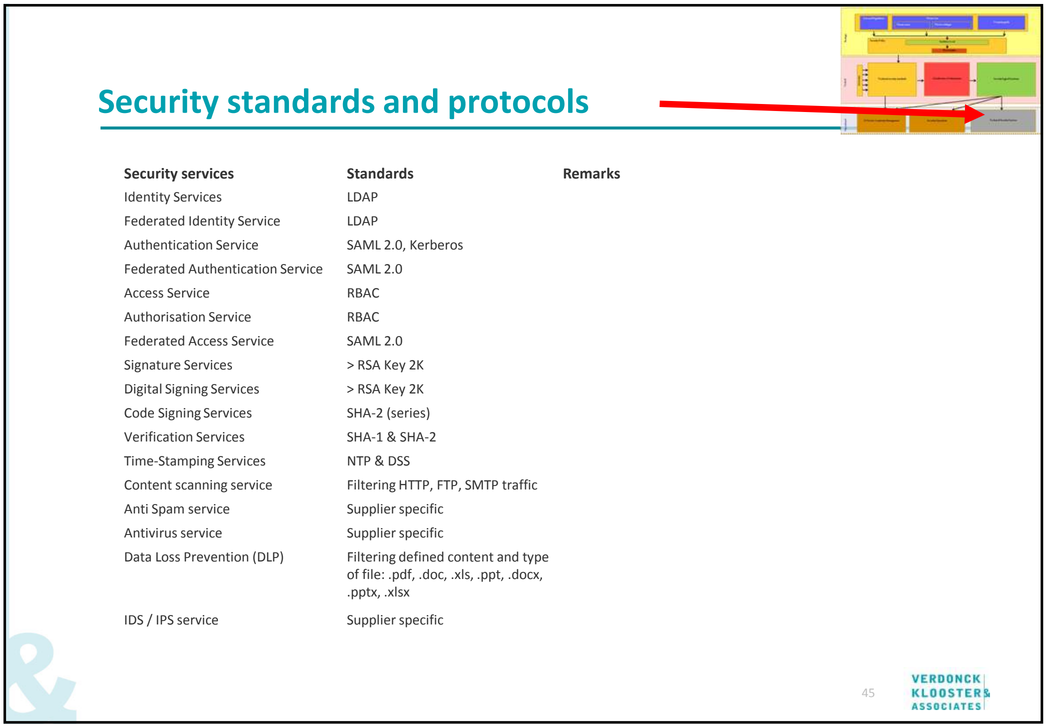
VERDONCK KLOOSTER& ASSOCIATES

Security services within the OSI stack



IS Function	Security Services Group	Security Services	Data	Applications	Middleware	Network	Platform	Storage	Workstation
	repudiation service	Services							
	Non-repudiation service	Verification Services	V	V					
	Non-repudiation service	Time-Stamping Services	V	V					
Filtering	Content Control Services	Content Scanning Service		V		V			
	Content Control Services	Anti Spam Service				V			
	Content Control Services	Antivirus Service		V			V		V
	Content Control Services	Data Loss Prevention (DLP)	V						V
Filtering	Detection Services	IDS / IPS Service		V	V	V	V		
	Detection Services	Anomaly Detection Service		V		V	V		
Zoning	Boundary Protection Services	Packet Filtering Service				V			
	Boundary Protection Services	Proxy / Reverse proxy Service				V			

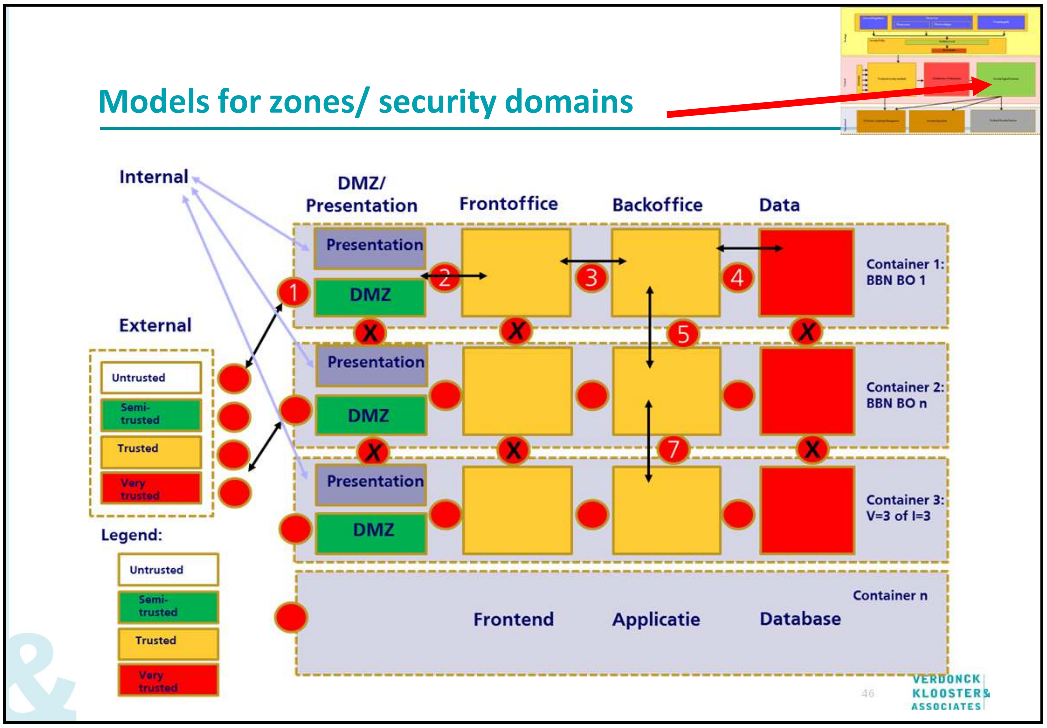
VERDONCK KLOOSTER& ASSOCIATES



Security standards and protocols

Security services	Standards	Remarks
Identity Services	LDAP	
Federated Identity Service	LDAP	
Authentication Service	SAML 2.0, Kerberos	
Federated Authentication Service	SAML 2.0	
Access Service	RBAC	
Authorisation Service	RBAC	
Federated Access Service	SAML 2.0	
Signature Services	> RSA Key 2K	
Digital Signing Services	> RSA Key 2K	
Code Signing Services	SHA-2 (series)	
Verification Services	SHA-1 & SHA-2	
Time-Stamping Services	NTP & DSS	
Content scanning service	Filtering HTTP, FTP, SMTP traffic	
Anti Spam service	Supplier specific	
Antivirus service	Supplier specific	
Data Loss Prevention (DLP)	Filtering defined content and type of file: .pdf, .doc, .xls, .ppt, .docx, .pptx, .xlsx	
IDS / IPS service	Supplier specific	

VERDONCK KLOOSTERS ASSOCIATES



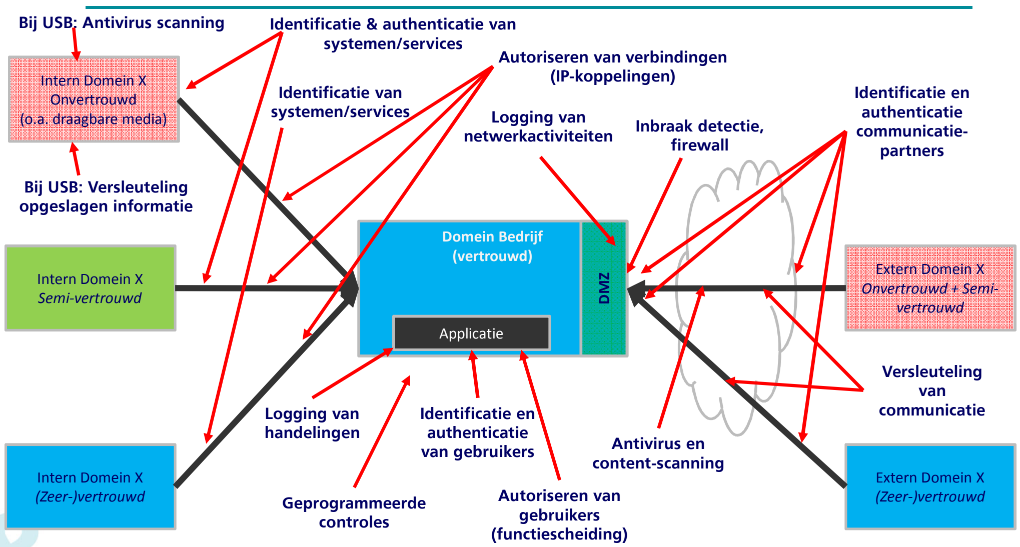
Models for zones/ security domains

Legend:

- 🟦 Untrusted
- 🟩 Semi-trusted
- 🟨 Trusted
- 🟥 Very trusted

VERDONCK KLOOSTERS ASSOCIATES

Waar security functies te gebruiken?



Bij USB: Antivirus scanning

Intern Domein X
Onvertrouwd
(o.a. draagbare media)

Bij USB: Versleuteling opgeslagen informatie

Intern Domein X
Semi-vertrouwd

Intern Domein X
(Zeer-)vertrouwd

Identificatie & authenticatie van systemen/services

Identificatie van systemen/services

Autoriseren van verbindingen (IP-koppelingen)

Logging van netwerkactiviteiten

Inbraak detectie, firewall

Identificatie en authenticatie communicatie-partners

Domein Bedrijf
(vertrouwd)

DMZ

Applicatie

Extern Domein X
Onvertrouwd + Semi-vertrouwd

Versleuteling van communicatie

Extern Domein X
(Zeer-)vertrouwd

Logging van handelingen

Identificatie en authenticatie van gebruikers

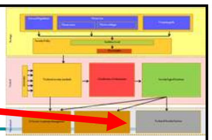
Antivirus en content-scanning

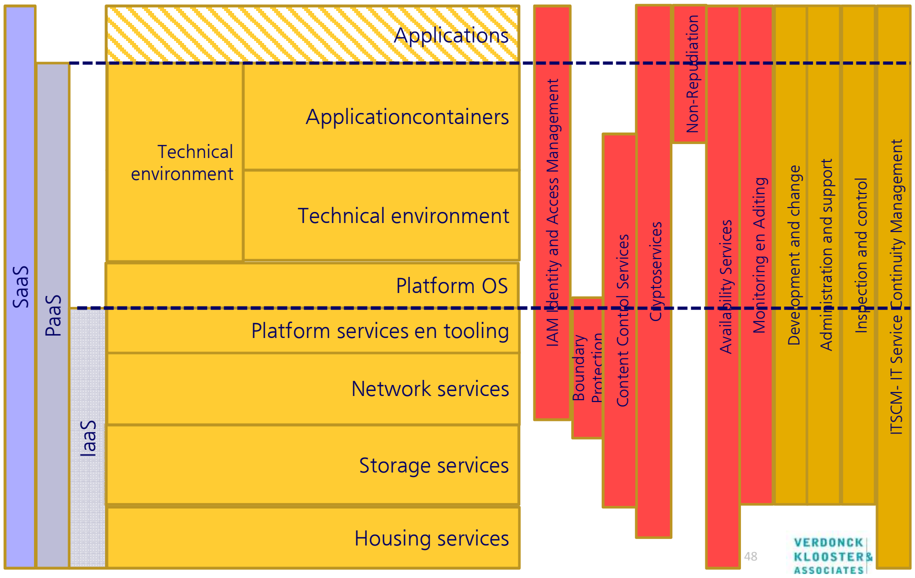
Geprogrammeerde controles

Autoriseren van gebruikers (functiescheiding)

Connect to generic security services like: IAM en SIEM

Security services and cloud





SaaS

PaaS

IaaS

Applications

Technical environment

Applicationcontainers

Technical environment

Platform OS

Platform services en tooling

Network services

Storage services

Housing services

IAM Identity and Access Management

Boundary Protection

Content Control Services

Cryptoservices

Non-Repudiation

Availability Services

Monitoring en Aditing

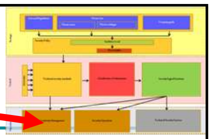
Development and change

Administration and support

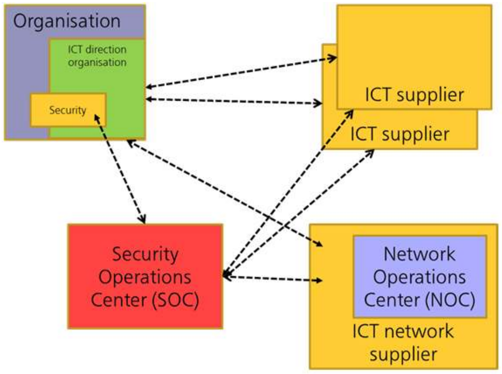
Inspection and control

ITSCM- IT Service Continuity Management

48



Security services (positioning of the SOC?)


Organisation
ICT direction organisation
Security
ICT supplier
ICT supplier
Security Operations Center (SOC)
Network Operations Center (NOC)
ICT network supplier

Operationall

Information Security management

Development/ change of Systems Applications

- Information Security Requirements
- Source Code Review
- Penetration Testing
- Hardening Proces
- Change Management

Administration and operations

- Incident Management
- Vulnerability Management
- Access Management
- Availability Management
- Patch Management

Supervision and Control

- Monitoring Services (SIEM)
- Technical security compliance
- Rapportage

VERDONCK KLOOSTERS & ASSOCIATES

Use of architectures in projects?

VERDONCK KLOOSTERS & ASSOCIATES

Use of architectures -1

For realizing programs and projects:

- Reference architecture as a starting point
- A project realizes a just a part of the reference architecture
- For defining a roadmap for realisation
- Support a logical grow in maturity
- Cost and budget estimations

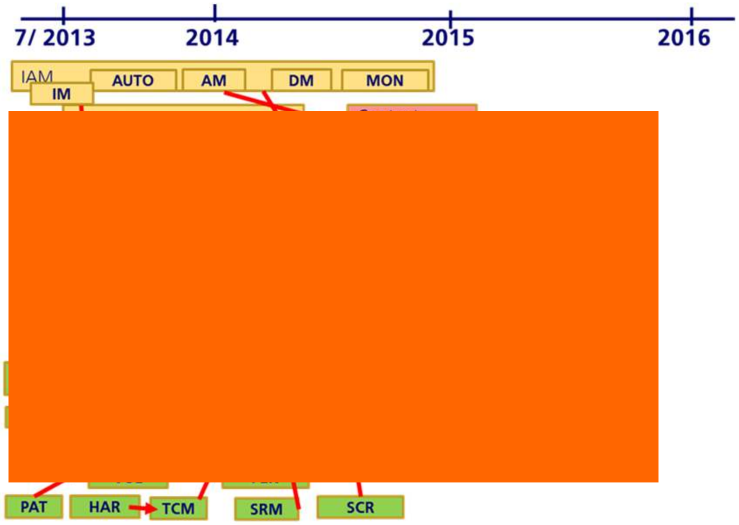
Project steering by

- PID: Project Initiation Document : **Process**
- PSA: Project Start Architecture: **Content (quality)**

- A PSA will be describes using part of all different sorts of reference architectures

51

Use of architecture-2: Projects and dependencies



[redacted]

Use of architecture -3 : Maturity on security topics

Fase 1: Basiscapaciteit | Fase 2: Gevorderde capaciteit | Fase 3: Volwassenheid

2014	2015	2016

INCIDENT RESPONSE

MONITORING

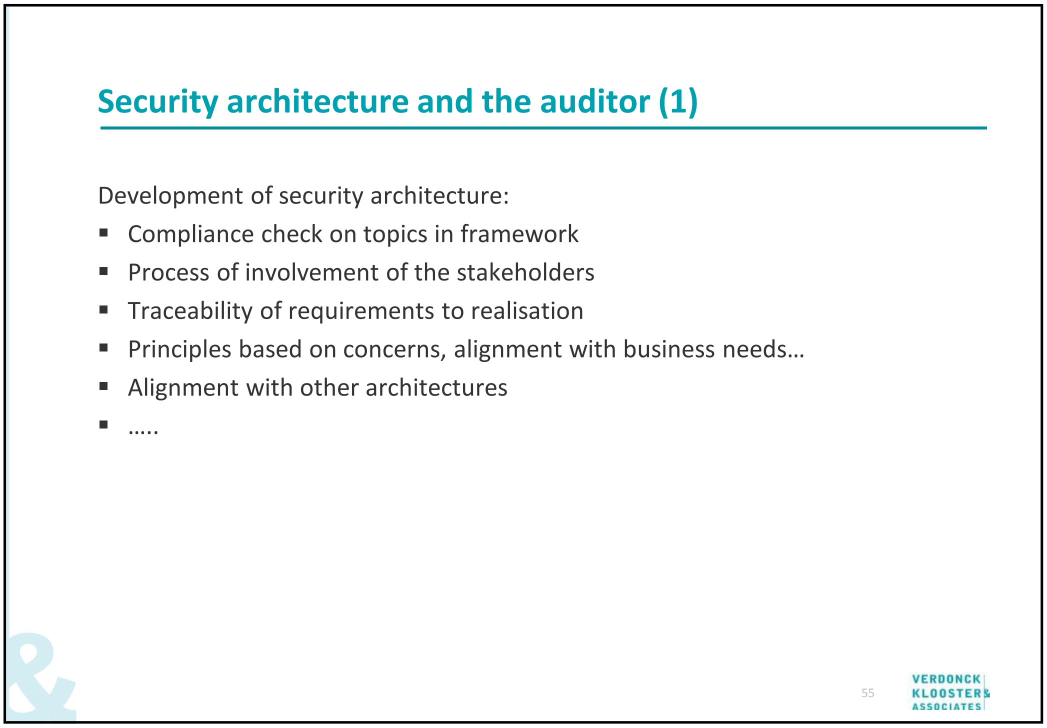
BASIS PROCESSEN

[redacted]

53

Use of architecture - 5: Cost of security through the years

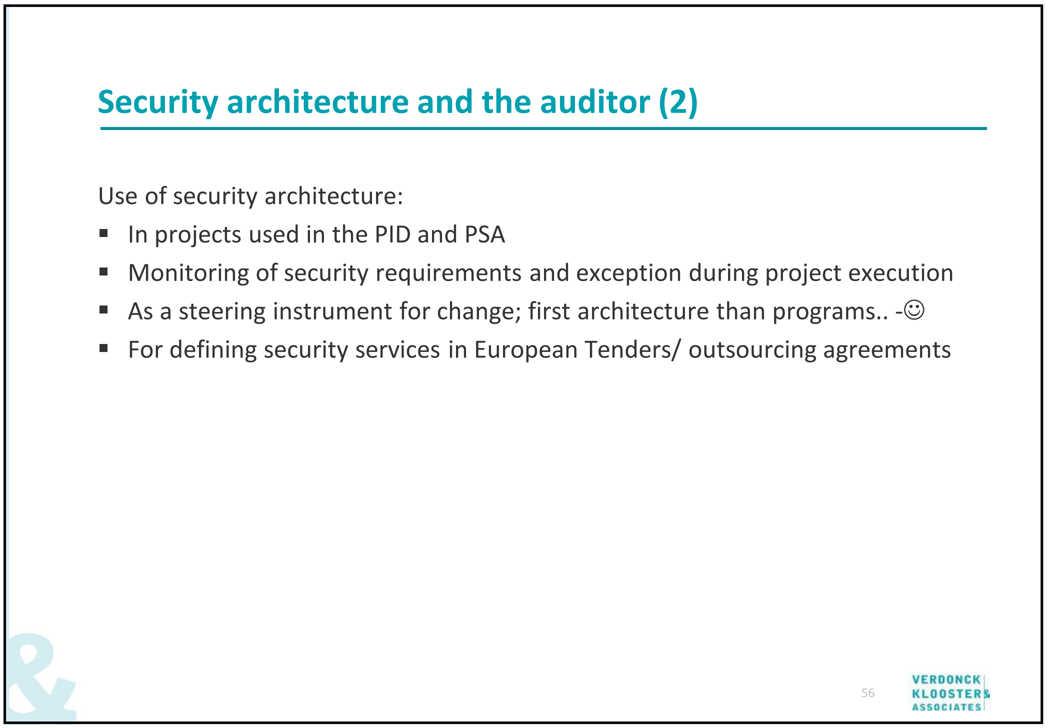
Maatregelenset		
Incident Response		[redacted]
	Investering	[redacted]
	Projecturen	[redacted]
	Onderhoud	[redacted]
	FTE	[redacted]
Monitoring		[redacted]
	Investering	[redacted]
	Projecturen	[redacted]
	Onderhoud	[redacted]
	FTE	[redacted]
IAM		[redacted]
	Investering	[redacted]
	Projecturen	[redacted]
	Onderhoud	[redacted]
	FTE	[redacted]
Basis Security Processen		[redacted]
	Investering	[redacted]
	Projecturen	[redacted]
	Onderhoud	[redacted]
	FTE	[redacted]
Infrastructuur		[redacted]
	Investering	[redacted]
	Projecturen	[redacted]
	Onderhoud	[redacted]
	FTE	[redacted]
Totalen		[redacted]
	Investering	[redacted]
	Projecturen	[redacted]
	Onderhoud	[redacted]
	FTE	[redacted]
		[redacted]
Parameters	Uurtarief	[redacted]
	FTE tarief	[redacted]
	Onderhoud	[redacted]



Security architecture and the auditor (1)

Development of security architecture:

- Compliance check on topics in framework
- Process of involvement of the stakeholders
- Traceability of requirements to realisation
- Principles based on concerns, alignment with business needs…
- Alignment with other architectures
- …..



Security architecture and the auditor (2)

Use of security architecture:

- In projects used in the PID and PSA
- Monitoring of security requirements and exception during project execution
- As a steering instrument for change; first architecture than programs.. -☺
- For defining security services in European Tenders/ outsourcing agreements

Security architecture and the auditor (3)

Maintenance on security architecture:

- Based on business changes (not foreseen in the plan period), Mergers and acquisitions
- Security policy changes
- Chances threat landscape (actors, motivation)
- Changes in other architectures (alignment)

As an auditor you can do much more, but if these topics are addressed the organization has made a great maturity step compared to the way it really works in practice…

Questions

There is never time enough to explain it all..

There is never time and money enough to do the right thing, there is always time and money for doing it again..

E-mail: Renato.kuiper@vka.nl