Guest lecture

INFOB3INSE

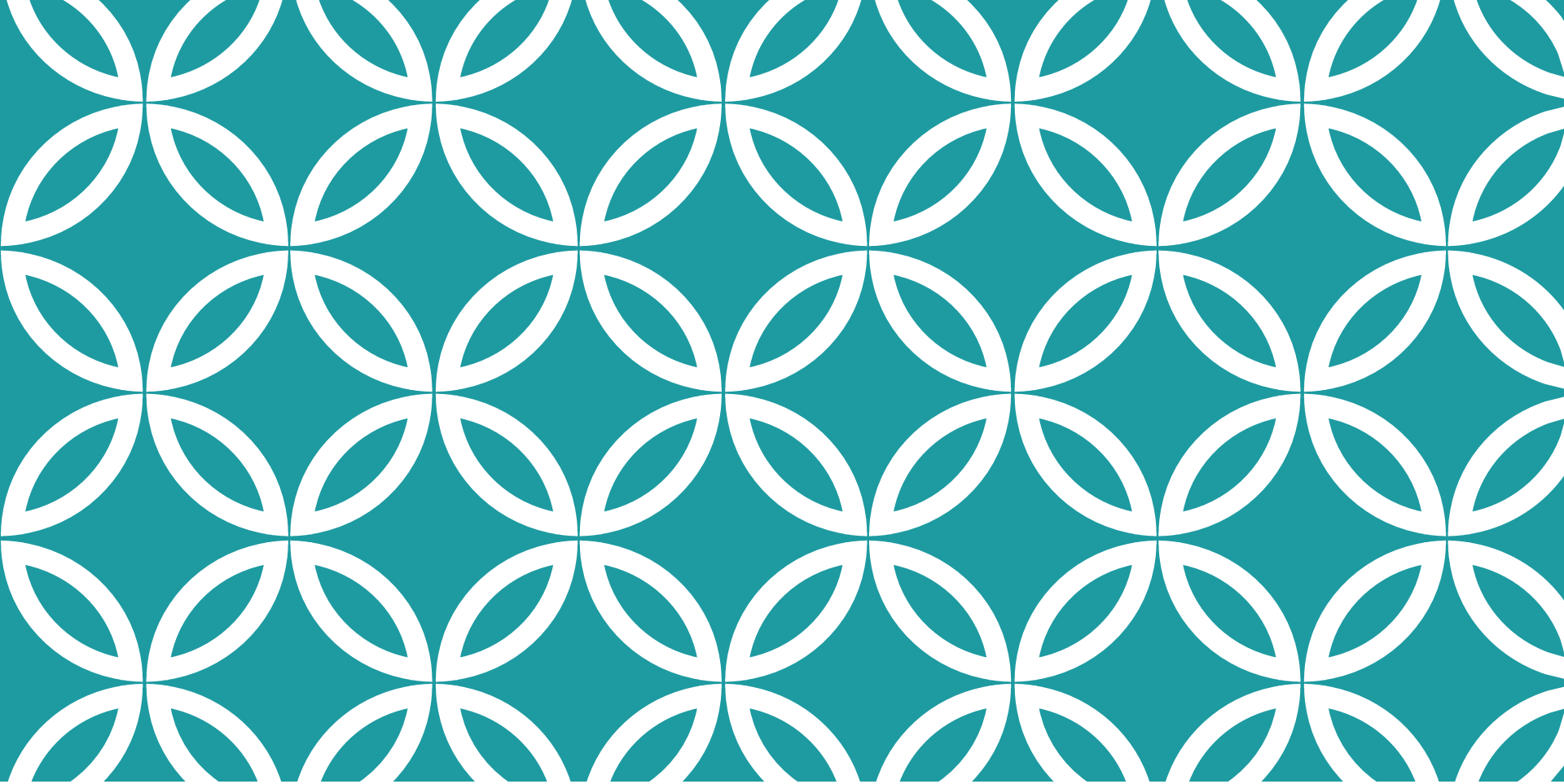
A maturity modeling approach of information security management

TOWARDS PERSONALISED INFORMATION SECURITY ADVICE

Dr. Marco Spruit

AGENDA

1. Spruit,M., & Roeling,M. (2014). *ISFAM: the Information Security Focus Area Maturity model*. 22nd European Conference on Information Systems. Tel Aviv, Israel. [pdf] [online]
2. Bek,L. (2014/06/27). Situationele factoren in cybersecurity.
3. Mijnhardt,F., Baars,T., & Spruit,M. (2016). Organizational Characteristics Influencing SME Information Security Maturity. *Journal of Computer Information Systems, 56*(2), 106-115. [pdf] [online]
4. Baars,T. (2014/09/23). *An Argument for Adaptive Maturity Frameworks by means of Organizational Characteristics*. (Duo project with F. Mijnhardt). Submitted.
5. Slot,G. (2015/07/14). Towards Rule-based Information Security Maturity.
6. Lingen,S. van (2015/01/30). Towards a Federative Information Security Focus Area Maturity Model.



0. PREFACE

Why a maturity model approach?

ORIGINAL GOAL OF ROELING (2010)

"How and by what means can the **gap** between business requirements with respect to information security and the actual level of Information security be minimized or closed?"

- Criteria
  - Define metrics to measure a gap
  - Identify the extensiveness of the gap
  - Represent a gap by a comprehensive model
  - Close the gap by being able to define a roadmap based on the representation
  - Decide on where to go after closing the gap
  - Determine how to take the next step

BUT… HOW TO DO IT?

4 possible solutions

- … a Gap Analysis?
- … a Dashboard?
- … a Maturity Model?
- … a List of metrics?

DEFINING METRICS & IDENTIFYING A GAP

	Gap analysis	Dashboard	Maturity model	List of metrics
Defining metrics	A Gap analysis does not necessarily define metrics. Since defining metrics for information security is one of the sub goals of this research gap analysis alone might not be a good solution.	To make a proper dashboard, metrics are needed. The results of the metrics are represented on the dashboard. Dashboards are mostly used for representing KPIs .	Metrics are needed to determine the level of maturity. All kinds of metrics can be presented in a maturity model	This is a good solution for defining metrics.
Identifying a gap	Gap analysis is good in identifying a gap.	A dashboard only measures the as-is situation and is therefore not able to identify a gap.	A maturity model, when presented to different roles in the organization, can lead to different results which indicate a gap.	A list of metrics, when presented to different roles in the organization, can lead to different results which indicate a gap.

CLOSING A GAP & MANAGERIAL REPRESENTATION

	Gap analysis	Dashboard	Maturity model	List of metrics
Closing a gap	Gap analysis does not suggest any solutions to the gap.	A dashboard does not identify a gap and is therefore also not able to close it.	The results from the gap identification can be used to close the gap and increase corporate knowledge.	The results from the gap identification can be used to close the gap and increase corporate knowledge.
Managerial representation (representing a gap)	Gap analysis does provide value to the business but does not provide a solution to the business.	A dashboard helps a manager get a quick overview of what is going on.	A maturity model gives an overview of where an organization is and where it should be going in a structured way.	A list of metrics is not supporting a manager in efficiently doing his tasks.

Roeling,M. (2012/08/28). Towards an aligned organization on Information Security - Closing the gap between the actual level of information security and business information security requirements.

STRATEGIC VALUE & GUIDELINE/ADVICE

	Gap analysis	Dashboard	Maturity model	List of metrics
Strategic/ tactical Value	Gap analysis can be of strategic value when talking about a gap between what a customer wants and what is already there. This gap is almost the same as in my case (only internal).	A dashboard can help setting up tactical or strategic goals when targets are included on the dashboard.	A maturity model helps in determining the next steps in becoming mature.	A list of metrics is not suggesting or presenting any tactical or strategic advantages. It represents the as-is situation.
Guideline	A gap analysis does not tell you what to do in the next years.	A dashboard does not guide an organization; it only shows what is going right and wrong.	A maturity model shows the best practice of what to do next to the benefit of the organization.	A list of metrics has a limited guidance. It can show bad results but does not relate them to other metrics.

TYPES OF MATURITY MODELS

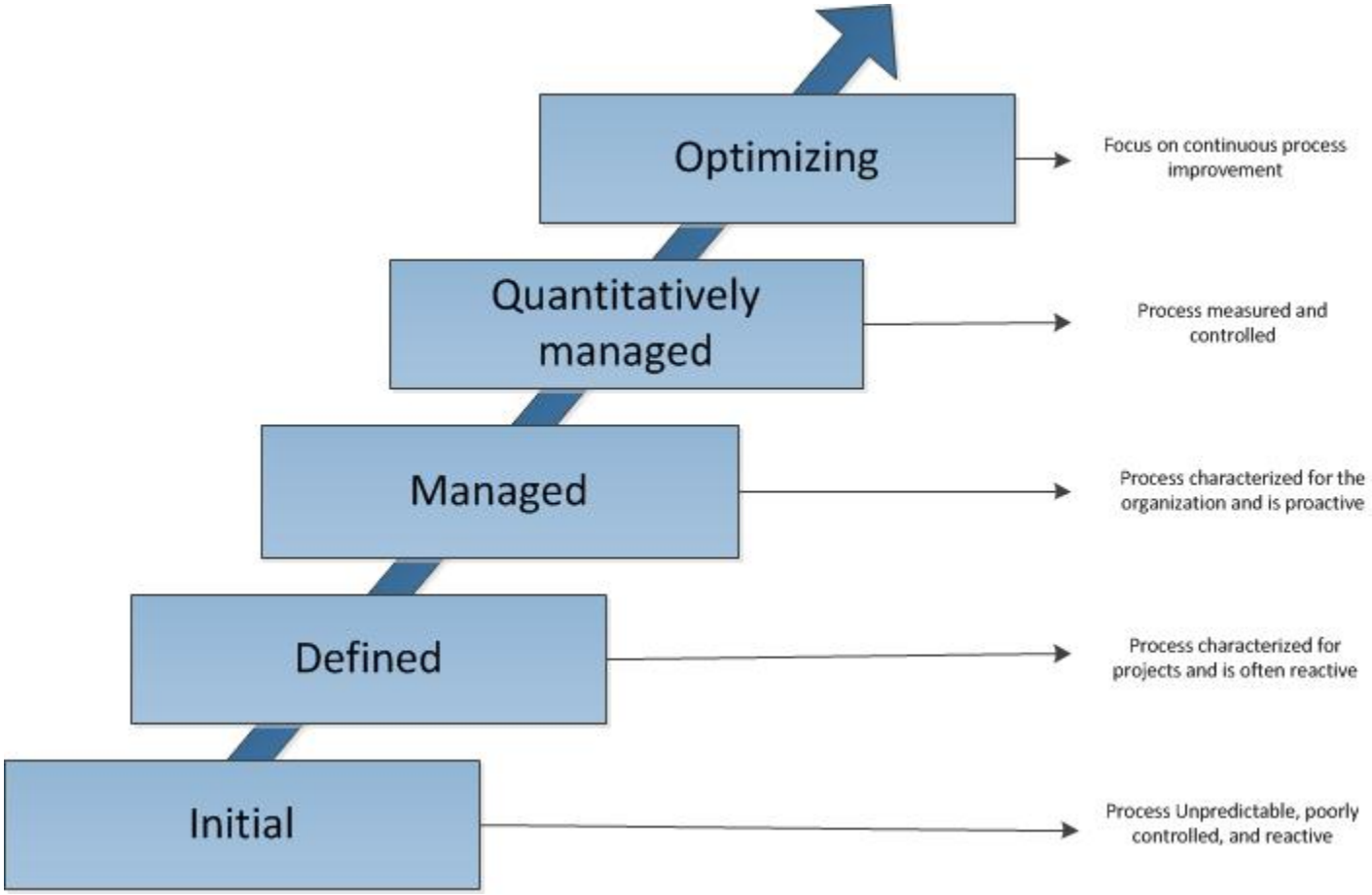
A *maturity model* provides an ordering of capabilities within a *functional domain* across *focus areas* over a sequence of maturity levels

A *maturity level* is a well-defined evolutionary *plateau* within a functional domain

Popular maturity model types

- Staged 5-level model (e.g. CMM)
- Continuous 5-level model (+stages per area)
- Focus area maturity model (+dynamic levels)

CAPABILITY MATURITY MODEL (CMM)



CONTINUOUS 5-LEVEL MODEL

Category	Process Area Including IPPD
Process Management	Organizational Process Focus Organizational Process Definition + IPPD (SG 2) Organizational Training Organizational Process Performance Organizational Innovation and Deployment
Project Management	Project Planning Project Monitoring and Control Supplier Agreement Management Integrated Project Management + IPPD (SG 3) Risk Management Quantitative Project Management
Engineering	Requirements Management Requirements Development Technical Solution Product Integration Verification Validation
Support	Configuration Management Process and Product Quality Assurance Measurement and Analysis Decision Analysis and Resolution Causal Analysis and Resolution

FOCUS AREA MATURITY MODEL

	0	1	2	3	4	5	6	7	8	9	10
Requirements management											
Requirements gathering		A		B	C		D	E	F		
Requirements identification			A			B		C			D
Requirements organizing				A		B		C			
Release planning											
Requirements prioritization			A		B	C	D			E	
Release definition			A	B	C				D		E
Release definition validation					A			B		C	
Scope change management				A		B		C		D	
Build validation					A			B		C	
Launch preparation		A		B		C	D		E		F
Product planning											
Roadmap intelligence				A		B	C		D	E	
Core asset roadmapping					A		B		C		D
Product roadmapping			A	B			C	D		E	
Portfolio management											
Market analysis					A		B	C	D		E
Partnering & contracting						A	B		C	D	E
Product lifecycle management					A	B			C	D	E

1. ISFAM in telecom
2. ISFAM in logistics
3. ISFAM situational factors
4. ISFAM situational modeling
5. ISFAM rule-based modeling in healthcare
6. CYSFAM in finance

1. ISFAM IN TELECOM

<EXTERNAL PPTX>

ISFAM:
THE INFORMATION SECURITY FOCUS AREA MATURITY MODEL

Dr. Marco Spruit & Martijn Roeling MSc, Utrecht University, The Netherlands

Universiteit Utrecht
m.r.spruit@uu.nl

1. roeling

ISFAM:

THE INFORMATION SECURITY FOCUS AREA MATURITY MODEL

Dr. Marco Spruit & Martijn Roeling MSc, Utrecht University, The Netherlands

Universiteit Utrecht
m.r.spruit@uu.nl

FROM PROBLEMS TO RESEARCH

- Problems
  1. Lack of understanding and awareness at the management level and service/product owners to effectively improve their information security
  2. Lack of attention a product/service owner pays to information security
  3. Esp. in SMEs
- Solution
  - Provide a maturity model to improve an organization's information security on a high level in a structured way
- Research Question
  - *"How can a maturity model be designed to assist in narrowing the gap between an organization's requirements and its actual level of information security to help improve information security maturity in a structured and effective manner?"*

DESIGN SCIENCE RESEARCH METHOD

- Hevner et al. (2004) approach, Takeda et al. (1990) steps

1. Awareness of the problem
2. Investigate design choices through comparative literature study
   - better understand information security capabilities and focus areas
   - focus area maturity model design (Steenbergen et al., 2010)
3. Develop a maturity model for every focus area using the CMM standard or literature
4. Each maturity model for a particular focus area is evaluated by one domain expert
   - Attach metrics to maturity model to ensure practical value.
   - Enable maturity measurement of an organization per focus area on a high level.
   - Repeat steps 2, 3 and 4 until an satisfactory model is constructed.
5. Construct conglomerate model out of the separate maturity models
   - at a small/medium sized organization, using experts, common sense and dependencies

COMPARATIVE ANALYSIS OF IS AREAS

IS focus area	*CISSP*	*ISO 27K*	*ISO-light*	*ISF*	*IBM*	*ISFAM*
Risk management	X	X	X	X		*Area 1*
Policy, laws & standards	X	X	X	X		*Area 2*
Organization	X	X	X	X		*Area 3*
HR security		X	X	X	X	*Area 4*
Compliance	X	X	X	X		*Area 5*
Identity/access management	X	X	X	X	X	*Area 6*
Software development	X	X	X	X	X	*Area 7*
Incident management	X (Disaster Rec.)	X	X	X	X	*Area 8*
Business continuity	X	X	X	X		*Area 9*
Change management	X	Comm./Oper. Mgt	X	X		*Area 10*
Physical/environmental	X	X	X	X	X	*Area 11*
Asset management		X	X	X		*Area 12*
Architecture	X (plus Design)			X		*Area 13*

IS AREAS *NOT* IN THIS MODEL…

IS focus area	*CISSP*	*ISO 27K*	*ISO-light*	*ISF*	*IBM*	*ISFAM*
Malicious attacks (prevent)		Partly		X		*Part of other areas*
Cryptography	X	Tool		X		*Part of malicious attacks*
Telecom./network security	X	X	X	X		*Part of architecture*
Governance	X	Organization	Organization	X	X	*Part of organization*
Privacy				X	X	
Transaction/data integrity				X	X	*Part of other areas*

PROFILE OVERVIEW OF INTERVIEWEES

#	*Topic(s)*	*Experience*	*Industry*
1	Risk Management Compliance	> 3 years	Finance/oil
2	Policy development	> 3 years	Finance/oil
3	Organization of information security	> 5 years	Security management/various industries
4	Asset Management	> 5 years	Security management/various industries
5	HR Security	> 10 years	Consultancy security manager
6	Physical & Environmental	> 3 years	Social Engineering in various industries
7	Change Management	> 1 year	Audit in several industries
8	Identity and access management	> 5 years	Telecom, Media & Technology
9	Software Development	> 3 years	Finance
10	Incident Management Business Continuity management	> 10 years	All Industries
11	Information Security Architecture	> 5 years	Finance

EXAMPLE: ASSET MANAGEMENT

- *"the process of guiding an information asset during its lifecycle in order to gain maximum benefit from the asset"*
- *Maturity modeled after Oarisk (2010)*

Maturity level	*Explanation*	*Capability*
Initial	The costs of asset management are unknown, no roles are defined and no reports are made. Typically, asset management is chaotic and unstructured.	
Repeatable	Senior management knows the importance of asset management but no concrete plans exist. Though there are some structured operational processes in place.	A
Defined	There are processes in place that help business objectives and individuals get training. These individuals also get roles in the change management process.	B
Managed	Processes are cross departmental, roles are well defined and asset management is coordinated across functions. Asset management is well thought of.	C
Optimized	Every single part of asset management is documented, aligned and known organization-wide.	D

FRAGMENT OF THE ISFAM ASSESSMENT CONSISTING OF 13/161 QUESTIONS

Area	Capability	Nr	Answer
Asset Management			
	Senior Management within departments takes responsibility for Asset Management	A1	**Yes**
	Senior Management within the organization recognizes the importance of Asset Management	A2	**Yes**
	There is a formal Asset Management policy in place that takes into account the asset management lifecycle phases.	B1	**Yes**
	All Asset Management roles and responsibilities are defined.	B2	**No**
	Asset inventory is created based on status, connectivity, classification and proximity.	B3	**No**
	All assets have been assigned to an owner	C1	**No**
	All stakeholders are familiar with Asset Management procedures and processes	C2	**No**
	Asset Inventory is maintained	C3	**Yes**
	Safe disposal, handled, processed, stored in line with the classification	C4	**No**
	Asset Management Policies are periodically reviewed and updated	D1	**No**
	The Asset Management process is continuously reviewed and updated.	D2	**No**
	An asset management system is in place to increase performance capacity	D3	**No**
	The classification is based on the asset's lifecycle	D4	**No**

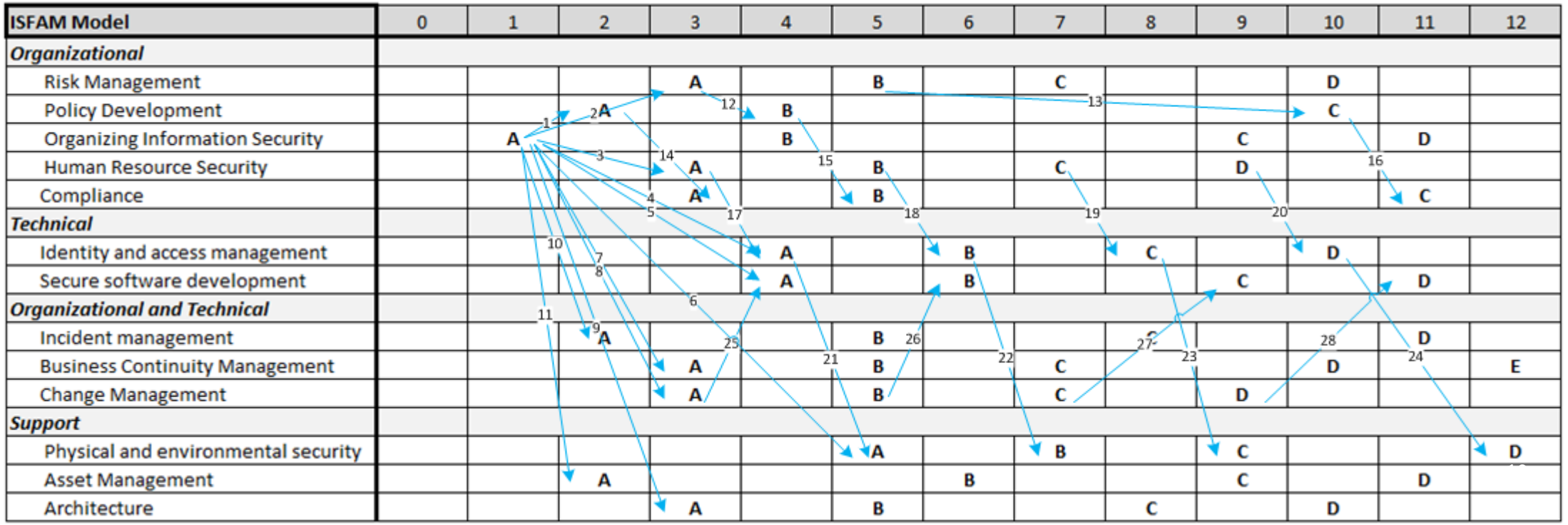
[In this example capability B of the focus area Asset Management is not achieved yet as not all Bx questions can be answered with yes]

ISFAM: THE INFORMATION SECURITY FOCUS AREA MATURITY MODEL

Focus Area: / Maturity Level:	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
1. Risk Management				A		B		C			D		
2. Policy Development			A		B						C		
3. Organizing Information Security		A			B					C		D	
4. Human Resource Security				A		B		C		D			
5. Compliance				A		B						C	
Technical													
6. Identity and access management					A		B		C		D		
7. Secure software development					A		B			C		D	
Organizational and Technical													
8. Incident management			A			B			C			D	
9. Business Continuity Management				A		B		C			D		E
10. Change Management				A		B		C		D			
Support													
11. Physical and environmental security						A		B		C			D
12. Asset Management			A				B			C		D	
13. Architecture				A		B			C		D		
	Design					*Implementation*		*Operational Effectiveness*			*Monitoring*		

DEPENDENCIES FROM LITERATURE

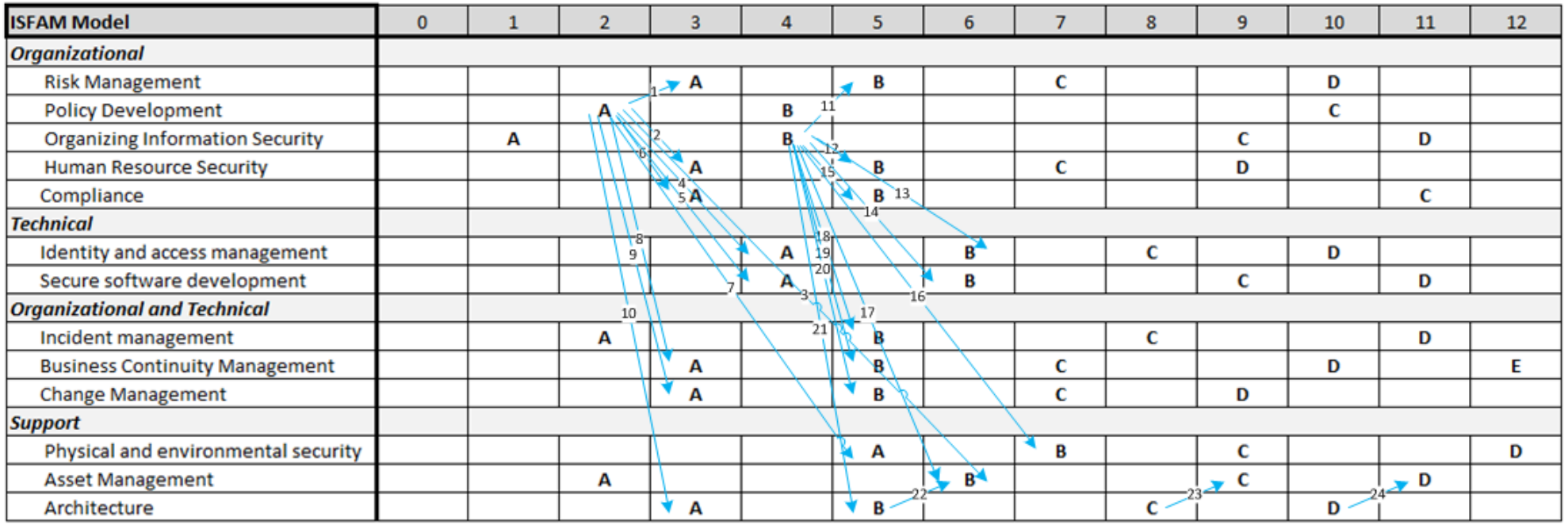
- dependent capabilities should always be positioned at a lower maturity level—i.e. to the left
  - For example, eleven arrows originate from capability A of the focus area Organizing information security. This capability 3A is the management awareness stage



ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management				A		B		C			D		
Policy Development			A		B						C		
Organizing Information Security		A			B					C		D	
Human Resource Security				A		B		C		D			
Compliance				A		B						C	
Technical													
Identity and access management					A		B		C		D		
Secure software development					A		B			C		D	
Organizational and Technical													
Incident management			A			B			C			D	
Business Continuity Management				A		B		C			D		E
Change Management				A		B		C		D			
Support													
Physical and environmental security						A		B		C			D
Asset Management			A				B			C		D	
Architecture				A		B			C		D		

DEPENDENCIES DEDUCED

- Deducible dependencies are dependencies that make sense or are derived from a top-down approach.
  - For example, to ensure consistency throughout the organization, policy guidelines have to be established on a high level before policies can be established for every other single focus area (arrows 1-10).



ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management				A		B		C			D		
Policy Development			A		B						C		
Organizing Information Security		A			B					C		D	
Human Resource Security				A		B		C		D			
Compliance				A		B						C	
Technical													
Identity and access management					A		B		C		D		
Secure software development					A		B			C		D	
Organizational and Technical													
Incident management			A			B			C			D	
Business Continuity Management				A		B		C			D		E
Change Management				A		B		C		D			
Support													
Physical and environmental security						A		B		C			D
Asset Management			A				B			C		D	
Architecture				A		B			C		D		

SINGLE CASE STUDY

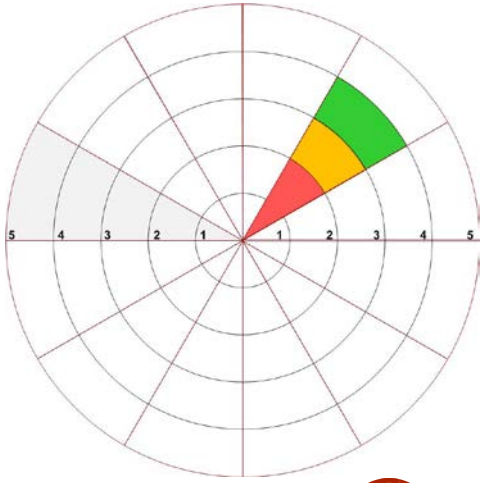
- ISFAM model evaluated at a small/medium sized telecommunications organization in the Netherlands we dub TELCOM.
  - Operates across the globe
  - Headquarters located in the Netherlands
  - Employs around 65 people
  - Serves relatively few business clients
- Goals
  1. To demonstrate the validity of the conceptual ISFAM model in representing an organization's maturity level, and
  2. To enable an organization to develop an information security program, and
  3. To verify whether capabilities are placed in the right order in the ISFAM model.

CONCLUSIONS

- *"How can a maturity model be designed to assist in narrowing the gap between an organization's requirements and its actual level of information security to help improve information security maturity in a structured and effective manner?"*
- The ISFAM Model
  1. Deduces thirteen focus areas is IS from various standards, certifications and methods
  2. Operationalises each focus area via closed-ended (yes/no) statements by defining area-specific maturity levels
  3. Covers the entire space of information security in 161 yes/no statements
  4. Takes approximately three hours
  5. Gives a good overview of what the current state of the organization is, and
  6. Shows in which security capabilities it currently is lacking in the most
  7. Is able to provide tangible process improvement advice due to its high granularity

FURTHER RESEARCH AND DISCUSSION

- Robustness over time due to new developments
  - Rule-based modeling
- Different organizations in different sectors with different sizes have different issues
  - Evaluate at non-IT focused organizations
  - Benchmarking versus tailor-made assessments
  - Situational Process Improvement in Cybersecurity (SPICY)
- Visualization of the results in a spider chart?
  - twelve cyclic maturity levels, thirteen focus areas as "pieces of pie"
  - Red, orange and green pie colors for improvement path
    - red being the history, orange the level that is current, and green for the future goals
- m.r.spruit@uu.nl



ADDENDUM: ISFAM QUESTIONS FRAGMENT

	A	B	C	D	F
1	**Area**	**Capability**	**Nr**	**Answer (Yes/No)**	**Maturity level**
80		All facilities are protected from theft and severe weather	D2	No	
81	**Change Management**				
82		Senior management is aware of the importance and existence of Change Management	A1	Yes	
83		Change management is used in large projects	A2	Yes	
84		Change Management is used to react on negative events.	A3	Yes	
85		There are formal roles and responsibilities defined for Change Management	B1	Yes	
86		Change Management is used in all projects	B2	Yes	
87		The Change Management process is structured	B3	No	
88		There is a formal Change Management procedure designed	C1	Yes	
89		The Change Management process is standardized and the changes documented	C2	Yes	1
90		Change Management is used to track configuration and other small changes to the organization's IT environment	C3	No	
91		Senior management is responsible for Change Management	C4	Yes	
92		Change Management is an organization wide integrated process	D1	No	
93		There is a formal Change Management procedure implemented.	D2	No	
94		The Change Management procedure is supported by information systems.	D3	Yes	
95		Emergency change procedures are covered in the Change Management procedure	D4	Yes	
96	**Identity and Access Management**				
97		There is a formal IAM policy in place	A1	No	
98		User Management is done on an ad-hoc basis OR C2	A2	Yes	
99		Individuals take responsibility for IAM OR C4	A3	Yes	
100		IAM is IT oriented and does not support Business OR C1, D2	A4	No	
101		Access to applications and buildings is logged	B1	Yes	
102		A formal IAM program and process is in place	B2	No	
103		The IAM policy contains a password policy which is business unit oriented OR C3, D1.	B3	Yes	
104		All Roles and responsibilities considering IAM have been defined	B4	No	
105		The IAM policy/documentation supports the vision and strategy of the company OR D2	C1	No	0
106		User Management is done periodically (every month/year) OR D4.	C2	No	
107		The IAM policy contains an organization wide password policy OR D1.	C3	No	
108		Senior Management is responsible for IAM	C4	Yes	
109		Access to applications and buildings is logged and reviewed on a periodical basis.	C5	Yes	
110		The IAM policy contains a password policy that is system/role oriented	D1	No	
111		IAM improves the business and generates new opportunities	D2	No	
112		The IAM program and processes are periodically reviewed and updated	D3	No	
113		User Management is a continuous process supported by an IT system	D4	No	

1. ISFAM in telecom
2. ISFAM in logistics
3. ISFAM situational factors
4. ISFAM situational modeling
5. ISFAM rule-based modeling in healthcare
6. CYSFAM in finance

2. ISFAM IN LOGISTICS

<EXTERNAL PPTX>

SITUATIONELE FACTOREN IN CYBER SECURITY

L. Bek
27 juni 2014

2. bek

SITUATIONELE FACTOREN: 16

1. Hoe groot is de vraag naar normen door de markt? **(Beleidsontwikkeling)**
2. Hoeveel activa is er binnen het bedrijf? **(Vermogensbeheer)**
3. Hoeveel FTE (Full-Time Equivalent) is er binnen het bedrijf?

	SF 1	SF 2	SF 3	SF 4	SF 5	SF 6	SF 7	SF 8	SF 9	SF 10	SF 11	SF 12	SF 13	SF 14	SF 15	SF 16
Beleidsontwikkeling	X															
Vermogensbeheer		X														
Personeelszaken			X	X												
Fysieke en omgevingsveiligheid					X	X										
Veranderingsbeheer			X				X									
Identiteits- en toegangsbeheer			X					X								
Veilige softwareontwikkeling									X	X	X					
Incidentbeheer												X	X	X	X	
Bedrijfscontinuïteitsbeheer																X

SITUATIONELE FACTOR: AANTAL FTE

Waarde	Betekenis (KvK)	Minimale volwassenheidsscore	Ideale volwassenheidsscore
weinig	< 10 medewerkers	0	1
gemiddeld	> 10 en < 250 medewerkers	1	3
veel	> 250 medewerkers	3	4

CASE STUDY: SITUATIONAL ASSESSMENT

Focusgebied	Minimale score	Ideale score	Behaalde score	Verbetering nodig?
Beleidsontwikkeling	3	4	2	ja
Vermogensbeheer	2	3	1	ja
Personeelszaken	3	4	3	niet noodzakelijk
Fysieke- en omgevingsveiligheid	2	3	3	nee
Veranderingsbeheer	1	3	4	nee
Identiteits- en toegangsbeheer	2	3	2	niet noodzakelijk
Veilige softwareontwikkeling	0	0	0	nee
Incidentbeheer	1	2	1	niet noodzakelijk
Bedrijfscontinuïteitsbeheer	4	4	3	ja

1. ISFAM in telecom
2. ISFAM in logistics
3. ISFAM situational factors
4. ISFAM situational modeling
5. ISFAM rule-based modeling in healthcare
6. CYSFAM in finance

3. ISFAM SITUATIONAL FACTORS

INPUT FROM THEORY

Table 1. Keywords used for the systematic literature review, combining items within groups 1, 2 and 3 to construct the actual search queries.

Keywords		
Group 1	Group 2	Group 3
Factor	Influencing	Information Security
Characteristic	Impacting	Information Security Management
Organizational Factor	Affecting	Risk Management
Organizational Characteristic	Effects	Information Risk
Situational Factor	<leave empty>	
Situational Characteristic		
EDP Audit		
IT Audit		
IT Environment		
IT Complexity		

INPUT FROM PRACTICE

Table 4. Overview of interviews performed with experts in information security.

Expert	Experience	Company type	Field of expertise	Expertise in	# interviews
1	6 years	Large consultancy firm	IT Security	SMEs	2
2	10 years	Large accountancy firm	IT Security & IS/IT Research	Small, Medium and Large enterprises	1
3	20+ years	Large accountancy firm	IT Security Consultancy	Small, Medium and Large enterprises	1
4	8 years	Large accountancy firm	IT Auditing	Small, Medium and Large enterprises	1
5	6 years	Large software firm	IT development & IS/IT Research	SMEs	1

OUTPUT: "CHOISS"

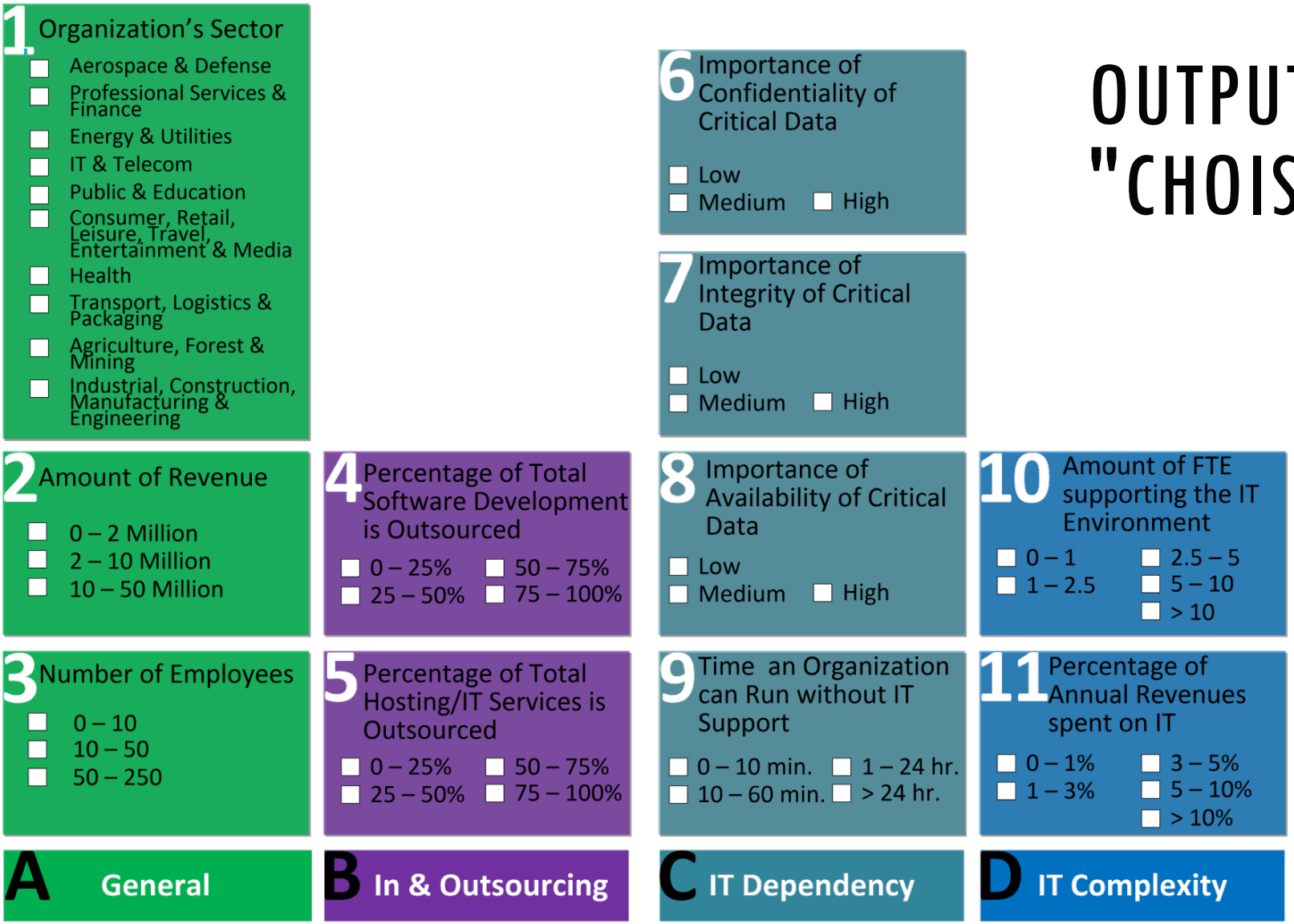


Figure 3. The CHaracterizing Organizations' Information Security for SMEs (CHOISS) model relates four categories (A-D), eleven OCs (1-11) and forty-seven measurement levels.

1. ISFAM in telecom
2. ISFAM in logistics
3. ISFAM situational factors
4. ISFAM situational modeling
5. ISFAM rule-based modeling in healthcare
6. CYSFAM in finance

4. ISFAM SITUATIONAL MATURITY

<EXTERNAL PPTX>

4- baars

THE INUENCE OF MEASUREMENT LEVELS ON MATURITY FRAMEWORKS…

Below: the influence of the measurement levels of OC: **sector**

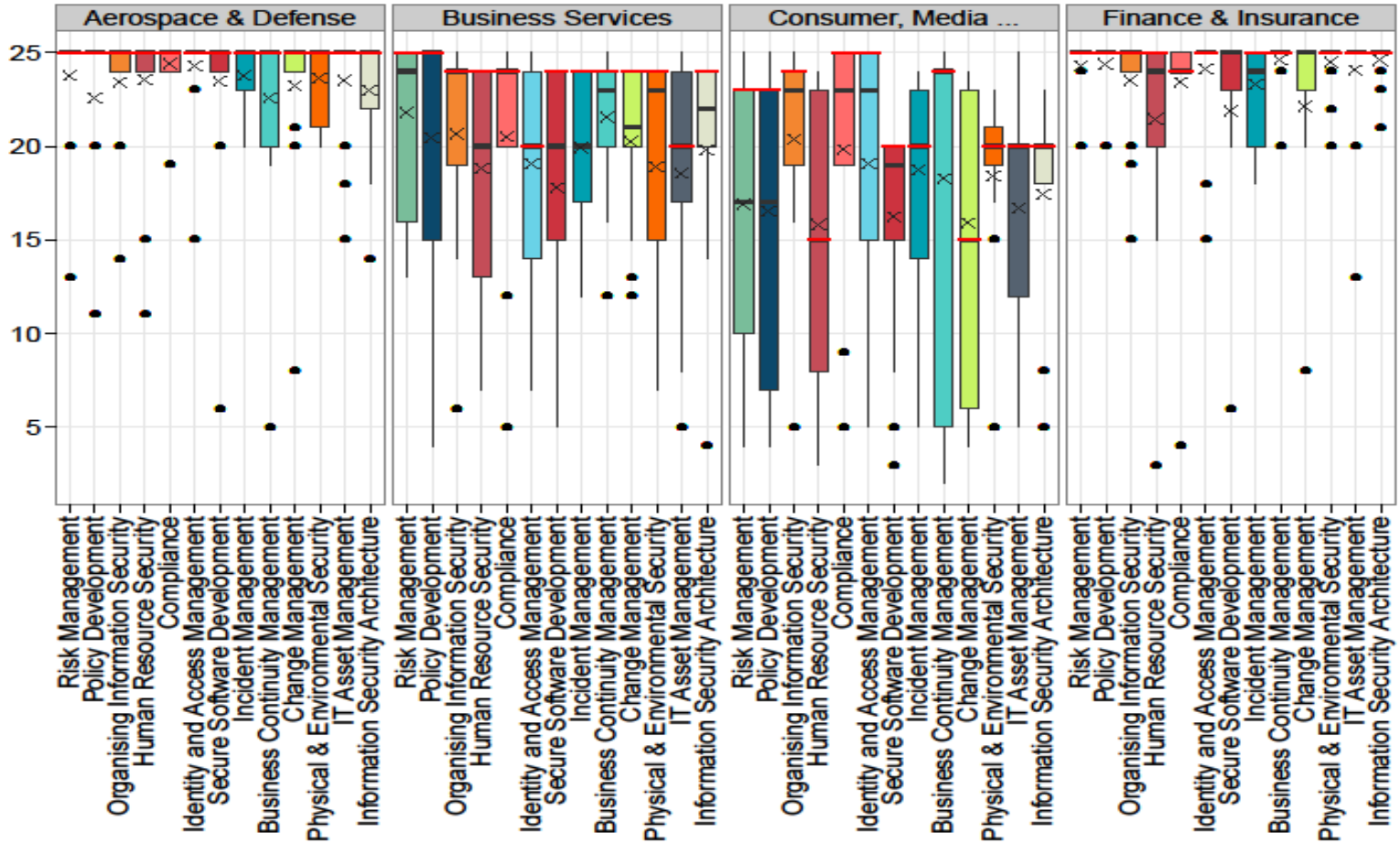


Fig. 1 Box-plots of the Aerospace & Defense, Consumer, Business Services & Consultancy and Finance sectors.

THE INUENCE OF MEASUREMENT LEVELS ON MATURITY FRAMEWORKS…

Below: the influence of the measurement levels of OC: **Hosting Outsourced**

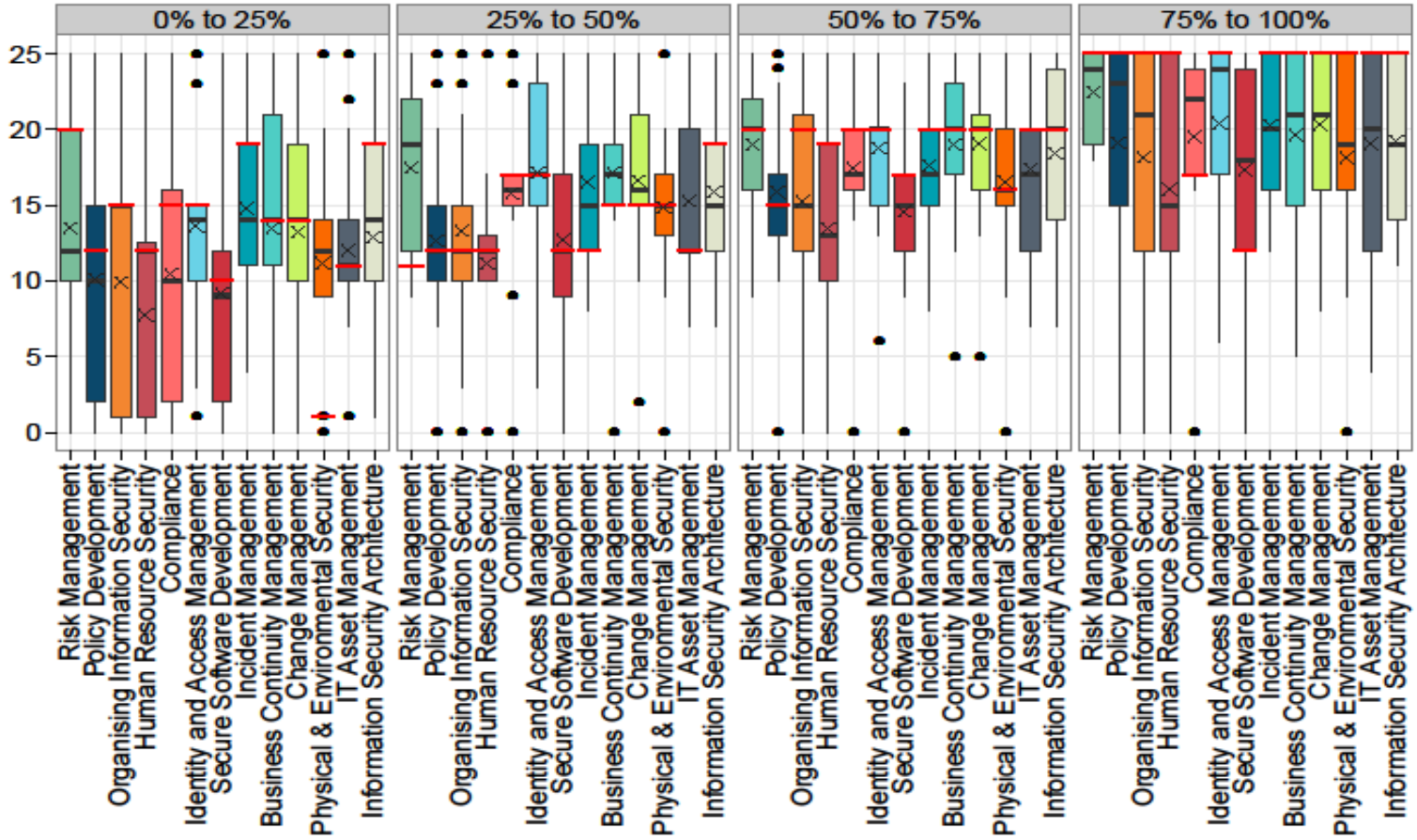
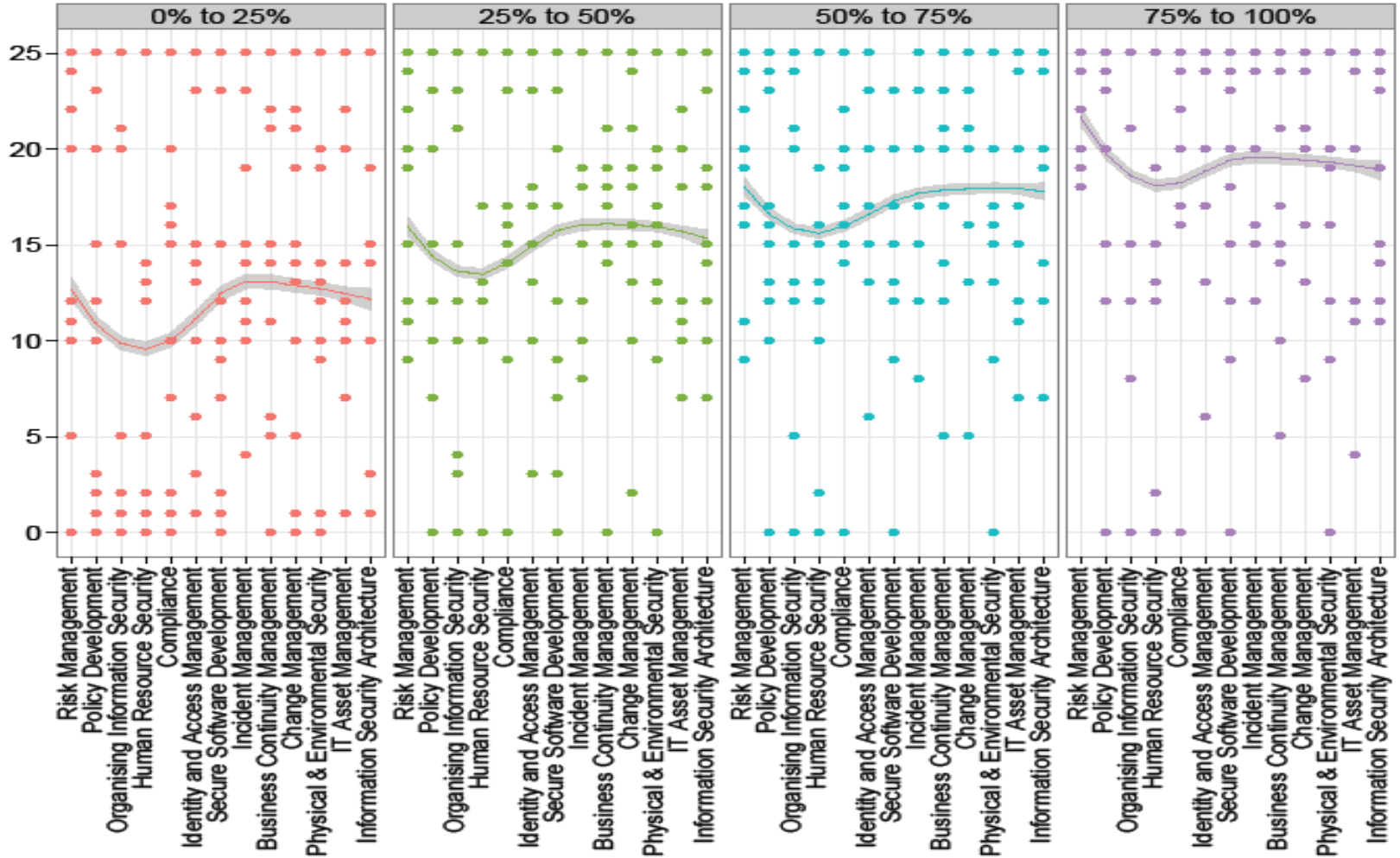


Fig. 2 Box-plots of the percentage of hosting outsourced, 0–25%, 25–50%, 50–75%, 75–100%.

SAME DATA, NOW IN SMOOTHED SCATTER PLOT



SECURITY IN IT IS IMPORTANT!

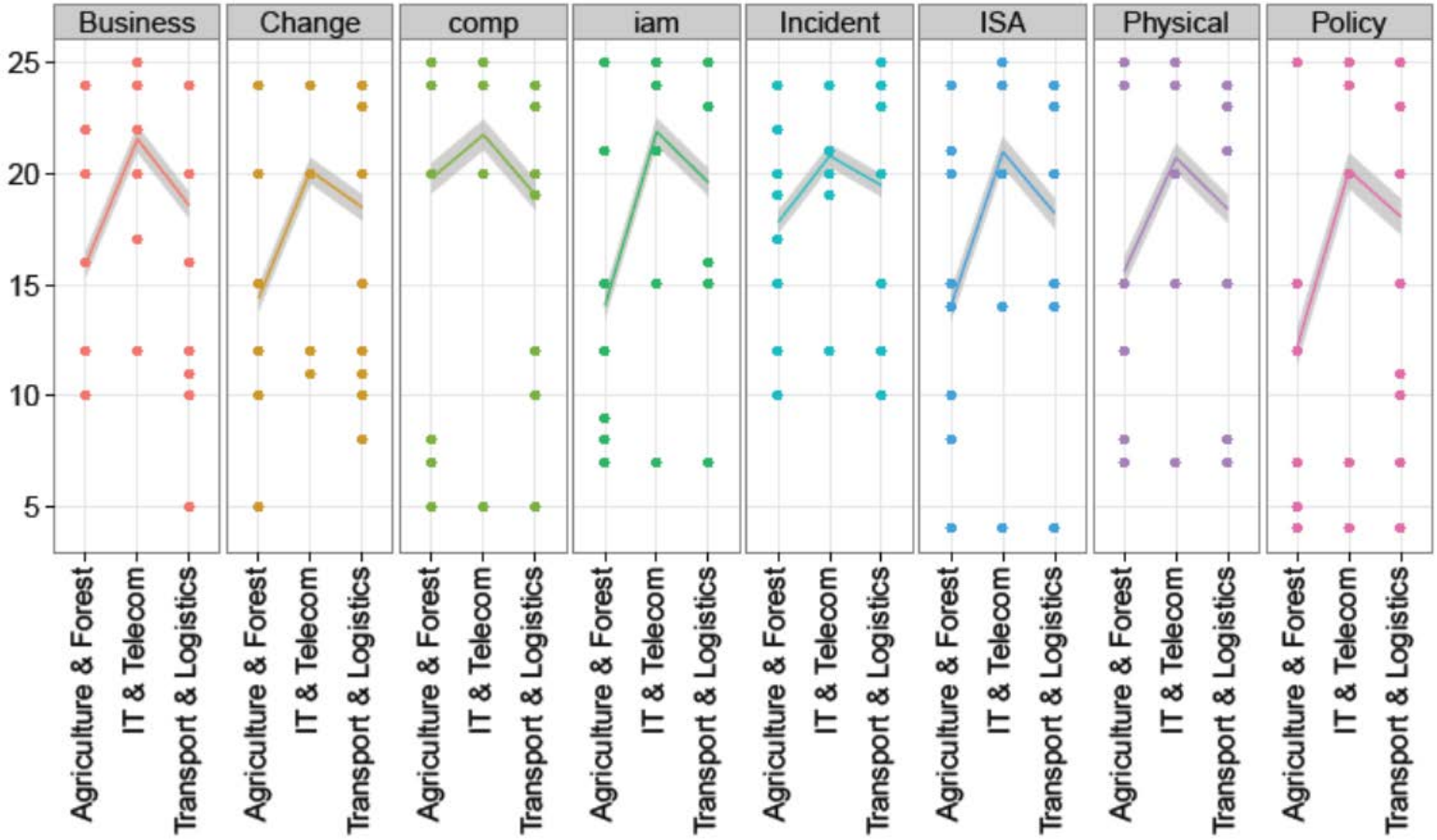


Fig. 6 Scatter-plots per focus area of the ISFAM displaying the sectors IT & Telecom, Transport & Logistics and Agriculture & Forest.

1. ISFAM in telecom
2. ISFAM in logistics
3. ISFAM situational factors
4. ISFAM situational modeling
5. ISFAM rule-based modeling in healthcare
6. CYSFAM in finance

5. ISFAM RULE-BASED MODELING IN HEALTHCARE

A NEWLY IDENTIFIED ISFAM FOCUS AREA…

Supply Chain Management	Capability description
A - Naïve	• Informal supply chain management policy; • Low monitoring of information flowing through the supply chain; • Low awareness and knowledge of risks in the supply chain; • Low support for supply chain management.
B - Novice	• Strategically defined supply chain risk management; • Growing awareness and knowledge of risks in the supply chain; • Proactive management support for supply chain management.
C - Normalized	• Investment in selecting and maintaining collaborative relationship of supply chain participants; • Knowledge of risks and risks are shared with participants in the supply chain; • Formalized Supply Chain Management is shared with participants in the supply chain; • Formalized supply chain management policy.
D - Natural	• Maintaining awareness of risks in the supply chain; • Monitoring of information flow; • Continual risk analysis; • Continual risk assessments.

ISFAM 2.0 BETA

ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management				A		B		C			D		
Policy Development			A		B						C		
Organizing Information Security		A			B					C		D	
Human Resource Security				A		B		C		D			
Compliance				A		B						C	
Supply Chain Management				A		B		C			D		
Technical													
Identity and access management					A		B		C		D		
Secure software development					A		B			C		D	
Organizational and Technical													
Incident management			A			B			C			D	
Business Continuity Management				A		B		C			D		E
Change Management				A		B		C		D			
Support													
Physical and environmental security						A		B		C			D
Asset Management			A				B			C		D	
Architecture				A		B			C		D		
	Design					*Implementation*		*Operational Effectiveness*			*Monitoring*		

EFFECTS ORGANISATIONAL CHARACTERISTICS 1/3

Expert	Function	Experience
# 1	IS Consultant	10
# 2	IS Consultant	10
# 3	IS Consultant	14
# 4	IS Consultant	8
# 5	IS Consultant	12
		54

Interview experts

- Information security consultants;
- Not working in the same company;
- Years of experience.

Interview

- Risk Management, A: There is an informal RM program in place.
- Is there a difference between an organization with 0-10 fte & an organization with 50-250 fte?

Focus Area	Number of Employees			Revenue*			Sector
	0-10	10-50	50-250	0-2	2-10	10-50	
A							
B							
C							

EFFECTS ORGANIZATIONAL CHARACTERISTICS 2/3

Experts: as of now, there are no effects

Examples:

- Identity and Access Management, measure: "The organization has a formal IAM policy in place."
  - Organization with 2 employees VS organization with 238 employees

- Policy Development focus area, measure: "Laws and regulations are part of the information security policy."
  - Organization in healthcare VS organization in finance

Successfully evaluated at multiple SMEs.

Conclusion: Applicable for different organizations

1. ISFAM in telecom
2. ISFAM in logistics
3. ISFAM situational factors
4. ISFAM situational modeling
5. ISFAM rule-based modeling in healthcare
6. CYSFAM in finance

6. CYSFAM IN FINANCE

ISFAM: TOO GOOD TO BE TRUE?

ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management				A		B		C			D		
Policy Development			A		B						C		
Organizing Information Security		A			B					C		D	
Human Resource Security				A		B		C		D			
Compliance				A		B						C	
Technical													
Identity and access management					A		B		C		D		
Secure software development					A		B			C		D	
Organizational and Technical													
Incident management			A			B			C			D	
Business Continuity Management				A		B		C			D		E
Change Management				A		B		C		D			
Support													
Physical and environmental security						A		B		C			D
Asset Management			A				B			C		D	
Architecture				A		B			C		D		
	Design					***Implementation***		***Operational Effectiveness***			***Monitoring***		

… VULNERABILITY MANAGEMENT?

Maturity level A

- The organization runs scheduled vulnerability scans on all production machines on their network.
- The organization has subscribed itself to vulnerability intelligence services, and this information is incorporated in the vulnerability management process.

Maturity level B

- The organization runs scheduled vulnerability scans on all DTAP machines on their network.
- The organization measures the delay of the patching of vulnerabilities.

Maturity level C

- The organization feeds a Vulnerability Management System (VMS) with the outcomes of the periodic machine scans.
- The organization has a process in which vulnerabilities are risk-rated based on the assets' characteristics.

Maturity level D

- The VMS compares systems to configuration baselines automatically.
- There is a Role Based Access Control (RBAC) solution to regulate who has access to the vulnerability management platform

… CRYPTOGRAPHY?

Maturity level A

- Key generation is consistent within applications AND recipients are authenticated before the key is handed out.
- The access to key storage is defined in the application's individual processes AND key backup is consistent within applications.
- Updating and renewing keys is dealt with and is consistent throughout applications AND recovery processes are implemented per application.
- Key revocation is consistent within applications AND key disposal processes are implemented.

Maturity level C

Key generation standards are managed at the organizational level AND all application in the enterprise comply to these standards.

Key storage standards are managed at the organizational level AND key back-up standards are managed at the organizational level.

Key update standards are managed at the organizational level AND key recovery processes are consistent with standards.

Key revocation standards are managed at the organizational level AND key disposal standards are managed at the organizational level.

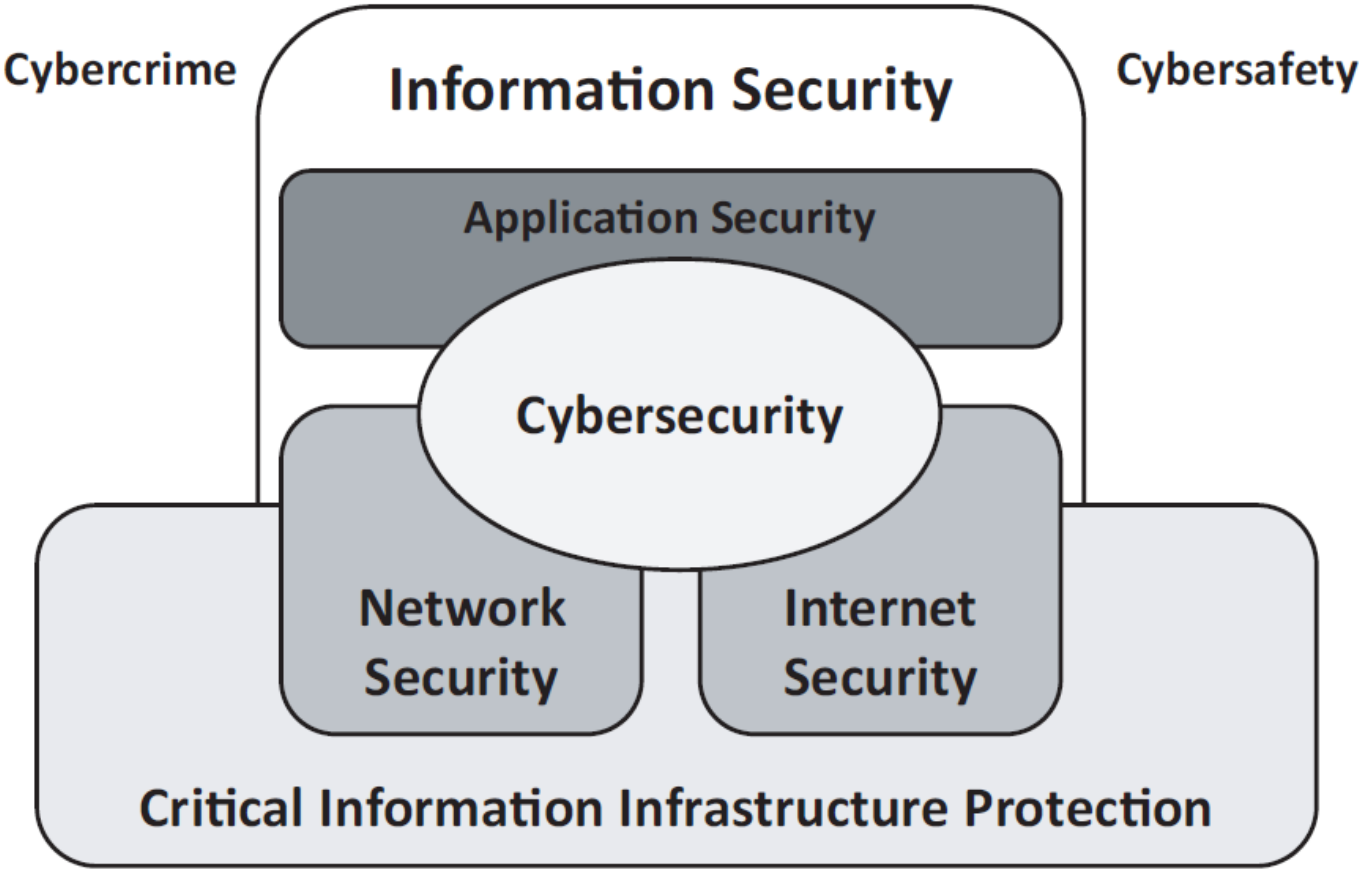
CYSFAM

Cyber Security Maturity Model	A	B	C	D	E	F	G
Organizational and Technical							
Server Protection	■	■	■				
End-user Controls	■	■	■				
Social Engineering Controls	■						
Network Security	■	■					
Application Security	■						
Cryptography	■						
Mobile Security	■	■					
Vulnerability Management	■						
Supportive							
Cyber Security Incident Management	■						
Cyber Security Awareness	■	■					
Cyber Security Governance	■	■					

ISFAM + CYSFAM =

information security + cybersecurity =

WHAT ABOUT...?


Cybercrime
Information Security
Cybersafety
Application Security
Cybersecurity
Network Security
Internet Security
Critical Information Infrastructure Protection

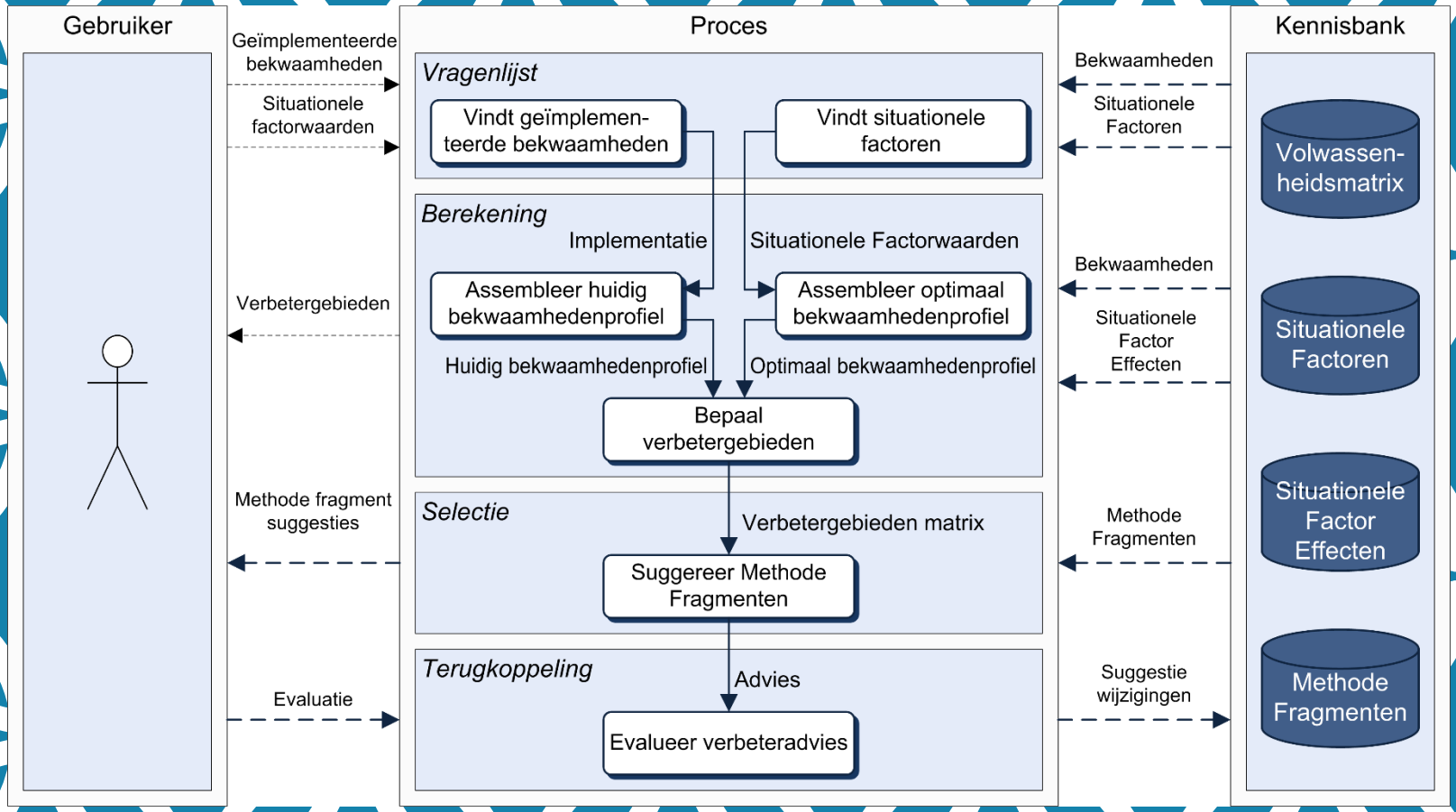
A FEDERATED MODEL

Federative Security Maturity Model	A	B	C	D	E	F	G
Information Security							
Risk Management							
Policy Development							
Organizing Information Security							
Human Resource Security							
Compliance							
Identity and access management							
Secure software development							
Incident management							
Business Continuity Management							
Change Management							
Physical and environmental security							
Asset Management							
Architecture							
Application Security							
Application Security							
Network and Internet Security							
Network Security							
Cyber Security							
Server Protection							
End-user Controls							
Social Engineering Controls							
Cryptography							
Mobile Security							
Vulnerability Management							
Cyber Security Incident Management							
Cyber Security Awareness							
Cyber Security Governance							

CONCLUDING CYSFAM REMARKS

Augmenting cyber security capabilities to an information security focus-area maturity model is of added value:

- Cyber security capabilities are not incorporated in contemporary information security focus areas.
- The ISFAM does not incoroprate these capabilities, while it is proven that it is desirable to do so.
- By surveying domain literature, a total of 12 cyber-security focus areas have been named.
- These focus areas have 3 to 5 distinct maturity levels.
- Information security maturity and cyber security maturity levels are not necesarily congruent.
- Conceptually modeling a federative security focus area maturity model seems fruitful, but needs to be more scientifically grounded.



Bekkers,W., & Spruit,M. (2010). The Situational Assessment Method Put to the Test: Improvements Based on Case Studies. *4th International Workshop on Software Product Management* (pp. 7–16). IWSPM, September 27, 2010, Sydney, Australia. [pdf] [online]

THX.

m.r.spruit@uu.nl