Enterprise Engineering in Business Information Security

Yuri Bobbert[1,2,4] and Hans Mulder[2,3,4(✉)]

[1] Radboud University, Nijmegen, Netherlands
[2] University of Antwerp, Antwerp, Belgium
[3] VIAGroep NV, The Hague, Netherlands
hans.mulder@viagroep.nl
[4] Antwerp Management School, Antwerp, Belgium
yuri.bobbert@ams.ac.be

Abstract. Implementing and maintaining Business Information Security (BIS) is cumbersome. Frameworks and models are used to implement BIS, but these are perceived as complex and hard to maintain. Most companies still use spreadsheets to design, direct and monitor their information security improvement plans. Regulators too use spreadsheets for supervision. This paper reflects on ten years of Design Science Research (DSR) on BIS and describes the design and engineering of an artefact which can emancipate boards from silo-based spreadsheet management and improve their visibility, control and assurance via an integrated dash-boarding and reporting tool. Three cases are presented to illustrate the way the artefact, of which the realisation is called the Securimeter, works. The paper concludes with an in-depth comparison study acknowledging 91% of the core BIS requirements being present in the artefact.

1 Introduction

When starting this research in 2008, security was mainly IT-oriented and the main focus was on using IT controls to mitigate or detect security threats. Research has shown that the number of IT security incidents has increased over the years, as has the financial impact per data breach [1]. In 2009, an average of 25% of EU organisations experienced a data breach [2]. Mastering emerging technologies such as big data, Internet of Things, social media and combating cybercrime [3], while protecting critical business data, requires a team instead of a single IT person. To protect this data, security professionals need to know about the value of information and the impact if it is threatened [4]. Several Risk & Security methods have been developed over the last years such as CRAMM (CCTA Risk Analysis and Management Method), OCTAVE, [5], NIST, [6] and ISFs' IRAM [7], particularly into risk analysis and risk assessments in order to analyse threats, vulnerabilities and the impact on information systems as part of the risk management process. The relationship of Risk Management (RM) to Risk

A case study & expert validation in Security, Risk and Compliance artefact engineering.

D. Aveiro et al. (Eds.): EEWC 2018, LNBIP 334, pp. 1–25, 2019.
https://doi.org/10.1007/978-3-030-06097-8_6

Assessment (RA) and information security control setting is visualized in Fig. 1 and is adopted from OCTAVE. To determine these information security controls in the form of process controls, technical controls or people controls is based on the risk and impact estimation on the critical *business* assets. Therefore IT risk management requires different capabilities, knowledge and expertise from the skills of IT security professionals [8]. Hubbard [8] refers to the failure of 'expert knowledge' in impact estimations and to the importance of experience beyond risk and IT security, such as asset valuation, collaboration and reflection.

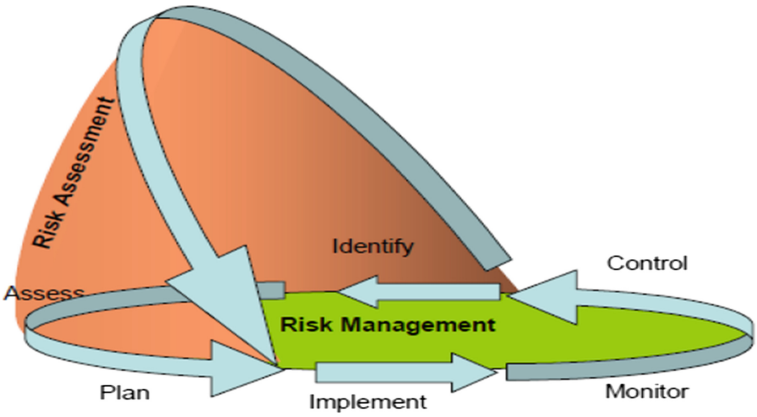


Fig. 1. The relationship between Risk Management and Risk Assessment taken from OCTAVE [9]

2 Practical Contribution

In the past [10] IT security controls were implemented based on best practices prescribed by vendors, without a direct link to risks or business objectives [10]. These controls depended on technology and the audits and assessments (in spreadsheets) were used to prove their effectiveness [11]. The problem with this approach lay in the limitations of mainly IT-focused security and security experts working in silos with limited, subjective views of the world [12]. This is important, as information security is subject to many different interpretations, meanings and viewpoints of several stakeholders [13]. Objectivism is a position that claims that social entities (e.g. 'actors' such as organisations) share exact the same observations and concepts of reality. This is often associated with the term social constructionism. Interpretivism involves the epistemology of a 'social subject'. Actors subjectively observe, analyse and interpret phenomena which they are part of. 'Intersubjective', according to Seale, relates to *"common-sense, shared meanings constructed by people in their interactions with each other and used as an everyday resource to interpret the meaning of elements of social and cultural life. If people share common sense, then they share a definition of the situation."* [14] In the case of BIS, this refers to interactions and reflection between actors e.g. the business, data owners and industry peers on the appropriate level of risk

appetite and security maturity [12]. Thus objectivity relates to reality, 'truth reliability', testability and reproducibility, while subjectivity refers to the quality of personal opinions. Intersubjectivity involves the agreements between social entities and the sharing of subjective states by two or more individuals [14].

In order to design a secure enterprise which uses theories and concepts of subjectivity, intersubjectivity and objectivity, the discipline of Enterprise Engineering (EE), which focuses on collaboration in and between organisations, was expected to deliver a contribution to the field of BIS, in 2008. The EE methodology Design and Engineering Method for Organisations (DEMO) therefor was applied in this research in 2009 [15]. DEMO is used to develop an ontological model and to develop a theoretical pattern that can be validated using the artefact (tool).

The field of security in 2010 shifted towards 'information security'. ISO specifies information security as *"protecting information assets from a wide range of threats in order to ensure business continuity, minimise business risk and maximise return on investment and business opportunities"* [16]. Its core principles are Confidentiality, Integrity and Availability (CIA) [16]. Later non-repudiation and auditability were added to comply with audit and compliance regulations. Thus Information Security should ensure a certain level of system quality and assurance [17]. In 2010 many organisations used spreadsheets to practice risk and security management and also proof their assurance via spreadsheets [18, 19].

The scope of Information Security was then expanded to Business Information Security (BIS). In their book 'Information Security Governance', Von Solms and Von Solms describe the growing number of disciplines involved in *BIS* [20]. By 2011 IT managers and IT security managers were increasingly urged to engage with business to determine risk appetite and the desired state of security. Up to 2016, the subjective silo approach to BIS was designed, maintained and reported via spreadsheets [11]. Experts mapped multiple control frameworks [21] from ISO, ISF, COBIT5 in spreadsheets and these are still used by regulators such as the Dutch Central Bank [22]. Volchkov stated that collecting evidence of effectiveness of the controls via spreadsheets has limitations [23]. So Governance Risk and Compliance (GRC) tools moved towards information risk, due to the Sarbanes-Oxley Act, and were designed for large enterprises. GRC implementations are complex and their maintenance requires dedicated staff [24]. Integration of GRC tools with operational data via Security Information and Event Management (SIEM) functionality is reserved for companies with extensive budgets and sufficient staff [24].

Filling in spreadsheets with answers to questionnaires is subject to manipulation because it is not a closed loop. Spreadsheet data is limited to subjective opinions and there is little room for reflection. Spreadsheet data cannot always be gathered from the original sources, which reduces authenticity and integrity [25]. Intersubjective aspects were missing from past timeframes, unless companies used third parties to interpret the data. Objective aspects are not covered, since the various objects (operational processes and data) are not interconnected. Objectivity can be achieved with GRC tools that connect operations to strategy, properly configured via clearly defined business rules. But GRC tools are expensive to implement and to maintain [24] and reserved for large organisations with deep pockets.

This paper describes a research journey from 2008 to 2016, focusing on the development of a BIS artefact that enables intersubjectivity via a dashboard and reporting function. It presents a set of core artefact functionalities that can assist company boards and managers in identifying organisational gaps, gathering operational factual data and thus increasing awareness. It also helps to prioritise investments and enables decision-making. This paper first presents an ontological model that is the precursor of the artefact, and a Design Science Research (DSR) approach [26] to continuous development, design, engineering and maintenance of the artefact. The artefact is later on compared to another artefact with a similar objective. The artefact was designed to incorporate multiple threat and risk models, such as OCTAVE [35], STRIDE and Information Security frameworks such as ISF, OWASP, Cloud Security Framework and ISO27000 series, to master the problem of security management with one single source of truth. Three cases describe the artefacts working and their practical contribution, finally an in-depth artefact comparison is performed by a panel of experts.

3 Enterprise Ontology

Performing a secure business transaction in a connected digitised world requires a view across the boundaries of the enterprise. To share a common, intersubjective view, risk management "could be integrated throughout the organisation. This made it easier to specify the knowledge and competencies needed to manage risk and to identify blind spots." [27]. This shows that all actors involved in the supply chain, i.e. the extended enterprise of secure transactions, needed to be involved. In 2009, at the start of this research, Electronic Patient Files (EPD in Dutch) were examined from the point of view of a customer with a business requirement. In this case, there is treatment by a surgeon and the use of data repositories in order to treat the patient [15].

DEMO – a methodology that is used to design enterprises – is based on several theories, including the ψ theory [28]. This Greek letter PSI stands for Performance in Social Interaction. The ψ theory focuses on the performance of the social interactions of actors. In this paper [15] the DEMO delayering in B-I-D takes into account inter-subjective communication between social actors, the reasoning of subjects and objective data in repositories of facts. The B layers represent *Business* transactions, the I layer the *Information* layers and the D layers the *Data* layer. In this research DEMO is used to provide the design for the BIS artefact and elicit the collaboration and interaction between parties to gain the required intersubjective assurance. To deal with some core transactions the Securimeter artefact contains business rules for actors. The DEMO model shown in Fig. 2 depicts the artefacts working, per transaction type, including actors and sources per case.

B-A represent the actors and require facts related to production and communication. T represents the transactions related to the handling of this request, whereas B-CA represents composite actors. B-APB represents the data repositories that contain facts such as transaction logs. The outlined area, described as 'Security Performance Meter', represents the BIS artefact. In the three examples below we describe transactions (e.g. business requirements) that were initiated by three different actors: a request from a board member and two requests from a manager. For page limitations we refer to the

online dataset (https://easy.dans.knaw.nl/ui/datasets/id/easy-dataset:77502/tab/2) tab Chapter 7 of this research project that captures all the required evidence accompanying each case.

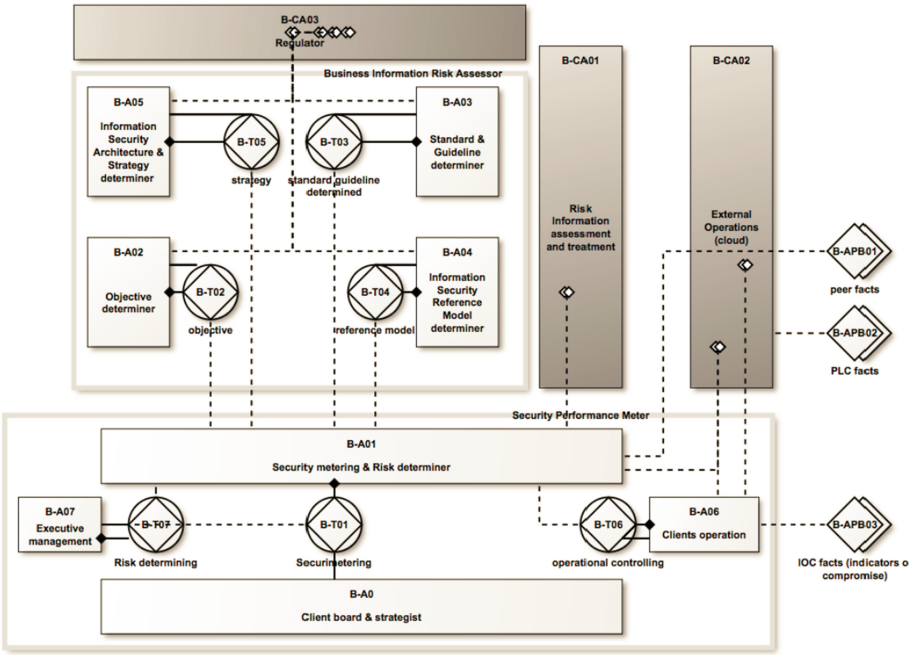


Fig. 2. The DEMO model for the BIS artefact.

4 Establishing the Requirements for the Securimeter Artefact: Three Cases

According to DEMO, a successful transaction is established after the acceptance from the requesting actor. In the context of BIS, we have identified three examples of a request from a board member or manager to deliver an overview of the risk and security level of the organisation. He or she might want to report this information to an audit committee or regulator. We refer to this actor as the 'Client board' (B-A0), since this is an entity who wants to gain or maintain a certain level of information risk assurance. This actor makes a request for a transaction (B-T01) and information is delivered via certain processes and extracted from internal or external data repositories B-APB01/02/03. In this section three examples are presented of a business request that leads to BIS artefact requirements. The first case involves a large government organisation with a broad and complex IT landscape. To maintain a certain level of *BIS* control, they adopted the Baseline Information Security Government (Baseline Informatiebeveiliging Rijksdienst (BIR). The BIR consists of 12 domains which are

categorised as people, process and technology controls. These domains were included in the artefact via 133 questions the organisation is required to answer. This case describes the artefact's contribution to effectively measuring, controlling, demonstrating and reporting on this BIR, since the organisation is subject to regulatory supervision. The second case involves a financial firm that wants to gain periodically insight into their critical risks and treatment plans. The third case relates to extracting operational data from a production environment to gain insight into critical assets. This information is necessary to gain control of new or missing assets (e.g. a production plant).

4.1 Government Case

The governmental organisation must comply with the BIR [29]. This norm is based on the ISO 27000 series and the 12 domains match the domains of the ISO such as; Information Security Policy, Information Security management organisation, Asset management, Personnel security, Access management etc. In order to frequently report on the status of BIR maturity, this actor requires a periodical status overview on the effectiveness of controls. This customer request starts a process which extracts the status of the key controls in the organisation within the BIR. These controls are implemented within for example IT operations, via processes and technology. The effectiveness of these controls can be measured and expressed in numbers, for example via maturity models with predefined scales (e.g. ISO 15504). Within this, a 0% score refers to Non-existent (N), everything in between is partially achieved (P) or largely achieved (L), and 100% represents fully achieved (F). This NPLF scoring leaves room for multiple criteria per maturity level of the control. By testing and scoring each control on its design and effectiveness, this can be reflected in a dashboard. In an ideal situation, there is an automated scripted process of proofing the design and effectiveness of most of these controls. The figure below shows a dashboard of the key BIR domains. Every domain reflects multiple controls that are weighted and collectively express, via NPLF scores, into the dashboard with meters per domain. The improvement values per domain are expressed in green or in red, if there is a decrease in maturity level. The overall colour of the meter shows the progression compared to the predefined desired state.

When an organisation is subject to multiple regulators (e.g. Authoriteit Persoonsgegevens) or internal control frameworks (e.g. ISO), it is desirable that all of these baselines are mapped on the existing baseline (BIR). This cross-referencing of models, labelled as 'x-ref' in the upper left in the meta-model, and their controls, is needed in order to establish a collective set of the existing controls in an exhaustive framework, in order to avoid double work on identical controls. In this case, the actor requests only to report on the BIR status via a reflection of control effectiveness via an NPLF score expressed in a dashboard with meters. See Fig. 3 for the Dutch dashboard, the domains mentioned in Dutch match the English translation of 5 = Information Security Policy, 6 = Information Security management organisation, 7 = Asset management, 8 = personnel security, 11 = Access management 12 = Acquisition and development of Systems, 13 = Incident management and 14 = Business Continuity Management.

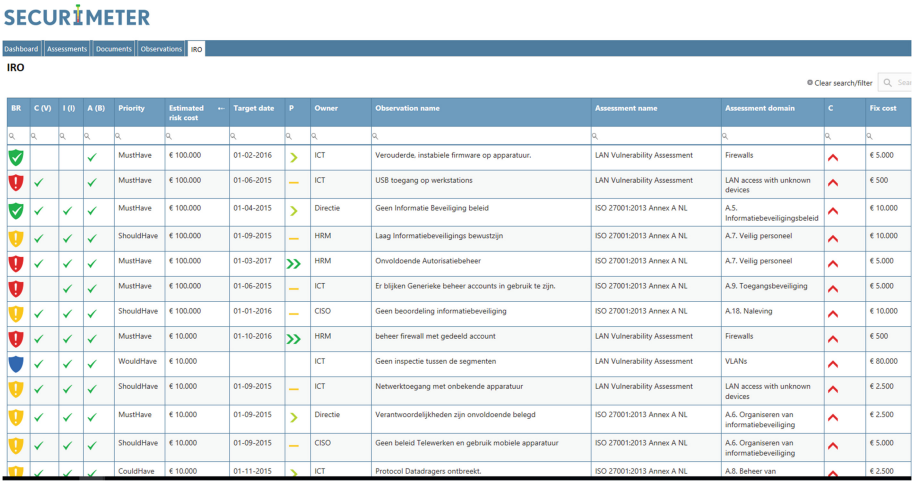
4.2 Finance Case Study

The second example of a business request shows insight into all information risks, expressed in a score ranging from low to critical. This is needed for executive management (B-A07) to be aware of the risks, the risk owners and the treatment plans, and for regular reporting on the functioning of the information risk assurance. This request kicks off a transaction (B-T07) that extracts information from the information risk determiner, where all risks are identified with a risk indication of low, medium, high or critical, derived from processes and documentation.

(B-CA01) in the repository of the artefact. This risk indication is based on the Business Impact Analysis (BIA) and various predefined treatments (e.g. security controls). Within the BIA, a thorough trade-off is made for the risk treatment plan, based on the risk appetite of the organisation. This is usually determined via policies and procedures stored in a repository (B-CA01). The person responsible for determining the information risk policies and standards is usually the Chief Risk Officer (B-T03). The security controls that might mitigate the risks are predefined in the IS standards and models, and the person responsible for determining this (B-T04) is usually the Chief Information Security Officer (CISO).

Figure 4 displays the result of a business request for an overview of risks and all relevant data needed to enable an intersubjective view. This view is called intersubjective because it involves sharing benchmark data on for example Open Web Application Security Project (OWASP) penetration testing results with other organisations. Capturing penetration testing data in the artefact makes it possible to compare the risk profile with those of peers (e.g. other business units). The information displayed in this dashboard can also be used in interaction with other stakeholders, such as regulators, auditors or committees.

Fig. 3. Artefact dashboard displaying BIR status per domain



BR	C (V)	I (I)	A (B)	Priority	Estimated risk cost	Target date	P	Owner	Observation name	Assessment name	Assessment domain	C	Fix cost
			✓	MustHave	€ 100.000	01-02-2016	›	ICT	Verouderde, instabiele firmware op apparatuur.	LAN Vulnerability Assessment	Firewalls	^	€ 5.000
	✓		✓	MustHave	€ 100.000	01-06-2015	—	ICT	USB toegang op werkstations	LAN Vulnerability Assessment	LAN access with unknown devices	^	€ 500
	✓	✓	✓	MustHave	€ 100.000	01-04-2015	›	Directie	Geen Informatie Beveiliging beleid	ISO 27001:2013 Annex A NL	A.5. Informatiebeveiligingsbeleid	^	€ 10.000
	✓	✓	✓	ShouldHave	€ 100.000	01-09-2015	—	HRM	Laag Informatiebeveiligings bewustzijn	ISO 27001:2013 Annex A NL	A.7. Veilig personeel	^	€ 10.000
	✓	✓	✓	MustHave	€ 100.000	01-03-2017	»	HRM	Onvoldoende Autorisatiebeheer	ISO 27001:2013 Annex A NL	A.7. Veilig personeel	^	€ 5.000
		✓	✓	MustHave	€ 100.000	01-06-2015	—	ICT	Er blijken Generieke beheer accounts in gebruik te zijn.	ISO 27001:2013 Annex A NL	A.9. Toegangsbeveiliging	^	€ 5.000
	✓	✓	✓	ShouldHave	€ 100.000	01-01-2016	—	CISO	Geen beoordeling informatiebeveiliging	ISO 27001:2013 Annex A NL	A.18. Naleving	^	€ 10.000
	✓	✓	✓	MustHave	€ 10.000	01-10-2016	»	HRM	beheer firewall met gedeeld account	LAN Vulnerability Assessment	Firewalls	^	€ 500
	✓	✓	✓	WouldHave	€ 10.000			ICT	Geen inspectie tussen de segmenten	LAN Vulnerability Assessment	VLANs	^	€ 80.000
	✓	✓	✓	ShouldHave	€ 10.000	01-09-2015	—	ICT	Netwerktoegang met onbekende apparatuur	LAN Vulnerability Assessment	LAN access with unknown devices	^	€ 2.500
	✓	✓	✓	MustHave	€ 10.000	01-09-2015	›	Directie	Verantwoordelijkheden zijn onvoldoende belegd	ISO 27001:2013 Annex A NL	A.6. Organiseren van informatiebeveiliging	^	€ 2.500
	✓	✓	✓	ShouldHave	€ 10.000	01-09-2015	—	CISO	Geen beleid Telewerken en gebruik mobiele apparatuur	ISO 27001:2013 Annex A NL	A.6. Organiseren van informatiebeveiliging	^	€ 5.000
	✓	✓	✓	CouldHave	€ 10.000	01-11-2015	›	ICT	Protocol Datadragers ontbreekt.	ISO 27001:2013 Annex A NL	A.8. Beheer van	^	€ 2.500

Fig. 4. Artefact dashboard displaying all identified risks.

4.3 Utility Company Case

A large utility company requires frequent inventories to be made of their critical IT assets that control the Programmable logic controller (PLC) environments. In this example, the security manager requests operational data to be mapped on one of the key controls “asset inventory” and be reflected in a delta score. The API function is a function in the artefact that makes it possible to import operational data into the artefact via ‘Dynamic-link library (DLL) parsing’, which enables data from operational sources, in this example QualysGuard vulnerability data, to be processed in the artefact. The API requirement implementation in the artefact resulted in the ability to parse data into the artefact and this reflects the key control effectiveness via the dashboard. In addition, other customer requests were engineered into the artefact. For example, in 2013–2015, core interventions designed to increase BIS governance were distilled into the initial requirements for the SecuriMeter artefact [30].

5 Artefact Requirements that Solve Problems

The objective of DSR research is to establish artefacts that solve real-life problems. The collective set of requirements within the DSR artefact should contribute in this goal. Frequent validation involving stakeholders, such as users, engineers and customers to confirm that the artefact requirements actually help solve the problem at hand is necessary. Wieringa [31] refers to using the regulative cycle to determine the right set of artefact requirements and to validate if it contributes to solving the problem. In Q1 of 2012 five managers participated in a Group Support System (GSS) session. GSS research was used to enable social interaction between stakeholders suffering from the problem of a one-dimensional spreadsheet approach that limits sharing of knowledge and thus intersubjectivity. GSS was used throughout this research project to establish

consensus on the artefact requirements [32]. The aim of this GSS session in 2012 was to discuss, select and prioritise the initial dashboard requirements for the artefact. The question was: *Which management information would CIOs and CISOs consider important for managing their business security (from governance to operation)?* The table below shows the top 5 items (out of a total of 22) (Table 1).

Table 1. Top 5 management information items for BIS according to CIOs and CISOs.

Management information for managing BIS	Rating *
1. Risk thermometer	10
2. Policy versus implementation versus checking with numbers	8.8
3. Factual figures (for management presentation purposes)	8.8
4. Hot items	8.3
5. Audits and 'traffic light reports'	8

*Scale from 1 to 10, in which 10 is most important.

These requirements were designed and engineered in the artefact, taking a Design Science Research approach. An important contribution was made by collaborating with experts in the field on extracting operational and process data and processes for use in the artefact. Since 2010 numerous GSS sessions contributed in additional requirements for the artefact such as assessments to capture operational data. Besides our own experience of GSS sessions to co-develop new requirements, De Vreede et al. [33] also revealed that brainstorming groups using GSS "to *generate more unique ideas, and higher quality ideas than groups doing manual brainstorming."* In the table below we highlight the most relevant and significant contributions that were made on the data level since the establishment of the artefact in 2010 (Table 2).

Table 2. Summary of security assessments in the artefact designed to solve practical problems.

Initiation date	Problem	Requirement to solve the problem	Result # tests at organisations
9-8-2011	Lack of insight into virtualisation risks (version 4)	Virtualisation Security Assessment	7 assessments on version 4 and 8 assessments on version 5 per 4-7-2013*
12-8-2011	Lack of insight into Web threats and risks	Web application vulnerability assessment	+20 assessments since 2011
12-8-2011	Lack of insight into firewall configuration vulnerabilities	Firewall security assessment	+10 assessments since 2011
9-8-2011	Lack of insight into Wireless networks' vulnerabilities and risks	Wireless vulnerability assessment	+5 assessments since 2011

(*continued*)

Table 2. (*continued*)

Initiation date	Problem	Requirement to solve the problem	Result # tests at organisations
12-8-2011	Lack in insights into LAN vulnerabilities	LAN vulnerability assessment	+40 assessments since 2011
5-6-2012	Lack of insight into social media usage and related risks	Social media vulnerability assessment	5 assessments taken on 4-7-2013*
11-4-2013	Lack of cookie compatibility	Cookie assessment	+2 assessments since 2013
11-4-2013	Lack of DigiD pre-audit requirements	DigID pre-audit	+10 assessments since 2013
9-11-2011	Lack of BYOD vulnerabilities and risks	BYOD assessment	
14-6-2013	Lack of insight into web application vulnerabilities	Web application vulnerability assessment	+20 assessments since 2013
13-10-2013	Lack of database vulnerabilities and risks	Database security assessment	+2 assessments since 2013

*Vulnerability reports in an XML format. This functionality provides the opportunity to import all XML reports into the artefact using the API for DLL parsing functionalities.

6 From Enterprise Ontology to Securimeter Artefact

An artefact comparison against an existing other artefact can bring additional insights on the working and the artefacts' positioning compared to other tools. It can also support the future development process of the artefact. In agreement with the manuscript commission an objective comparison between SecuriMeter and a similar security measurement and reporting tool is proposed. The manuscript commission and then researcher agreed to compare the SecuriMeter Artefact with the tool of the Information Security Forum (ISF), "The ISF Accelerator". By comparing both tools based on the ENISA criteria (1), these criteria were set based on an extensive examination by ENISA into Information Security and Risk management tooling. According to the manuscript commission these criteria are sufficient for the required comparison and will contribute the research project in its' academic contribution. In agreement with the promotors and the manuscript commission it was decided that in addition to the ENISA criteria, both tools also needed to be compared based on the scientific claim (e.g. functionalities) that were derived from this research work and as presented in this paper (2). Since this research project is based on Design Science Research, and the control over progress and effects within DSR are typically at the hands of the person designing, i.e., the researcher, the comparison needs to be objective, thus without interference of the researcher, and repeatable. Important note is that during the comparison study no new release of the artefact was made, thus the entire study was executed on the same version.

I have selected GSS as a method for this qualitative comparison of tooling since GSS is also proposed in the entire project as a research method to gain a deeper understanding of the topic and to record intermediate steps. GSS is a research method

that can use multiple iterations, with or without group interactions [31] and all steps, scores and arguments are recorded in the GSS software to assure objectivity, controllability, repeatability. With this in mind the following research approach is proposed.

Research Approach for the Artefact Comparison
The risks of objectivity, controllability, repeatability and generalisability are taken into consideration during this comparison study. Therefor the following objective criteria and controllable steps are embedded. The criteria that form a "Frame of Reference" are:

– 1. ENISA Criteria, and
– 2. Additional criteria derived from the deliverables in this PhD research project:

The following controllable research steps and goals are proposed;

First Step:
- The researcher submits the criteria proposed by the commission, being ENISA criteria, and the presented functionalities of the SecuriMeter artefact to the promotors. The entire list of criteria is also attached in the appendices. The goal is to have clear predefined criteria which can be compared in the next steps (Table 3).

After this the 100 + criteria are delivered to co-promotor professor Mulder who processed the criteria in an online survey tool so a group of experts can prioritize the criteria on relevance for comparison. Before submitting it in final version to the experts Mulder requested a group of nine people to test the set-up, in this pre-test the criteria, the listing and the online tooling. This is called step 1a. According to Recker [34] Page 78, "*a pre-test is a tryout, and its purpose is to help produce a survey form that is more usable and reliable. Pre-testing helps refine the instrument and ensure executability of the survey"*. Recker describes on page 80 of his book to perform an instrument pre-test three objectives to pursue when doing pre-tests of survey instruments:

- *Evaluate the authenticity of the questions,*
- *Evaluate the survey interface and layout, and*
- *Establish validity and reliability of the survey instrument.*

Table 3. List of participant characteristics of the online survey test step 1a.

Participant	Role	Industry	Submitted
1	Project manager security	Financial services	Y
2	Director	HR services	Y
3	Director	Educational services	N
4	Manager SOC	Telecom	Y
5	Manager call center	Financial services	Y
6	Director	Risk & security company	Y
7	Security architect	Government	Y
8	Teacher security	Educational services	Y
9	Security officer	Government	Y
10	Project manager security	Airport/Aviation	Y

After the test feedback is gained to improve the tool, listing and prepare the real sessions. Also potential ambiguous terms or vague items can be detected and anticipated on. After this a large heterogeneous group from multiple business domains can score the provided criteria based on relevance for comparison and on the validity for the risk and security field. In this initial step the participants are not able to influence each other [35] nor are they influenced by the session operator professor Mulder (Table 4).

Table 4. Participant characteristics in the comparison study step 1b.

Participant	Role	Industry	Submitted online	Present at 6 July session
1	CISO	Media	Y	N
2	CISO	Financial services	Y	N
3	Software security specialist	Software testing	Y	Y
4	Manager	Accountancy	Y	Y
5	Consultant	Security services	Y	Y
6	Consultant	Security advisory	Y	N
7	Director/Professor	Research institute	Y	Y
8	Partner at consulting firm	Security and risk advisory	Y	Y
9	Director EMEA	Security and risk advisory	Y	N
10	Director security services	Security and risk advisory	Y	N
11	Consultant	Security and risk advisory	Y	Y
12	Auditor	Financial services	Y	N
13	Information security officer	Government	Y	Y
14	Auditor	Financial services/Auditing	Y	N
15	Consultant in education	Educational services	Y	N

With this step all scores are recorded per participant and analytical motivations are submitted in the system. This is to assure the objectivity, controllability and repeatability during and after the research project.

An additional GSS session is held based on the online pre-submitted data. This so called “Relay Group method” increases the productivity of the group and enables a double loop learning which increase the quality of the outcome [33]. To address the large deviations between the individual scores and to discuss this in the group a better qualified core set of criteria is established which has been validated by experts from the

field. Also a prioritisation of all the criteria is done based on the relevance for a comparison study.

All steps, scores and arguments are submitted in the GSS system to assure the objectivity, controllability and repeatability. The sessions are moderated by an experienced session moderator, which is required according to the ground rules of group moderation published by Hengst [36] and addressed in multiple other publications [37–39]. The objective of this first step is to selectively narrow down the 100 + list of criteria to eventually establish a core set of criteria that can be considered relevant according to experts opinion and to do a further thorough comparison analysis on in the next steps.

Second Step

The second step is to record the two tools in a video demonstration on their performance with regard to the selected criteria.

1. SecuriMeter tool is presented in a demo to present the previous derived criteria (origin; 1 (ENISA) and 2 (Additional)). This demonstration is recorded on film to assure objectivity, controllability, repeatability.
2. ISF "Accelerator" tool is presented in a demo to present the previous derived criteria (origin; 1 (ENISA) and 2 (Additional)). This demonstration is recorded on film to assure objectivity, controllability and repeatability.
   The objective of this second step is to deliver two tool demonstrations on video about the core functionalities/criteria of both tools.

Third Step

In this third step eleven other participants from a heterogeneous group participate in a GSS session which will be moderated by co-promotor professor Mulder. A predefined agenda is set and shared prior to the meeting so the participants can individually prepare the GSS session. The GSS session is introduced by the two video demonstrations of the artefacts. According to Recker video films increase the credibility (e.g. internal validity) (page 94), this method was chosen to assure the objectivity and controllability of the comparison study [34]. All 11 participants are asked to compare the presented functionalities and score the functionalities. All steps, scores and arguments are recorded in the GSS system to assure the objectivity, controllability and repeatability of the research. The objective here is to deliver an in-depth analysis on the predefined selected criteria and an analysis on the deviations given by the expert respondents (Table 5).

The Final Deliverables of These 3 Steps Are:

- Clearly defined criteria for the tool comparison.
- Two demonstrations of both tools recorded on film.
- An in-depth comparison analysis of both tools based on predefined criteria.

Deliverables

The first an online pre-test to test the working of the meeting wizard tool was executed among 9 participants. After that step an online survey (blind, different time different place) was executed to get the initial input on all the comparison criteria. The objective

Table 5. List of participant's characteristics of the GSS expert panel held on 10th August 2017 (step 3).

Participant	Title	Role	Industry	Invited	Present at 10th Aug
1	Dr.	Security consultant	Information security services	Y	Y
2	Drs, MA	Advisor	Government	Y	Y
3	Dr. RE	Auditor/lecturer	Government	Y	Y
4	MSc CISA	Consultant	Information security services	Y	Y
8	Drs, CISM, CISA	Auditor/ISACA Chair	Financial services	Y	Y
6	MSc, RE	Auditor	Financial services	Y	Y
7	Prof. Dr. ir.	Professor	Education	Y	Y
8	MSc	Consultant	Security services	Y	Y
9	MSc MISM	Information security officer	Transportation	Y	Y
10	BC, RE	Auditor	Financial services	Y	Y
11	MSc	Information security officer	Government	Y	Y

Table 6. Type of test during the comparison including dates.

Type of test	Date	Step
Online survey test	20 June 2017	1a
Blind test	2 July 2017	1b
Criteria selection session	6 July 2017	1b
Video demonstration	2 Augustus 2017	2
Comparison session	10 August 2017	3

is to have the participants of this session get to know the items and prepare their own session. The answers that are submitted by the participants via the online tool are captured in the GSS database and presented to the group based on the largest variance (above 40% non-consensus). The objective in this stage is to get a better understanding on the items that have a large variety. All participants that scored high are asked to provide their feedback. The feedback on all 29 discussed items is captured in the GSS Meeting tool and later on visible in the report. Below are the most relevant comments and learnings and the related decisions are highlighted (Table 6).

- On the criteria "pricing" the remark was made about the fact it can be two folded; price of the product and the pricing model (e.g. user based, processor based, fixed fee, pay per use?)
- It doesn't matter how big the company is, that's only relevant for the scaling. Not relevant for the importance. Small companies can process large amounts of money or sensitive data.
- According to two participants a trail license is key. This is the only way, "seeing is believing". You need to get your hands on the product. One participant scored this low in his first online submission but wants to revise his answer based on the discussion; he thinks it is really relevant.
- The view point on how to look at items is determined by the role you fulfil in the organisation. For example a manager weighs his criteria different than for example the subject matter expert (auditor).
- Initially language seems not relevant by the group but after the discussion that tools in other languages (e.g. Hebrew, Chinese) are limiting in use of acceptance. For example government in Netherlands demands tools in Dutch.
- One participant mentioned: "Some criteria are scored completely different before the session than after the group discussion within the group"
- Another participant raised: "Important is to determine the objective of the tool (doel van de tool) before selection"
- Some of the criteria are not smart was a remark of most of the participants. The ENISA list seems outdated.
- Setting the criteria and the relevance of criteria is also determined based on the level of maturity of the organisation. A less mature organisation requires more guidance.

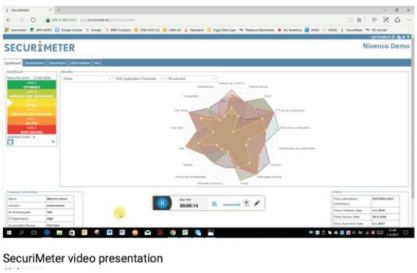
Comparison Criteria

In the final round it is the objective to have the participants selects the core criteria which they think are relevant for the eventual tool comparison. With the knowledge they have gained from the previous rounds and discussions (double loop learning [40]). All criteria are presented via the Meeting Wizard iPad interface and all participants were asked to answer Yes = useful for the comparison, No = not useful for the comparison. A complete list of all comparison criteria arose, ranked based on the score of the group. Below is a list of all criteria with +85% consent, thus 6 out of 6 scored yes.

Videos with Artefact Demonstrations

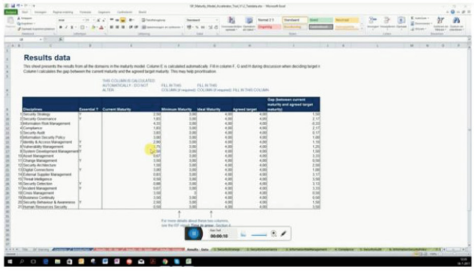
Based on these criteria two video demonstrations are recorded and delivered:

- Securimeter video, accessible via: https://youtu.be/wBNg2oyK4c4. Recorded on 1 August 2017 in Ede
- ISF Accelerator video, accessible via: https://youtu.be/EXLyGUFDwu0. Recorded on 18 July 2017 in Nieuwegein



SecuriMeter video presentation

SecuriMeter



ISF Accelerator

As a final deliverable the objective of the last research step 3 is to collectively compare the core functionalities of a Business Information Security (BIS) artefact. The prepared video clips of two consultants presenting the predefined criteria in the two artefacts, being the "ISF accelerator" and the "SecuriMeter" are required to be watched by the participants prior to the GSS session. The two movies are also shown during the session and will collectively - through group discussion – being used to assess the tools on the availability of the functionalities and thereby compare the two tools.

Prior to the meeting the experts need to prepare this session by looking into the list of predefined functionalities (comparison criteria) and the video script that is used to record the presentations. By looking into this list prior to watching the video the experts will be better prepared for the group session. The entire list of all 37 criteria items including the video demonstrations of the two artefacts were shared one week prior to the session. In the table below the scores of both tools are presented. The variance represents the deviation of the scores of the experts. The deviations above 40% are discussed in the group and further detailed in the analysis section.

Additional Insights after Demonstrating, Evaluating and Comparing the Artefact

In 2000 de Vreede et al. [33] stated that discussion groups working on outcomes of others have better results than groups that start from scratch. De Vreede et al. refer to Decathlon Groups when Groups need to start from scratch and Relay Groups when they work on previous collected data. De Vreede stated: *"Relay groups appeared to be more productive than Decathlon groups, in particular in terms of elaborations to previous contributions" Relay groups also produced slightly more unique ideas, but not significantly. Hence, we may conclude that overall a Relay method is preferable in terms of productivity than a Decathlon method.* In this research project the last expert group used the data of the previous group in order to enable productivity of the group, since rating such an amount of criteria *and* compare the tools based on these criteria may take multiple hours and may be a mental stretch. This might have an impact on the participant's satisfaction. As De Vreede et al. continue in their research *"Relay groups were also found to be more satisfied"*, in terms of interest accommodation.

With this knowledge an additional step was added to the GSS meeting. In addition to the comparison of the two artefacts the experts were also asked, based on their prior gained and shared knowledge, to brainstorm on the research question "*Which parameters that influence the Maturing Business Information Security (MBIS) process can be considered as requirements for an artefact designed to capture, measure and report the MBIS process?*

The objective of this question was to gain a qualified insight through discussion and listing of parameters via experts' opinions. This seems specifically interesting for me as a researcher to see if the experts perceive the same artefact requirements compared to the ones I have gained via this research project. From all 98 answers given by the experts I will highlight the most relevant one that are "already part of the SecuriMeter" artefact, marked as AP, "not yet in the artefact" marked as NP, or are a "part of the analysis method", marked as PAM. PAM refers to the analysis method which enables knowledge sharing, consensus building on priorities, decision-making, stakeholder engagement, increasing the awareness and enables reflection. PAM encompasses two artefacts:

One being the collaborative analysis method that enables team collaboration to define the parameters for analysis of the BIS maturity and two the SecuriMeter tool that supports the administrative work (for measuring and reporting purposes), which can be used to report insights into the state of BIS maturity on multiple levels (strategic, tactical and operational).

A subset of the list that was derived via experts is displayed in the table below. The relevant –new - items that gave new/or inspiring insights on the topic, are listed including my reflection (as a researcher).

Interesting finding from the expert participants is that most of the submitted answers relate to either "preconditions" or "enablers" of the BIS improvement process such as; tone at the top, culture, enable lower in the organisation decision-making, knowledge, education etcetera. These items are most of the time collectively determined based on strategic objectives, regulatory requirements or the type of industry an organisation is in. Therefor the majority, 55 of the total 98, of the items were marked as "part of the analysis method". This means that the majority of the parameters raised by the experts are subject to some form of –team- collaboration.

21 items of the total 98 are already functionalities present within the SecuriMeter aretfact.

10 items are both subject to PAM as well as a future requirement since these are not present in SecuriMeter yet. These items are interesting and reflected below since they can serve as future artefact requirements. 18 items are not yet present but can well be considered as a requirement and are potential backlog items that the developers can take into consideration for the next sprints. Therefor this additional comparison was a meaningful exercise (Table 7).

Table 7. Abstract of the 98 requirement suggested by the experts on multiple levels.

Organisational level	Artefact requirement suggestion submitted by the experts	AP = Already Present in SecuriMeter	NP = Not Present in SecuriMeter	PAM = Part of the Analysis Method	Researchers reflection on suggestions
Governance					
G	Needed: governance structure in which interconnectivity exits between stakeholder on several layers			PAM	Collectively fill in the questionnaires via GSS
G	Link to business objectives			PAM	Can be done via referencing the domains of a standard towards a strategic objective
G	Country of operation		NP		Very relevant functionality for a multinational dealing with multiple foreign regulatory requirements
G	Awareness of what the desired level of maturity is: compliance-driven or self-imposed goals?	AP		PAM	Defining the desired level can be done in SecuriMeter, and how the organisation is engineered in its processes (control oriented, self-imposed, or threat oriented) can also be defined. Stating this is always subject to debate on interpretation for example via GSS
Management					
M	Freedom for taking action			PAM	Needs to be set and mandated by management, for example by working in small Agile teams (DevOps way of working)

(*continued*)

Table 7. (*continued*)

Organisational level	Artefact requirement suggestion submitted by the experts	AP = Already Present in SecuriMeter	NP = Not Present in SecuriMeter	PAM = Part of the Analysis Method	Researchers reflection on suggestions
M	Support prioritizing specific risks and measures: best value for your money.	AP		PAM	This is partly present but can be improved via the IRO. Making the IRO part of a collaborative process to prioritize risk treatments tuned to the value for money
M	Translate known risks into costs of business discontinuity or lost opportunities		NP	PAM	This is partly present but can be improved via the IRO. Making the IRO part of a collaborative process to link risks to lost opportunities
M	Security as part of KPIs, yearplan of employees		NP	PAM	Integrate with HR rewarding mechanisms
M	Tone at the bottom			PAM	
M	Available budget		NP		
M	Look outside the organisation and learn from others their mistakes		NP		
M	Trustworthyness or (un)certainty of data. Data regarding the maturity of a control deteriorates over time.		NP		
M	Different mitigation options incl pro's and con's		NP	PAM	
M	Reliability of management information		NP		Reliability can be improved via sign off process and retention policies on the information submitted in SecuriMeter

(*continued*)

Table 7. (*continued*)

Organisational level	Artefact requirement suggestion submitted by the experts	AP = Already Present in SecuriMeter	NP = Not Present in SecuriMeter	PAM = Part of the Analysis Method	Researchers reflection on suggestions
M	Management approach/type		NP	PAM	Increasingly important due to agile way of working were decision making is delegated more down in the organisation and teams
M	Level of knowledge and expertise of management		NP	PAM	Current knowledge and expertise of management can be assessed via SecuriMeter (e.g. via number of certifications or taken courses), defining the gap can also be done by setting clear knowledge requirements per maturity level per domain. Improvement is needed in explicating the expertise gap
Operations					
O	Every 4 years: review all operations for usefulness and lean		NP		
O	All security operations must have a purpose. if not, DELETE		NP		Enforce alignment of controls towards business objectives. Mandatory functionality to reference a control towards an objective
O	Security data must be an integral part of operational data		NP	PAM	Therefor requires the same BIA process as regular data

(*continued*)

Table 7. (*continued*)

Organisational level	Artefact requirement suggestion submitted by the experts	AP = Already Present in SecuriMeter	NP = Not Present in SecuriMeter	PAM = Part of the Analysis Method	Researchers reflection on suggestions
O	Make improvements visible to employees	AP		PAM	
O	Include operations as active component in improvement of security, not just as only serving for execution of what is decided at other levels		NP	PAM	
O	Skilled employee		NP	PAM	Current skills level can be assessed via SecuriMeter (e.g. via number of certifications or taken -online-courses), defining the gap can also be done by setting clear knowledge requirements per maturity level per domain. Improvement is needed in explicating the expertise gap

7 Conclusions

A key finding of this research is that BIS frameworks and tools mainly focus on subjective opinions, gathered via questionnaires and processed in spreadsheets. In recent years, such opinions have being shared, discussed and evaluated by teams in organisations, making subjective questionnaires intersubjective. However, the structure of these questionnaires is not well suited to scale up within an organisation or in an industry as a whole. The main reason for these limitations of scalability is the need for a unifying ontological model and centralised tool that supports intersubjectivity.

Another finding is that technological monitoring using objective data (e.g. log files, technical state compliance monitoring, etc.) isn't combined with an intersubjective organisational approach, such as SIEM, where data is linked to the ontological layer of transactions. The research on this BIS artefact combines ontological, infological and

data logical layers of information. In the artefact a combination of subjective, intersubjective and objective data is collected, monitored, evaluated and used as a steering mechanism. The first step in this research project (in 2010) was to carry out a literature review and prioritise parameters to be used in the artefact. This was supported by expert views gathered using the 'decathlon' [33] approach to meetings. These were supported by technology that enables many meetings on the same data and with the same outcome requirements to be linked together. In this case, the outcome was to define the functionalities of the experimental artefact. Examples include the ISO 27000 mapping in the research published in 2011 and core interventions designed to improve the maturity of BIS [41]. Study outcomes were all included in the artefact according to this DSR method [26]. Besides these scientific steps, a great deal of empirical data was collected during thousands of development hours in collaboration with individual scholars, universities of applied science, companies and the Dutch Ministry of Economic Affairs.

As shown in this paper, the artefact consists of numerous subjective, and, when shared and discussed, intersubjective questionnaires, import log data collected with the XML parser (objective data) and checklists with weighing that deliver mandatory proof of control effectiveness (intersubjective). Capturing data from multiple security devices (e.g. firewalls), combined with checklists that require evidence, e.g. from DigiD (a Dutch identification method used by the Government) audits, BIC (baseline for Information Security for housing corporations) and BIWA (baseline for Information Security for water companies) audits, virtualisation and cloud audits, is not feasible with spreadsheets. Data showing evidence can be captured in the artefact using the document management function. Combining data and comparing it across industries (benchmarking) is limited, but necessary according to the latest Antwerp Management School validation [42] and numerous studies. Industry measurements e.g. BIWA and Baseline Informatiebeveiliging Gemeente (BIG) are examples of a growing body of valuable benchmarking data in the artefact. Numerous other measurements on for example OWASP (software vulnerability scans) and DigiD, offer other perspectives which provide factual insights into the operations of organisations and enable benchmarking. This contributes to the assurance that boards, senior management, regulators etc. are increasingly demanding in order to achieve more visibility and control.

The discussion during the paper presentation at the Enterprise Engineering Working Conference on 30th of May 2018 in Luxembourg focused on the comparison of two types of Security artefacts showed from the video. Namely the differences between the adoption in organizations spreadsheet based tool 'ISF Accelerator' and the collaborative tool 'Securimeter'. In essence this discussion reflected the relevance of the problem statement and rigour of the artefact requirements.

For page limitations we refer to the online dataset (https://easy.dans.knaw.nl/ui/datasets/id/easy-dataset:77502/tab/2).

Appendix

See Fig. 5.

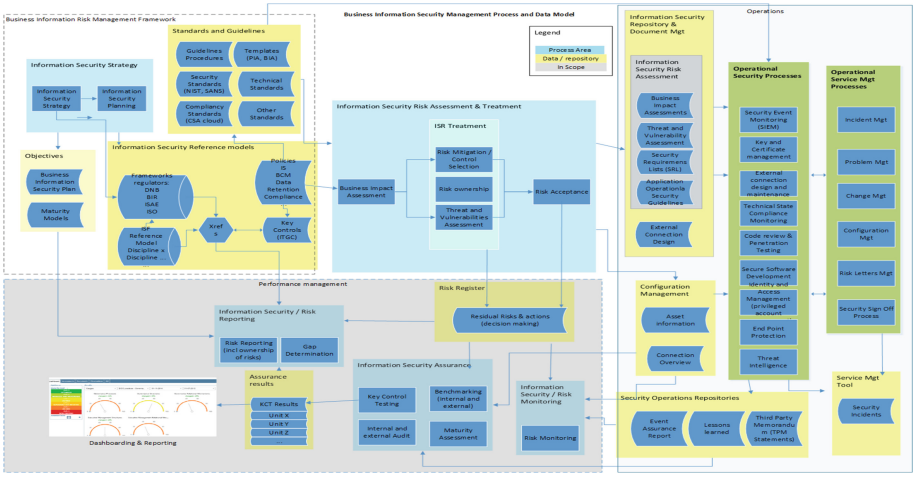


Fig. 5. Meta-model for the BIS processes and data. The grey areas represent the scope of the artefact (dashboard tool).

References

1. Ponemone: Cost of Data Breach Study: Global Analysis, Ponemon Institute LLC, United States (2016)
2. Ponemon Institute: Business Case for Data Protection, Ponemon Institute LLC (2009)
3. Cashell, B., Jackson, W., Jickling, M., Webel, B.: The Economic Impact of Cyber-Attacks, Congressional Research Service, The Library of Congress, United States (2004)
4. ITGI: Information Risks: Who's Business are they?, United States: IT Governance Institute (2005)
5. Alberts, C.J., Dorofee, A.: OCTAVE Method Implementation Guide version 2.0, Carnegie Mellon University Software Engineering Institute, Pittsburgh, Pennsylvania, (2001)
6. Stonenburner, G., Goguen, A., Feringa, A.: NIST Special publications 800-27 Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, Gaithersburg (2002)
7. ISF, IRAM: Information Risk Assessment Methodology 2, Information Security Forum (2016). https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/
8. Hubbard, D.: The Failure of Risk Management. Wiley, Hoboken (2009)
9. ENISA: Principles and Inventories for Risk Management/Risk Assessment methods and tools, Brussel: European Network and information Security Agency (ENISA) (2006)

10. Yaokumah, W., Brown, S.: An empirical examination of the relationship between information security/business strategic alignment and information security governance. J. Bus. Syst., Governance Ethics **2**(9), 50–65 (2014)
11. Zitting, D.: Are You Still Auditing in Excel?. Sarbanes Oxley Compliance Journal (2015). http://www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=4156
12. Flores, W., Antonsen, E., Ekstedt, M.: Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Comput. Secur. **2014–43**, 90–110 (2014)
13. Van Niekerk, J., Von Solms, R.: Information security culture; A management perspective. Comput. Secur. **29**, 476–486 (2010)
14. Seale, C.: Researching Society and Culture, 2nd edn. Sage Publications, Thousand Oaks (2004). ISBN 978-0-7619-4197-2
15. Bobbert, Y.: Use of DEMO as a methodology for business and security alignment. Platform for Information Security, pp. 22–26 (2009). www.ee-institute.org/download.php?id=133&type=doc
16. ISO/IEC27001:2013, ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC, Geneva (2013)
17. Cherdantseva, Y., Hilton, J.: A reference model of information assurance & security. In: IEEE proceedings of ARES, vol. SecOnt workshop, Regensburg, Germany (2013)
18. GOV.UK: The Security Policy Framework (SPF), Statement of Assurance questionnaire in Excel - Gov.uk
19. Halkyn, ISO27001 Self Assessment Checklist hits record downloads, 19 February 2015
20. von Solms, S., von Solms, R.: Information Security Governance. Springer, New York (2009). https://doi.org/10.1007/978-0-387-79984-1. ISBN 978-0-387-79983-4
21. ITGI: COBIT Mapping: Mapping of CMMI for Development V1.2 With COBIT. IT Governance Institute, United States of America (2007). ISBN 1-933284-80-3
22. Koning, E.: Assessment Framework for DNB Information Security Examination, De Nederlandsche Bank, Amsterdam (2014)
23. Volchkov, A.: How to measure security rom a governance perspective. ISACA J. **5**, 44–51 (2013)
24. Papazafeiropoulou, A.: Understanding governance, risk and compliance information systems the experts view. Inf. Syst. Front. **18**, 1251–1263 (2016)
25. Deloitte: Spreadsheet Management, Not what you figured (2009)
26. Bobbert, Y.: Defining a research method for engineering a Business Information Security artefact. In: Proceedings of the Enterprise Engineering Working Conference (EEWC) Forum, Antwerp (2017)
27. Bobbert, Y.: Porters' elements for a business information security strategy. ISACA J. **1**, 1–4 (2015)
28. Dietz, J.: Enterprise Ontology. Springer, Heidelberg (2006). https://doi.org/10.1007/3-540-33149-2
29. MBZK: Baseline Informatiebeveiliging Rijksdienst 2017, Den haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2017)
30. Bobbert, Y., Mulder, J.: Governance practices and critical success factors suitable for business information security. In: International Conference on Computational Intelligence and Communication Networks, India (2015)
31. Wieringa, R.: Design Science Methodology for Information Systems and Software Engineering. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-43839-8
32. Bobbert, Y., Mulder, J.: Group support systems research in the field of business information security; a practitioners view. In: 46th Hawaii International Conference on System Science, Hawaii US (2013)

33. De Vreede, G., Briggs, R.O., Van Duin, R., Enserink, B.: Athletics in electronic brainstorming; asynchronous electronic brainstorming in very large groups. In: Proceedings of the 33rd Hawaii International Conference on System Sciences (2000)
34. Recker, J.: Scientific Research in Information Systems. Springer, Australia (2013). https://doi.org/10.1007/978-3-642-30048-6
35. Asch, S.: Effects of group pressure upon the modification and distortion of judgment. In: Guetzkow, H. (ed.) Groups, Leadership and Men, Carnegie Press, Pittsburgh (1951)
36. den Hengst, M., Adkins, M., Keeken, S., Lim, A.: Which facilitation functions are most challenging: a global survey of facilitators, Delft University of Technology, Delft (2005)
37. Vreede, G., Boonstra, J., Niederman, F.: What is effective GSS facilitation? A qualitative inquiry into participants' perceptions. In: Proceedings of the 35th Hawaii International Conference on System Sciences, Delft University of Technology, Netherlands (2002)
38. Vreede, G., Vogel, D., Kolfschoten, G., Wien, J.: Fifteen years of GSS in the field: a comparison across time and national boundaries. In: Proceedings of the 36th Hawaii International Conference on System Sciences, HICSS 2003 (2003)
39. Kolfschoten, G., Mulder, J., Proper, H.: De fata morgana van Group Support Systemen. Informatie **4**(5), 10–14 (2016)
40. Argyris, C.: Double-loop learning, teaching, and research. Acad. Manag. **1**(2), 206–218 (2002)
41. Bobbert, Y., Mulder, J.: A research journey into maturing the business information security of mid market organizations. Int. J. IT/Bus. Align. Gov. **1**(4), 18–39 (2010)
42. Mari, G.: Cyber Security; Facts or Fiction, Antwerp Management School, 14 November 2016. http://blog.antwerpmanagementschool.be/