Proceedings of the 2014 Federated Conference on Computer Science and Information Systems pp. 863–870
DOI: 10.15439/2014F38
ACSIS, Vol. 2

Enterprise-oriented Cybersecurity Management

Tomasz Chmielecki, Piotr Chołda, Piotr Pacyna, Paweł Potrawka, Norbert Rapacz, Rafał Stankiewicz, and Piotr Wydrych
AGH University of Science and Technology, Kraków, Poland
Department of Telecommunications
al. Mickiewicza 30, 30-059 Kraków, Poland
Email: pacyna@kt.agh.edu.pl

***Abstract*—Information technology is widely used in processes vital to enterprises. Therefore, IT systems must meet at least the same level of security as required from the business processes supported by these systems. In this paper, we present a view on cybersecurity management as an enterprise-centered process, and we advocate the use of enterprise architecture in security management. Activities such as risk assessment, selection of security controls, as well as their deployment and monitoring should be carried out as a part of enterprise architecture activity. A set of useful frameworks and tools is presented and discussed.**

I. Introduction

CYBERSECURITY has been recognized as a business concern and declared an enterprise-wide activity. There is a growing understanding that cybersecurity requirements for the confidentiality, integrity and availability of services provided by the IT infrastructure in an enterprise must be elevated to the same, or higher, level, as the security requirements for the elements of the enterprise that deliver a business function. In consequence, cybersecurity should not be associated with IT technology alone and should no longer be regarded as purely an IT domain. In essence, IT departments are not able to conduct proper risk assessment and mitigation on their own. The information necessary to conduct risk analysis properly is available to business management. When decisions and actions are taken in a process in which IT and business management work together to assess risks and determine priorities in risk mitigation, we can speak about *enterprise-oriented cybersecurity management*. Current practice shows, however, that cybersecurity is still based on technical rules of thumb. The use of formalized methodologies like risk management is not common. The perception of business goals in the process is fragmentary; so many aspects are omitted in cybersecurity. In consequence, the process is incomplete. In this paper, we promote the usage of enterprise architecture-based tools and methodologies to deal with cybersecurity in enterprises which rely on IT infrastructures to deliver products and services.

The proposed approach calls for a paradigm shift in cybersecurity. It requires management personnel to share essential data with IT people to enable business impact analysis and to rely on outcomes that define security priorities. The knowledge of risks in IT departments (likelihood and impact of various threats) and countermeasures should complement the knowledge in business departments. A common workspace for business and IT is an enterprise architecture. It enables collaboration, owing to an improved awareness of the business processes that support the company's mission on one side, and their realization through operational activities, supported by IT, on the other side. The decisions pertaining to security are based on a proper assessment of vulnerabilities and threats and provide options for a response (e.g., continuity and recovery plans, security controls).

Enterprise-oriented cybersecurity management is not a state but a persistent process, with the ability to adapt continuously to a changing environment. Cybersecurity must not be considered an isolated activity—merely a domain-specific precaution against isolated hacking or sabotage activity. Attackers will tend to affect business by targeting general, enterprise-level goals by impairing applications and supporting infrastructure (e.g. platform systems). A vulnerability at one level impacts other levels. Consequently, loss expectancy tends to magnify through cross-layer dependencies. To understand vulnerabilities, risks need to be studied and evaluated top-down: from business principles, through business objectives, and business functions, down to security controls, and also bottom-up for traceability and evaluation. Such analysis is enabled by a thorough description of the enterprise architecture along with an aligned *risk assessment*. Afterwards, the main goal of the *risk response* is to select countermeasures dealing with the risks recognized. The effects of the deployed measures are *continuously monitored*. The enterprise architecture should also drive transition with change management, including major upgrades in security policies and their implementations. One of the critical methods for achieving the goal is risk management [1]–[3]. This should employ enterprise architecture as a valuable source of information about the enterprise. While this may seem engaging too much overhead and may seem counterproductive, even the first exercise will provide value in a reasonable time. In the course of the paper we discuss a collection of tools (e.g., frameworks and software applications) supporting change or risk management.

In our paper, we elaborate on the pillars fundamental to organizing cybersecurity management (enterprise architecture, threat meta-models, risk assessment and response, risk moni-

This scientific research was partially financed by the Polish Ministry of Science and Higher Education from the research budget for 2013-2015, Project No. IP2012 022972 and partially supported by the Polish Ministry of Science and Higher Education under Grant O R00 0119 12. Part of this work was also funded by the Polish Ministry of Science and Higher Education under project 1310/7.PR UE/2010/7.

TABLE I
SELECTED ENTERPRISE ARCHITECTURE FRAMEWORKS

Framework	Context	Description	Advantages	Drawbacks
TOGAF 9.1 (2012)	Open, universal	Provides a process lifecycle to build and manage architecture transitions within an enterprise—Architecture Development Method (ADM) and a set of models.	• ADM is the central point • Ensures a controlled environment for change • Substantially aimed at transitional architectures	Lack of precise model guidance (Archimate 2.0 fills that gap)
DoDAF 2.0 (2009)	Military	Defines a set of views and models for visualizing the complexities in an architecture description and reasoning for various stakeholders. The architecture data gathered becomes central, and the data schemes provided define its structure. There is no obligatory method of development	• Provides data schemes and a precise meta-model • Aimed at transitional architectures • Supports SOA • Tailored for large and complex systems	• No single obligatory method of development • Military-oriented • Limited support for non-functional requirements (like cybersecurity)
The Zachman Framework (2008)	Business	Is best described as a scheme or taxonomy of EA. It classifies views based on six interrogative questions (why, how, what, who, where, when) and five abstraction layers (contextual, conceptual, logical, physical, detailed). No methodology is defined for developing an architecture	• Compact and easy to follow • Well defined viewpoints	• No methodology for building EA • No transitional architectures • Limited support for non-functional requirements (like cybersecurity)

toring) and then summarize how they are integrated. Section II introduces enterprise architectures. Section III deals with the main processes in cybersecurity provisioning, that is, risk management. Section IV summarizes the ideas presented in a unified view. Afterwards, we shortly conclude.

II. ENTERPRISE ARCHITECTURE

Enterprise architecture (EA) is used for the description of complex enterprises. The description includes business processes and their mapping to operational activities for the key processes. It serves as a blueprint for the enterprise structure and operations. Enterprise architecture is a set of models that depict how various business and technical elements work together [4]. Along with ontologies or meta-models, it describes the terminology, the composition of enterprise components, and their relationships with the surrounding environment, as well as the guiding principles for eliciting requirements, design and evolution. The enterprise architecture frameworks (see examples in Table I) are templates for development of instances of EA. A set of languages used to describe the enterprise architectures has been developed and a few of the popular options are sketched in Table II.

A. Role of EA in Security Management

Technically speaking, cybersecurity activity is about establishing a linkage between secured objects and vulnerabilities, threats and countermeasures, as well as monitoring them. Risk is the perception of a relation between these and business objectives. A balance is required between these elements for three essential, interdependent objectives: confidentiality, integrity, and availability. The enterprise approach to cybersecurity requires that risk management should be carried out simultaneously at the business, application, data and technology layers, and combined. Business impact analysis, as a basic step in risk assessment, and business continuity planning, the main concern of risk response, requires precise data about the enterprise. Such knowledge should embrace at least simplified principles defining the enterprise's mission and the manner in which this is accomplished.

Security management should be organized as a process of continuous improvement. Activities such as, for example, risk monitoring, risk assessment, selection of security controls and their deployment need to be carried out repeatedly. Short iterations lend themselves to rapid response to risks that require prompt response.

The security management process causes modifications to the enterprise. These changes can be considerable. As such, they should be staged in transitions describing the change of enterprise architecture.

B. Sample Case Study of EA

To illustrate various EA-related aspects, we have developed a sample view of EA presented in Fig. 1. It shows an architecture for an IT infrastructure supporting a gas transportation process using a networked SCADA control system. As can be seen on the right, EA describes the structure of enterprise organization, business processes, applications and technology that allow the enterprise's goals to be achieved. The notation uses the Archimate 2.0 language, which allows for linking the elements of the architecture together and tracing the relationships among elements. Here, the main business process is gas transportation. This is supported by four subprocesses at the application layer (agreement management, etc.). Those subprocesses are supported by software applications

TABLE II
SELECTED ARCHITECTURE DESCRIPTION LANGUAGES

Framework	Context	Description	Advantages	Drawbacks
Archimate 2.0 (2012)	Enterprise-oriented	Archimate is an architecture description language. The main part covers business, application, and technology layers. There are two extensions: motivation and implementation which makes it compatible with the TOGAF framework. Archimate defines multiple views, but it is possible to define other views, too	• Allows for modeling dependencies • In line with the newest version of TOGAF	• Suitable only for modeling on the enterprise level, lower levels need another notation (like BPMN) • Thus far, a limited set of the supporting software tools
UML 2.1.4 (2013)	Software	UML is a universal language, but is usually perceived as software-oriented and is used for the solution architecture description	Wide modeling software support	Seldom used for business purposes
BPMN 2.0 (2011)	Business	Standard for business process modeling. Provides a graphical notation and model elements focused on business processes and roles. Flow diagrams are similar to UML activity diagrams	Widely used in business analytics	Not possible to map business processes to applications or technologies
UPDM 2.1 (2013)	Military	UML profiles and graphic notation supporting the models and views taken from DoDAF framework	Full enterprise architecture support	Military-oriented
SysML1.2 (2010)	System engineering	Extension of a subset of UML	• Compact set of diagrams • System-of-systems support	No relationships modeled to business

(like CRM system) and cyberinfrastructure (file management system, databases, etc.). After adding security knowledge, it becomes possible, for instance, to trace the impact of a file server fault (induced by DDoS attacks) on two systems: CRM and capacity planning, which as a consequence influence (via the information service) the SCADA control system and impair business processes. A real EA will contain much more information for use by stakeholders (like clients, owner, or governmental administration) and formulated with multiple views. The data can be stored in a repository, where a formal representation of the structure along with the related threat models enables reasoning and reporting on the likelihood or impact of various incidents, thus supporting risk assessment.

C. Vulnerability and Threat Meta-Model

Cybersecurity management requires deep knowledge of vulnerabilities and threats. This knowledge is maintained in respective databases and needs to be incorporated intothe enterprise architecture. To make this possible, efficient meta-model of cybersecurity-related data is necessary. This introduces a vocabulary, syntax, and constraints as well as enables cybersecurity modeling. The enterprise architecture description is enriched by risk assessment with contextual information on cybersecurity issues.

A fragment of an example cybersecurity meta-model is shown in Fig. 2 (see for instance [7] for an alternative model). *Secured objects* span many categories: humans, physical resources, and immaterial assets. All in all, these fall into two classes, being an *asset* or a *process*. They have their own *security attributes* (like a predefined value of availability, for instance). *Vulnerabilities* are attached to security objects during risk assessment. Vulnerabilities will manifest as incidents in the event of a *threat* materialization, which will exploit them. *Risk* is a measure of *likelihood* and *impact* of threat realizations. After the vulnerabilities and threats are identified, it is possible to produce countermeasures using *security controls*, which are a technique for risk response. A control can be accomplished with an organizational procedure (like authentication enforcement) or with an asset protecting other assets (e.g. IPS/IDS systems) or a combination of the two.

III. RISK MANAGEMENT

As a formalized process, risk management aims at dealing with all the threats and related countermeasures in a cyclic manner as shown in Fig. 3. Risk serves as an explicit interface between the business and IT. The following three aspects are taken into account during risk assessment: *exposure* of a secured object to selected threats; and two quantifiable aspects—the *likelihood* of those events, and the *impact* on the enterprise, if they occur. While threat analysis and likelihood evaluation are evaluated by IT experts, the evaluation of impact on business processes is of a non-technical character only, related to financial measures (for instance, penalties for outages), or public safety and liability issues. The business impact is assessed either in qualitative terms (high-medium-low), or preferably in quantitative ways, as this allows for finding a risk response based on optimization methods. Risk assessment has been studied for a long time and commercial frameworks to perform it are also present [8], see Table III. Typically, frameworks suggest what should be done, but not exactly how to carry it out.

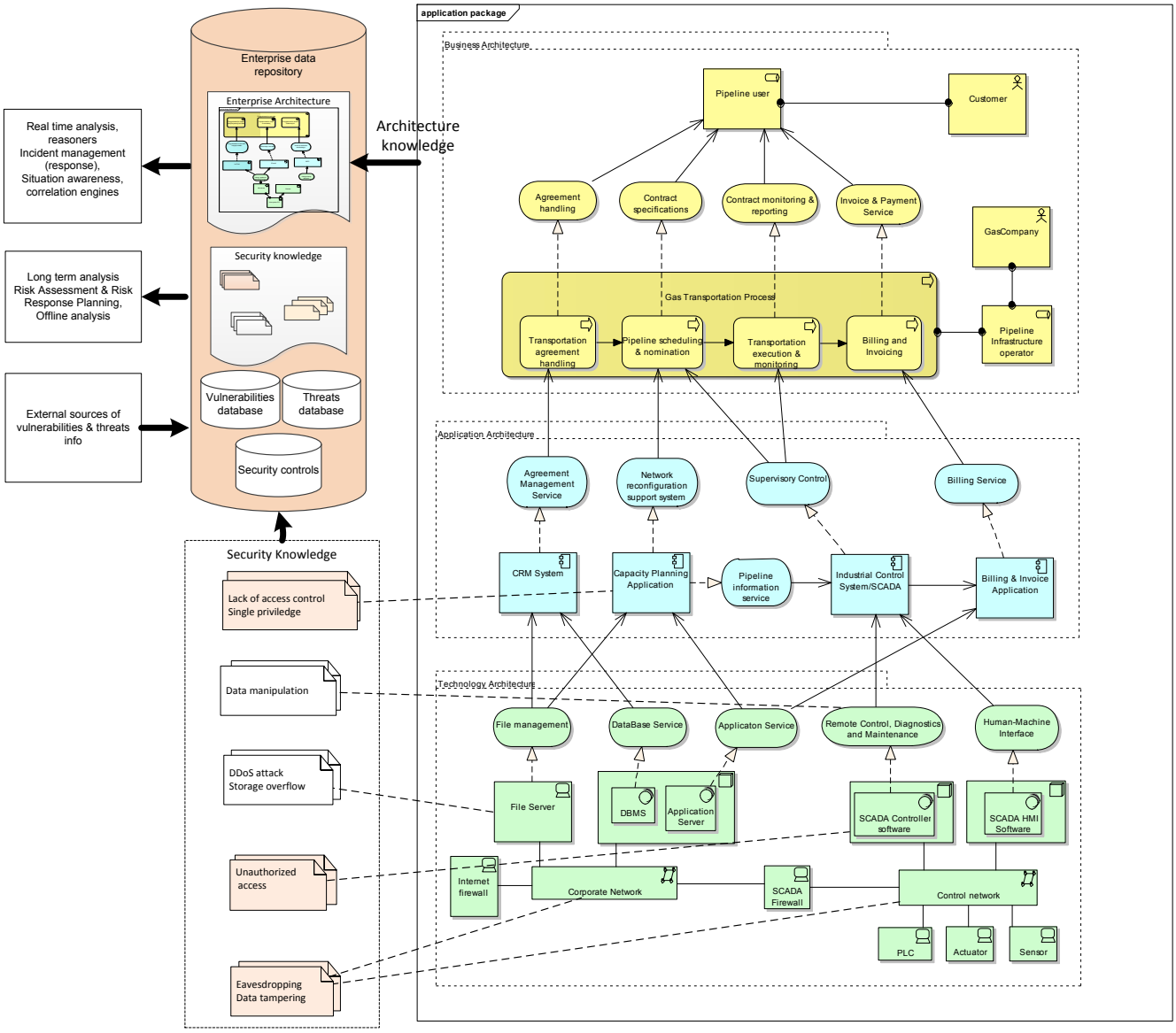

Fig. 1. Role of an example instance of an enterprise architecture in cybersecurity management [5], [6].

Risk management has become overwhelming in information technology as it covers a broad range of issues, as shown in Fig. 4. Its usage in the context of network resilience against attacks is covered in [10] and against random failures in [2]. Sometimes, it is even postulated to engage the end user in this [11], despite some concerns: no clear goals from customers, a low level of considering their actions, a lack of interest in security, a pure lack of technical expertise, or even a slowdown in the adoption of new technologies. Enterprises have better knowledge of their goals, actions and technology to be able to effectively combine the data provided by the enterprise architecture and use it with risk management techniques to improve its operations.

A. *Risk Assessment*

Risk assessment analyzes the enterprise operation from various domain viewpoints: public safety (against threats of massive human injuries); business logic (like checking for process deadlocks); IT cybersecurity in relation to a specific industry field (e.g. SCADA concerns in oil transportation systems); The system-of-systems analysis encompasses methodologies for analyzing multi-scale, interconnected and interdependent systems with emergent behaviors [12]. The following three types of failures are characteristic of interdependent infrastructures [13], but can also be observed in Fig. 1.

- Cascading: when a failure in one infrastructure causes the failure of other infrastructures (note the propagation of technology failures all the way up to business process

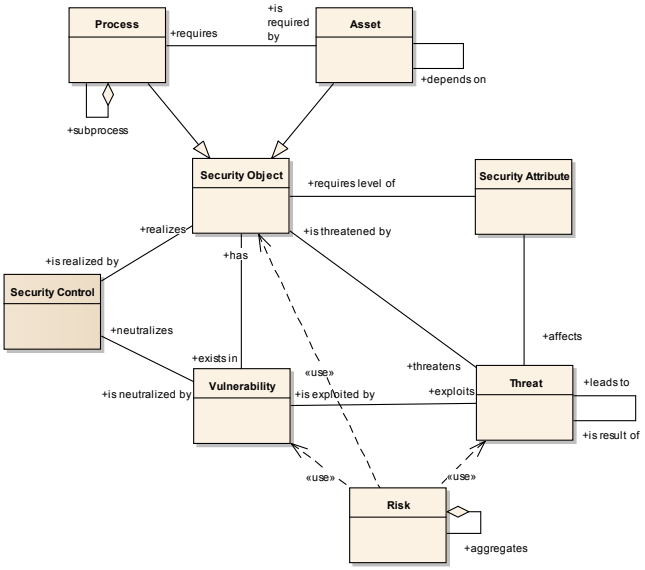

Fig. 2. Cybersecurity meta-model [5], [6].

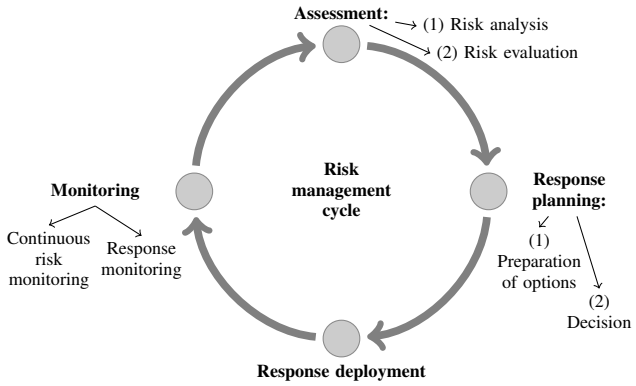

Fig. 3. Simplified risk management cycle [9].

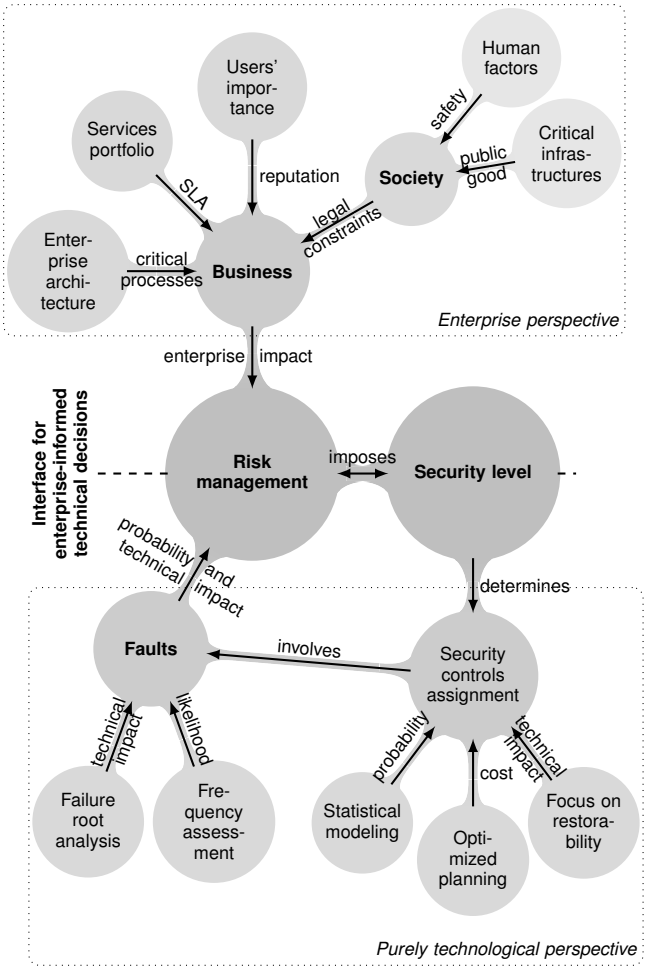

Fig. 4. Different aspects of risk management.

discontinuity).

- Escalating: when an existing failure in one infrastructure exacerbates an independent failure in another infrastructure, increasing its impact (see the earlier example of a file system failure in combination with SCADA control faults).
- Common cause: when two or more infrastructures are affected simultaneously because of a common event (see the destructive impact of corporate network outages on all subprocesses).

Basically, risk assessment consists of risk analysis (identifying vulnerabilities, threats, and related risks) and risk evaluation, determining their probability and impact on the business goals. Although risk can be assessed qualitatively, where probability and impact are assessed using ordinal scales (e.g. small-medium-high) and their combinations, a more sophisticated approach, known as probabilistic risk assessment (PRA), is more meaningful. It is a strictly quantitative approach during which both impact and probability are assessed and expressed mathematically [14]. In the best case scenario, the full probability distribution function (PDF) of the impact expressed in monetary units can be found. In this case, business-related measures like Value-at-Risk (VaR) can be applied. These are easily understood in the investing sector, and therefore can be useful in communicating risk to management. Although such measures were invented for the banking sector to assess the obligatory level of savings, it is suggested that they be used in the telecommunications sector to assess the level of cybersecurity-related investments in network design [2], [10], [15], [16]. The usage of such metrics is especially useful as there is a large toolbox of optimization methods elaborated in the modern portfolio theory, for which VaR is the basic quantitative risk measure and can be used during risk response planning.

B. Risk Response

After analyzing threats and evaluating the related risks, it is necessary to prepare a risk response proposal to be decided and accepted by business management. One of the

TABLE III
SELECTED FRAMEWORKS SUPPORTING RISK MANAGEMENT FOR IT CYBERSECURITY

Framework	Scope	Advantages	Drawbacks
COBIT 5.0, **Risk IT**, **Val IT** (2012)	IT governance (COBIT) combines a business perspective and IT control model approach. Risk IT focuses on IT-enabled risk management and Val IT covers financial IT governance	• Emphasizes relationships between business and IT processes • Includes aspects of control, risk, cost efficiency and maturity • Compatible with audit procedures • Uses RACI (Responsible-Accountable-Consulted-Informed) charts presenting a detailed allocation of responsibilities	• Lack of technical details and low level practices • No description of methods to transition
SABSA (2009)	Framework for the development of a security architecture in an enterprise	• Intuitive and understandable distribution of layers • Well planned and described risk management processes and their succession, interfaces and attributes	• Lack of coverage of all aspects of IT cybersecurity at an equal detail level • The concepts covered without the required explanation, which makes it difficult to properly implement
ITIL 3.0, **M_o_R** (2011)	A set of practices for IT service management, combining IT services with a business perspective	• Popular and widely used description language • Recommendations based on best practices • IT service management considered in a systematic and consistent manner	• Expensive to implement • Long time to implement correctly • Neither generic nor self-sufficient, should be combined with another risk management framework
CC-ISO 15408 ver. 3.1 (2009)	International technical standard for IT cybersecurity certification of products related to IT	• Facilitates risk assessment in relation to particular assets (systems, applications, devices) • Defines different levels of cybersecurity and quality requirements	• Expensive to implement • Used mainly at the development stage • Does not support a holistic approach to the organization, but focuses only on the evaluation of a particular resource or product

most important parts of the risk response is to ensure continuity in the business process operation. This is performed by *business continuity planning* and *disaster recovery* [17], where continuity may be defined as a state in which a system is operational again after disruption at a well-defined level after a certain time, bounded by the maximum tolerable downtime parameter. While it is possible that this goal can be realized by various methods, scenarios are prepared. Each scenario should contain a set of countermeasures (*security controls*), their manner of implementation, the resulting risk change and the cost involved. The first decision is how to deal with recognized risks. Typical decisions that are relevant in the technical context are as follows: *acceptance* when nothing is done about the recognized risks (no changes in comparison to the actual state are necessary); *avoidance* of situations where threats take place (elimination of a problematic information system with many vulnerabilities); *reduction* of the likelihood (addition of a firewall decreasing the number of successful attacks); *mitigation* of the impact, the most popular decision (encryption of data so that it cannot be used even if stolen). Three most common strategies apply to mitigation [18], [19], see Fig. 5:

- *Risk minimization*: choice of the minimum impact possible; can be very costly but might be the first choice especially in critical infrastructures, where the public good is most important.
- *Total (benefit) coverage*: a strategy where the cost of scenario implementation is balanced with the reduction in impact; the strategy is imposed by NIST series of recommendations [20] for US federal institutions.
- *Profit maximization*: a choice of scenario where the marginal impact reduction is balanced by the marginal cost of this reduction, ensuring minimization of the total cost of incidents and risk mitigation.

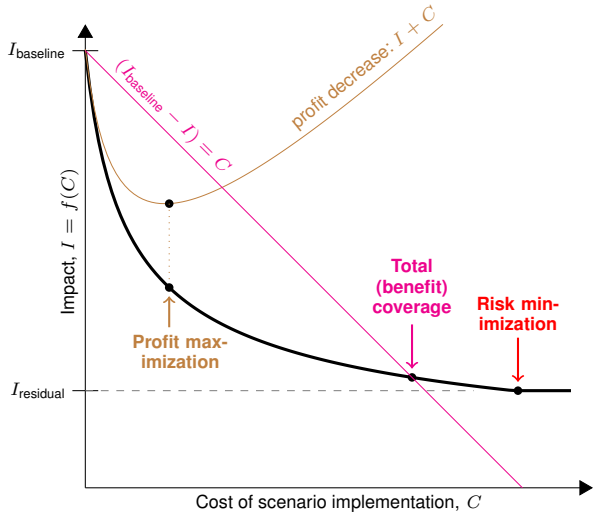

Fig. 5. Illustration of the three basic risk mitigation strategies.

C. Examples of Security Controls

Security controls are countermeasures aimed at avoiding, reducing, or mitigating risk. Two popular catalogues of security controls are ISO 27002 [21] and NIST 800-53 [22] (see Fig. 6). ISO 27002 provides 176 cybersecurity controls organized into twelve sections. The controls contain well defined objectives as well as implementation guidance. Its broad scope makes it applicable to any industry and business of arbitrary size. NIST SP 800-53 groups 317 controls into 18 families organized under three classes:

- *Technical* (e.g. AC-11: session locks).
- *Organizational*: for managing information cybersecurity programs (e.g. MP: media marking).
- *Management*: pertaining to business governance (e.g. PM-10: cybersecurity authorization process).

D. Continuous Monitoring

The main goal of the continuous monitoring process is to maintain up-to-date knowledge about the effectiveness of the risk response scenarios implemented in the enterprise. The monitoring has the following goals:

- to deliver the information about the state of the processes and assets to appropriately assess the current risk;
- to discover changes in processes and assets state that may influence the level of security and effectiveness of the implemented security controls, resulting in new threats;
- to recognize cybersecurity incidents.

Continuous monitoring is responsible for ensuring consistency between the implemented security controls and standards, recommendations and regulations. Collection of cybersecurity related data is a discrete process triggered by incidents, changes, etc. Some of the monitoring tasks can be called repeatedly or on schedule. However, monitoring is a continuous process.

IV. Consolidated View on Enterprise-oriented Cybersecurity Development

So far, we have defined various elements of an enterprise-oriented approach to security deployment. Here, we show how they are integrated. The cybersecurity management process will consist of at least four repetitive steps: risk assessment (adjust), risk response (plan), implementation of security controls (do), and continuous monitoring (check).

Each of the four phases of the cybersecurity management process consists of several tasks. The scope, granularity and time frame depend on the enterprise. The activities of the process are carried out with a focus on various aspects pertaining to different layers of the EA: business, application, or technology. Security principles, requirements, goals and constraints are thus formulated at various levels of enterprise description. The implementation process should be coordinated at various levels, in accordance with the four steps. The scope is tailored to the enterprise's needs, priority and the available level of funding. The activities may have different durations, but they complement each other. For example, an implementation of a security control protecting a server against a specific attack at the technology level supports a security implementation process at the application level dealing with the classification of confidential information which, in turn, protects a well defined business goal (e.g. compliance with the regulations on personal data security).

The processes organizing the cybersecurity management cycle operate on various time scales. The incidents require a rapid response. Also, new vulnerabilities should be addressed without delay. In such cases, primarily risk assessment, response and implementation of security controls must be performed rapidly. Then, these are based on common IT cybersecurity practices, not always optimal from the cost viewpoint. Immediate solutions are called 'quick wins.' On the other hand, a security implementation related to a new project run in the enterprise, the deployment of new assets, or the creation of novel operational processes result in triggering a long-term process. Each phase will then require very careful analyses and involve much more time.

The EA transition process should be closely related to the security implementation process. While defining current state and intermediate state (transitional) enterprise architectures, all recognized assets and processes will require risk assessment and the preparation of a risk response. The security controls should be employed together with the implementation of the new enterprise architecture.

A new instance of security implementation process may be triggered in various cases:

- Continuous monitoring recognizes that an implemented security control has become ineffective or inadequate (e.g. due to a change in the surrounding environment).
- A new vulnerability in an asset or a new threat exploiting a recognized vulnerability has been announced.
- New assets have been deployed in the enterprise: all dependent systems must at least be assessed from the risk viewpoint.
- The process of enterprise architecture transition has started (e.g. due to a business management decision).

V. Conclusions

Cybersecurity is crucial to the contemporary enterprise. We describe a business view of cybersecurity by showing recognized frameworks known thus far in enterprise governance. Enterprise architecture frameworks allow the development of an EA, which is crucial to properly address risk, but differ in the extent to which they guide through the cybersecurity aspects. Given the vast number of incidents, machine-assisted decision support becomes a decisive factor and this is the main issue to be solved in the future.

References

[1] M. E. Johnson *et al.*, "Security through Information Risk Management," *IEEE Security & Privacy*, vol. 7, no. 3, pp. 45–52, May/Jun. 2009. [Online]. Available: http://dx.doi.org/10.1109/MSP.2009.77

[2] P. Chołda *et al.*, "Towards Risk-aware Communications Networking," *Reliability Engineering & System Safety*, vol. 109, pp. 160–174, Jan. 2013. [Online]. Available: http://dx.doi.org/10.1016/j.ress.2012.08.009

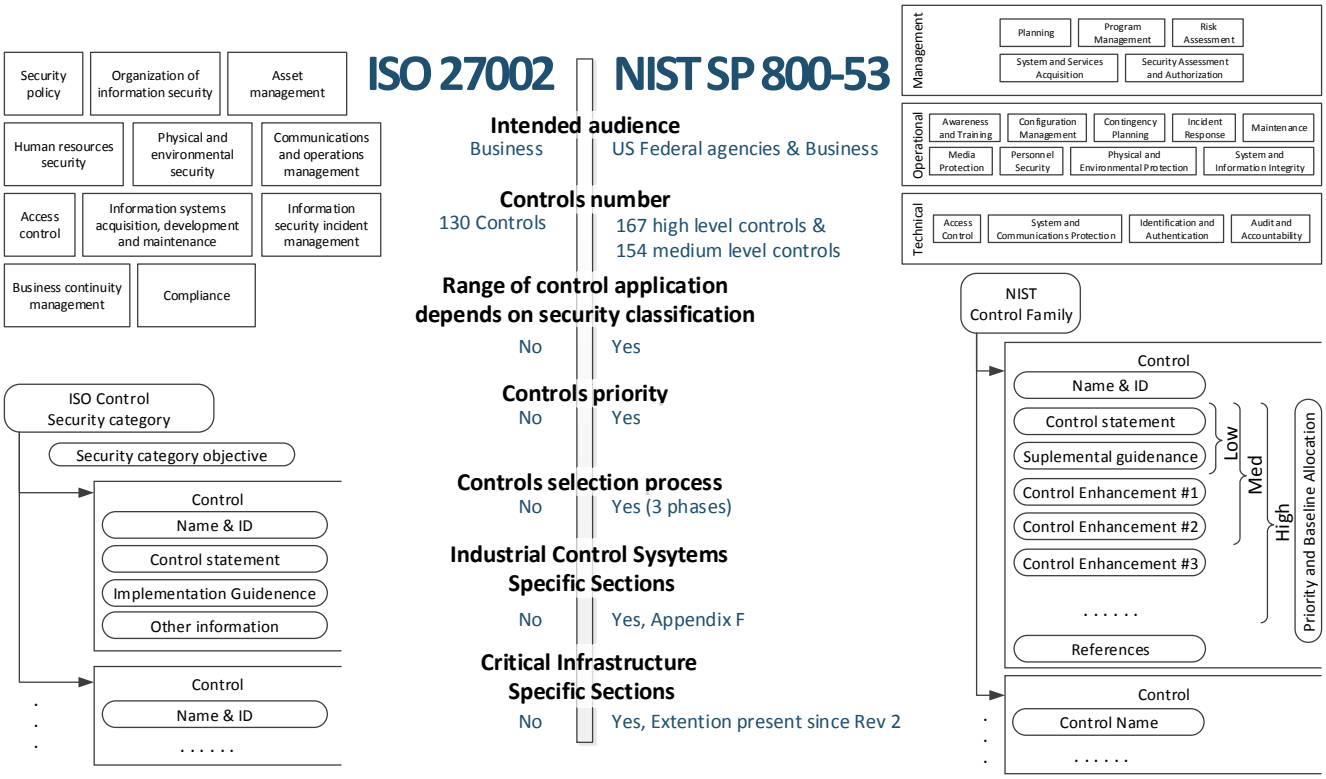

Fig. 6. Comparison of security controls defined by ISO and NIST.

[3] P. Pacyna *et al.*, "Założenia i cele metodyki OKIT do wdrażania systemu bezpieczeństwa teleinformacyjnego w infrastrukturach krytycznych," in *Nowoczesne systemy łączności i transmisji danych na rzecz bezpieczeństwa. Szanse i zagrożenia*, A. R. Pach *et al.*, Eds. Warszawa, Poland: Wolters Kluwer Polska SA, 2013, pp. 442–457, (in Polish).

[4] J. Barateiro *et al.*, "Manage Risks through the Enterprise Architecture," in *Proc. 45rd Hawaii International Conference on System Sciences HICSS-45*, Grand Wailea, Maui, HI, Jan. 4-7, 2012. [Online]. Available: http://dx.doi.org/10.1109/HICSS.2012.419

[5] N. Rapacz *et al.*, "Elementy skutecznego zarządzania bezpieczeństwem w przedsiębiorstwach obsługujących infrastruktury krytyczne," in *Nowoczesne systemy łączności i transmisji danych na rzecz bezpieczeństwa. Szanse i zagrożenia*, A. R. Pach *et al.*, Eds. Warszawa, Poland: Wolters Kluwer Polska SA, 2013, pp. 458–475, (in Polish).

[6] P. Pacyna *et al.*, *OKIT. Metodyka ochrony teleinformacyjnych infrastruktur krytycznych*. Warszawa, Poland: Wydawnictwo Naukowe PWN, 2013, (in Polish).

[7] S. Fenz *et al.*, "Information Security Risk Management: In Which Security Solutions Is It Worth Investing?" *Communications of the Association for Information Systems*, vol. 28, no. 22, pp. 329–356, May 2011.

[8] J. Araujo Wickboldt *et al.*, "A Framework for Risk Assessment based on Analysis of Historical Information of Workflow Execution in IT Systems," *Computer Networks*, vol. 55, no. 13, pp. 2954–2975, Sep. 15, 2011. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2011.05.025

[9] P. Chołda and B. E. Helvik, "Reliable Network-based Services," *Computer Communications*, vol. 36, no. 6, pp. 607–610, Mar. 15, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.comcom.2013.01.003

[10] T. Ackermann, *IT Security Risk Management. Perceived IT Security Risks in the Context of Cloud Computing*. Wiesbaden, Germany: Springer Fachmedien, 2013.

[11] A. van Cleeff, "A Risk Management Process for Consumers: The Next Step in Information Security," in *Proc. New Security Paradigms Workshop NSPW'10*, Concord, MA, Sep. 21-23, 2010. [Online]. Available: http://dx.doi.org/10.1145/1900546.1900561

[12] Y. Y. Haimes, "Models for Risk Management of Systems of Systems," *International Journal of System of Systems Engineering*, vol. 1, no. 1/2, pp. 222–236, 2008. [Online]. Available: http://dx.doi.org/10.1504/IJSSE.2008.018138

[13] S. M. Rinaldi *et al.*, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 11–25, Dec. 2001. [Online]. Available: http://dx.doi.org/10.1109/37.969131

[14] M. Todinov, *Risk-Based Reliability Analysis and Generic Principles for Risk Reduction*. Amsterdam, The Netherlands: Elsevier Science & Technology Books, 2006.

[15] L. Mastroeni and M. Naldi, "Violation of Service Availability Targets in Service Level Agreements," in *Proc. Federated Conference on Computer Science and Information Systems FedCSIS 2011*, Szczecin, Poland, Sep. 18-21, 2011.

[16] A. J. Gonzalez and B. E. Helvik, "SLA Success Probability Assessment in Networks with Correlated Failures," *Computer Communications*, vol. 36, no. 6, pp. 708–717, Mar. 2013. [Online]. Available: http://dx.doi.org/10.1016/j.comcom.2012.08.007

[17] T. Costello, "Business Continuity: Beyond Disaster Recovery," *IT Professional*, vol. 14, no. 5, pp. 62–64, Sep./Oct. 2012. [Online]. Available: http://dx.doi.org/10.1109/MITP.2012.92

[18] E. E. Anderson, "Firm Objectives, IT Alignment, and Information Security," *IBM Journal of Research and Development*, vol. 54, no. 3, May/Jun. 2010, paper 5. [Online]. Available: http://dx.doi.org/10.1147/JRD.2010.2044256

[19] P. Chołda, "Risk-Aware Design and Management of Resilient Networks," in *Proc. 4th International Workshop on Resilience and IT-Risk in Social Infrastructures RISI 2014*, Fribourg, Switzerland, Sep. 8, 2014.

[20] "Managing Information Security Risk. Organization, Mission, and Information System View," NIST SP 800-39, Mar. 2011.

[21] "Information Technology—Security Techniques—Code of Practice for Information Security Management," ISO/IEC 27002, Oct. 2005.

[22] "Security and Privacy Controls for Federal Information Systems and Organizations," NIST SP 800-53, Feb. 2012.