A SYSTEMS APPROACH TO INFORMATION SECURITY FOR THE TWENTY-FIRST CENTURY ORGANIZATION

Author(s) / Auteur(s) :

Dimitrios S. VARSOS
Management system consultant; CSAP Professional
University of Piraeus, Department of Informatics; Hellenic Society for Systemic Studies (HSSS);
MSI Hellas Consulting Group
dvarsos@msi.gr

Stergiani A. GIANNAKOU
Ph.D.; GMP Inspector, CSAP Professional
National Organization for Medicines of Greece; Hellenic Society for Systemic Studies (HSSS)
sgiannakou@eof.gr

Nikitas A. ASSIMAKOPOULOS
Professor
University of Piraeus, Department of Informatics; Hellenic Society for Systemic Studies (HSSS)
assinik@unipi.gr

Abstract / Résumé :

A crisis resulting from disruptive events that threaten to harm the organization or its stakeholders can originate from a plethora of sources. Data breaches, unauthorized disclosures of confidential information, and data leaks, are on the news almost daily. Most guidelines and standards published by prominent International Standards Organizations hold that risk-based thinking supports public, private, and community enterprises (referred for convenience in this work by the generic term "organization") in determining the forces that could cause their key and enabling processes to deviate from planned arrangements, to apply preventive measures to modify risk, and to take advantage of opportunities as they arise. A well-structured Information Security Management System that is developed, implemented, and maintained through sound risk-based thinking, enables the organization to take appropriate actions to address the risks and opportunities associated with its information resources, in a manner that is commensurate to the complexity of its socio-technical infrastructure and the external environment associated with its activities. In this work we explore the Risk Management Process that is outlined in the ISO 31000 international standard, through the requirements/guidelines defined in the ISO/IEC 27000-series of international standards. The knowledge gained is applied to develop a systems driven conceptual structure that can be employed by any organization operating on the complexities of an interconnected environment, for the purpose of designing, implementing, monitoring, reviewing and continually improving a structured Information Security Management System.

Keywords / Mots-clés :

Information security management system, risk managenent, information security model, systems approach.

1. INTRODUCTION

Information security (IS) is fast becoming a necessary condition to operating in a dynamic environment that is often characterized by ambiguity and uncertainty. IS refers to the preservation of the confidentiality, the integrity, and the availability of information, where *confidentiality* relates to non-disclosure of sensitive information, *integrity* relates to the information's accuracy, consistency, reliability, and completeness, and *availability* relates to the information's accessibility by authorized persons, upon demand (International Organization for Standardization, 2018b). A *Management System* is composed of the set of interrelated and interdependent elements that establish policies and objectives, and the means through which to achieve these objectives. The explicit objective of an *Information Security Management System* (ISMS) is to ensure business continuity by minimizing overall risk to the

organization's information resources. The term *information resources* is used in this work to refer to information generated by human activity and the elements of infrastructure used to capture, record, store, process, display, and transmit information, including business application systems, e-commerce, computer installations, networks, and system development activities. An effective ISMS needs to be commensurate to the complexity of the organization's socio-technical infrastructure and the external environment associated with its activities (International Organization for Standardization, 2013a). Organizations, however, frequently adapt IS practices that fail to effectively address the dynamic complexity that is embedded in their (internal and external) business environment, relying on simplification rather than the holistic treatment of complexity. Moreover, IS is frequently treated as an isolated activity rather than an integral part of the organization's management paradigm. In this context, decision-makers often identify and mitigate risks through actions that are derived through *analytical methods* in the context of a *reductionist approach*: *(1)* reducing the whole into its constituent parts, *(2)* understanding each part separately, and *(3)* aggregating understanding of the parts, into an understanding of the whole (Ackoff, 1999).

Although the concept that complex wholes are formed from smaller elements is common to both reductionism and *systems theory*, the reductionist approach simplifies the whole by concentrating on the isolated elements (analysis), while systems theory addresses the dynamic relations that exist among the elements of the whole, focusing on the behaviors that emerge from their interaction (synthesis) (Assimakopoulos & Varsos, 2015).

This work will explore the (generic) *risk management process* that is outlined in the ISO 31000 international standard, which can be used to identify, analyze, and monitor issues of risk. The standard will be examined through the requirements/guidelines that are defined in the ISO/IEC 27000-series of international standards[1]. Further, it will introduce a conceptual structure (model) that is based on a systems approach that can be employed by any organization for the purpose of designing, implementing, monitoring, reviewing, and continually improving a structured ISMS, which can be instrumental in effectively addressing the issues of risk that impact its short, medium, and long-term objectives.

1.1 Paper Structure

This introduction is followed by an epigrammatic presentation of terms and concepts relevant to systems science, and a brief overview of terms and concepts related to IS that are distilled from the ISO/IEC 27000-series of international standards and established literature, which will be used throughout the paper. Then follows an outline of the risk management process that is provided by the ISO 31000 international standard. We continue with the conceptual structure that can used for the purpose of designing, implementing, maintaining, and continually improving an ISMS. It is the objective of this conceptual structure to enable the various operations comprising a modern organization (e.g., business units, departments, functional teams, and the like) to bring the risk(s) associated with their operating environment within their individual response range, while ensuring that their net contribution is congruent with the goals and objectives of the organization's overall risk tolerance. The work concludes with a brief discussion of the implications of our contribution and remarks for future research.

2. THE LANGUAGE OF SYSTEMS & IS: A BRIEF INTRODUCTION

2.1 Systems and the Language of Systems

An organization may be viewed as a purposefully organized system (Figure 1), which is composed of a bounded set of interconnected and interdependent elements that work together in order to achieve one or more desired outcomes (e.g., Forrester, 1968; Flood & Carson, 1988; Ackoff, 1999). The term *element*

[1] The ISO/IEC 27000-series (also known as the 'ISMS Family of Standards') comprises IS standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

refers to an identifiable entity that is capable of behavior that is subject to change. As a building block of a unified whole, each element affects and is affected by every other element in the set, and through its actions and interactions contributes to the function of the whole, relative to its desired outcomes (von Bertalanffy, 1950; Ackoff, 1999). The term *function* is used here to mean the structured process or processes through which resources are transformed from one state to another. In other words, function refers to the production of the outcomes that define the organization's goal or goals (Ackoff, 1971). The interconnections among the elements and the relations that hold them together define the system's *structure*. Subsets of closely coupled elements and the relations that hold them together form *subsystems* that perform specific functions as parts of the system's overall structure. Subsystems exhibit the same characteristics as elements relative to their interdependence and connectivity (Ackoff, 1999).

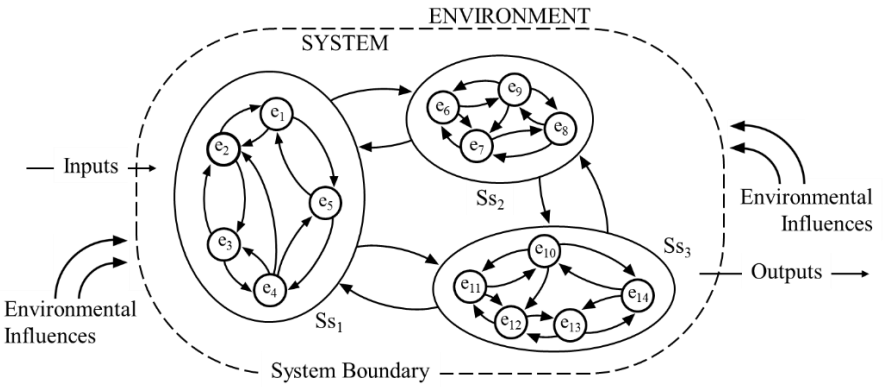

Figure 1. System components: e_x denotes a system element, Ss_x denotes a subsystem, while the arched arrows denote influences. Source: Varsos & Assimakopoulos (2018).

An *open system* interacts with its external *environment*, which is itself a higher order system of increased complexity that is composed of its own elements that can be arranged into subsystems (von Bertalanffy, 1950). An open system secures *input* from its environment in the form of material, information, and energy, and through its function, transforms this input into *output*, which it then released back to the environment. In contrast, a *closed system* is completely self-contained, and as such, does not interact with any elements that are not contained within its non-permeable boundary. The specific values of the variables that describe a system at a moment in time are collectively referred to as the *state* of the system. A system is said to be in a *steady-state* when the internal variables that define its behavior remain stable and constant despite changing environmental conditions. Finally, a system is said to be *effective* when its structure has the capacity to realize through its function the system's overall desired outcome(s), while its *efficiency* is expressed as the ratio between the system's useful output to total input (Varsos & Assimakopoulos, 2018).

2.2 Information Security: Overview of Terms and Concepts

The Business Dictionary (2018), defines *information* as "data that is *(1)* accurate and timely, *(2)* specific and organized for a purpose, *(3)* presented within a context that gives it meaning and relevance, and *(4)* can lead to an increase in understanding and a decrease in uncertainty". In turn, the international standard ISO/IEC 27000 holds that "information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected" (International Organization for Standardization, 2018b). Information may be acquired, stored, organized, manipulated, and displayed/presented in a variety of forms, including material (e.g. paper), digital (binary), and knowledge (in someone's mind). Moreover, information may be transmitted/disseminated by a variety of means, including physically, electronically, and/or through verbal communication.

Risk refers to the effect of uncertainty on the organization's objectives. In this context, an *effect* is a deviation (positive or negative) from the expected, and *uncertainty* is the state (even partial) of a deficiency of information that relates to understanding or knowledge of an event, its consequences, or

its likelihood of occurrence. Risk is characterized by reference to potential events and consequences (or a combination of these) and expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. An IS *event* refers to the occurrence or change of a particular set of circumstances, while *consequences* refers to an outcome of an event affecting the organization's objectives. An IS *incident* refers to a single or a series of undesirable or unanticipated IS events that have a significant probability of compromising the organization's operations. The potential cause of an unwanted incident that may result in harm to a system or the organization is generally referred to as a *threat*. A *control* is a measure that modifies risk, while a *vulnerability* is a weakness in system security, procedures, design, implementation, or a control that can be accidentally triggered or intentionally exploited by one or more threats (International Organization for Standardization, 2018b).

3. THE RISK MANAGEMENT PROCESS

Risk management refers to the coordinated activities that are carried out for the purpose of directing and controlling an organization in regard to risk, within a *risk management framework* A risk management framework is the set of elements (components) that provide the foundations (policy, objectives, mandate and commitment to manage risk) and organizational arrangements (plans, relationships, accountabilities, resources, processes and activities) that are embedded within the organization's overall strategic and operational policies and practices, for designing, implementing, monitoring, reviewing and continually improving risk management (International Organization for Standardization, 2017, 2018b, 2018c). Figure 2 illustrates the key elements of the risk management process defined by the ISO 31000 international standard, which includes: *(a)* communication and consultation, *(b)* establishing the scope, context, and criteria, *(c)* the risk assessment, *(c)* risk treatment, (*d)*, recording and reporting and (e) monitoring and review (International Organization for Standardization, 2018a).

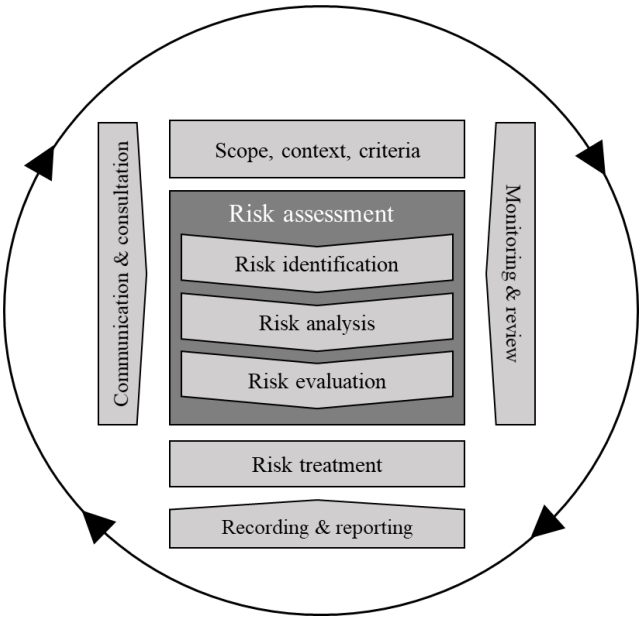

Figure 2: Risk Management Process. Source: International Organization for Standardization (2018)

3.1 Communication & consultation

The stakeholders associated with the organization's activities impacting the ISMS need be identified, and integrated into the decision making process, based on a structured communication and consultation plan. The plan should: *(a)* identify the internal and external stakeholders that are associated with the ISMS, *(b)* address the issues relating to their pluralistic perceptions relative to risk, and, *(c)* provide a coherent strategy that alleviates the actual and/or potential barriers to the plan's effective execution.

Through appropriate communication and consultation the organization ensures that both internal staff (according to their roles and responsibilities) and external stakeholders (depending on the nature of their interest in the organization) are engaged in a manner that promotes alignment to the organization's overall risk strategy and its risk priorities. Bi-directional communication and consultation underlies every subsequent stage in the risk management process. Information exchange with the stakeholders needs to be truthful, relevant, and accurate, taking into account both confidentiality issues and all applicable contractual, legal, and regulatory requirements.

3.2 Scope, context, and criteria *(Framing Risk)*

The scope establishes the purpose of the risk management activities and its processes. Establishing the context includes all the activities that are carried out by the organization for the purpose of understanding the internal and external environment in which it will make its risk-based decisions. The IS criteria are the terms of reference against which the significance of risks that are identified during the risk assessment will be evaluated. In essence, the purpose of this stage is to define the boundaries of the ISMS and to produce a sound risk management strategy that effectively addresses *how* the organization intends to assess, respond to, and monitor risk, making clear the risk assumptions that will be used in making sound decisions concerning IS.

3.3 Risk assessment

The risk assessment includes all the activities that are carried out for the purpose of evaluating the organization's risk exposure, within the context of its risk frame. This stage includes *risk identification, risk analysis* and *risk evaluation. Risk identification* is the process of identifying, recognizing and describing risks. *Risk analysis* refers to the process employed for the purpose of comprehending the nature and level of risk (expressed in terms of the combination of consequences and their likelihood). *Risk evaluation* refers to the process of comparing the results of the *risk analysis* against the risk criteria to determine whether the risk is tolerable.

3.4 Risk treatment

The purpose of this stage is to provide the most appropriate risk treatment option(s) to risks identified during the assessment, in the context of the organization's risk frame. This is accomplished by: *(a)* developing alternate courses of action for responding to risk(s), *(b)* evaluating the alternatives and determining an appropriate course of action that is consistent with the organization's overall risk tolerance, and *(c)* implementation.

3.5 Monitoring and review

Monitoring refers to all aspects of observing and determining the current state of the system's performance, while review encompasses all activities that are carried out for the purpose of ensuring the system's continual suitability, adequacy, and effectiveness. Together, monitoring and review activities provide the required information to improve the risk assessment process and to capture lessons learned from IS events (including near-misses), changes, trends, and successes and failures. Finally, through monitoring and review the organization is able to detect changes in its context and the need to revise the IS Policy and the risk criteria that have been adapted.

3.6 Recording & reporting

Recording and reporting relates to the documentation of outcomes (e.g., intentions, monitoring and measurement results, events, and incidents) and communication to all internal and external stakeholders.

4. A SYSTEMS APPROACH TO INFORMATION SECURITY

The process that is illustrated in Figure 2 reflects the relations that hold among the various elements of a coherent risk management process and their individual and collective contribution to the achievement of an organization's desired outcomes in relation to the risk management of its *information system*. Ackoff (1974) argues that a system is a unified whole that has one or more defining functions and that consists of a set of two or more essential elements (parts) that satisfy three conditions: *(1)* every essential part can affect the behavior or the properties of the whole; *(2)* none of the essential parts can have an independent effect on the defining function(s) of the whole; and *(3)* every possible subgroup of the system's essential parts has to meet the first two conditions. He concludes that the properties of a system are derived from the way that the parts *interact* and not from the manner in which the parts *act* separately. Thus, a systems approach emphasizes the important difference between considering the function of the parts that work together to create a unified whole based on their relations with one another and within the system's larger context (synthesis), versus considering the linear cause-and-effect chains in a disconnected set of parts (analysis) (Assimakopoulos & Varsos, 2015). Synthesis consists of three steps: *(1)* identifying the principle whole of which the object to be studied is a part, *(2)* explaining the behavior and properties of that containing whole, and *(3)* disaggregate the understanding of the containing whole by identifying the role or function of the object to be studied in that whole (Ackoff, 1974).

The level of complexity that is embedded in any risk management process is amplified by the fact that the organization's multiple operations (e.g., business units, departments, functional teams, and the like), which are traditionally organized into specific structures with specialized functions, often pursue diverse outcomes, under varied conditions, which are subject to different forces, at different times (Varsos & Assimakopoulos, 2016). Given the complexity that emerges from this diversity, implementation of a structured ISMS should enable the various operations to bring the risks associated with their specific contexts within their individual response range, while ensuring that their net contribution is congruent with the organization's IS Policy. The organization's ISMS, therefore, should provide a coherent foundation that reinforces top management's capacity to cultivate and cascade IS goals and objectives that are proportionate to the organization's risk attitude, rather than requiring it to rigidly dictate the operational activities that are necessary for the purpose of execution. The later, however, should be carried out by the operations within the strategic boundaries that are defined by the IS Policy, in the context of the constraints that make overall outcomes attainable.

This section introduces a conceptual structure that is based on a systems approach, which can be used as a pragmatic framework to enable the various operations comprising an organization to bring the risks associated with their operating environments within their individual response range, while ensuring that their net contribution is congruent with the goals and objectives of the organization's overall attitude to risk. Prior to the development of the ISMS, an IS Committee (ISC) needs to be appointed that will provide direction, coordination, and control on key issues relating to the system's design, deployment, review, and refinement. The ISC should be composed of a minimal number of individuals with different functional specialties and multidisciplinary competencies, ensuring a balanced representation from each organizational function and level. The ISC members' competence should be enhanced through appropriate education and training, as it relates to IS, performance evaluation systems, and the practical application of theoretical lessons learned in the context of the system's overall goals and objectives.

Figure 3 illustrates the systemic relations that holds among the various stages of the model. It should be noted that the different stages do not unfold as a linear succession of isolated activities, but rather, as a dynamic process that supports fact-based decision-making for effective IS.

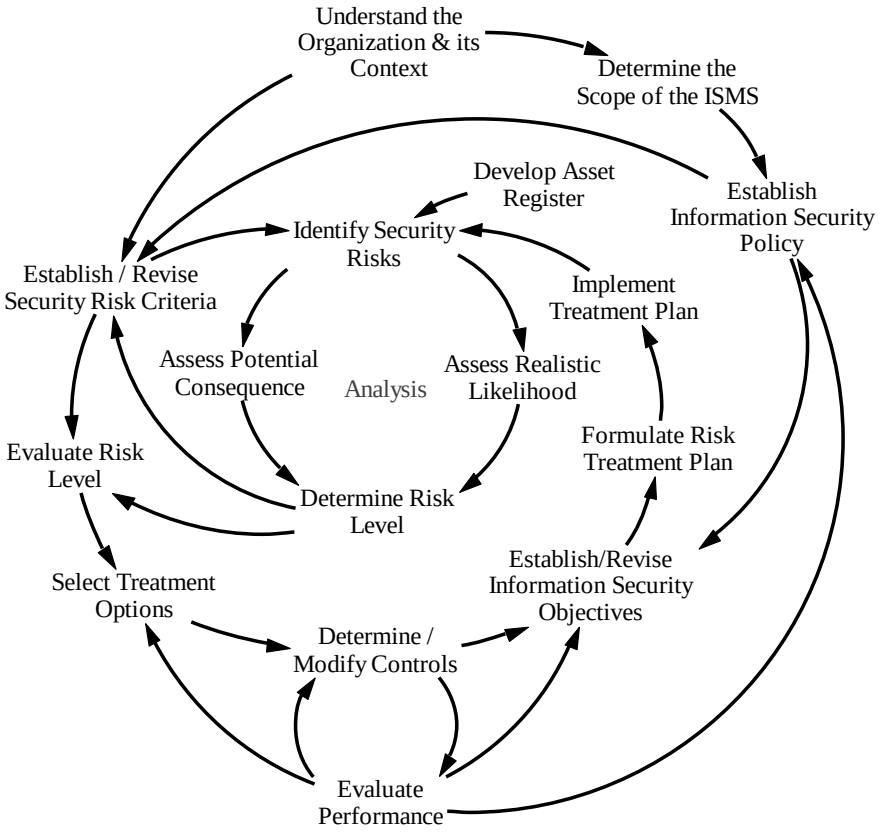

Figure 3: Information Security Management Model.

4.1 Understand the Organization & its Context

Understand the organization & its context refers to the organized output of a structured process through which the ISC will define the external and internal parameters to be taken into account when managing risk. In this context, the organization may be viewed as a complex multi-layered system that is composed of a bounded set of interconnected component parts (subsystems) that work together in order to achieve one or more desired outcomes. The ISC will need to identify the boundaries within which the organization's purpose is pursued, and determine the relevant environment in which the organization carries out its activities. Boundary critiques should consider those elements and their properties that are not a part of the organization but which may nevertheless affect the organization's information resources. The bi-directional channels of interaction between the organization and its environment need to be defined, and the means through which resources are exchanged clearly stipulated. The external context includes (as appropriate): *(a)* the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment that is associated with the organization's activities; *(b)* the key drivers and trends that impact the organization's objectives; and *(c)* the relationships with external stakeholder, their perceptions, values and expectations. The internal context includes (as appropriate): *(a)* the organization's governance model; *(b)* its authority structures, roles and accountabilities; *(c)* policies, objectives, and the strategies that are in place to achieve them; *(d)* capabilities, understood in terms of resources and knowledge; *(e)* the relationships with and perceptions of internal stakeholders; *(f)* the organization's culture; *(g)* information systems, information flows and decision making processes; *(h)* standards, guidelines, and models adopted by the organization; and *(i)* the form and extent of contractual relationships, both with staff members and outsourced service providers (International Organization for Standardization, 2018a).

4.2 Determine the Scope of the ISMS

The scope of the ISMS needs to be articulated having identified the boundaries, purpose, relevant environment, pertinent stakeholders, and having considered the interfaces and dependencies between the activities that are performed by the organization, and the activities that are performed by other, on the organization's behalf. In short, the ISMS's scope articulates (explicitly) *what* the organization intends to protect through its ISMS, irrespective of its storage location and information access policies and procedures.

4.3 Establish the IS Policy:

The organization's top management will need to establish an IS Policy, which provides overall direction relative to the protection of the organization's physical and information technology resources. The IS Policy needs to be aligned with the organization's purpose, provide a framework for setting IS objectives, and include a commitment to satisfy applicable contractual, legal, and regulatory requirements. Moreover, the IS Policy needs to include a commitment to the continual improvement of the ISMS and its results. The IS Policy must be communicated within the organization, be available to all external interested parties, and be revised (as appropriate) following formal system reviews.

4.4 Establish / Revise IS Objectives

Objectives are distinct, time-bound, and quantifiable result that are sought in relation to goals. IS objectives should be developed for all relevant organizational functions and levels within the boundaries of the scope of the ISMS. Further they need to be consistent with the organization's context and IS Policy, and tracked with the use of quantitative performance metrics. Finally, the IS objectives need to: *(a)* take into account all applicable IS requirements (including contractual, legal, and regulatory requirements), *(b)* be communicated to all relevant stakeholders, and *(c)* be updated (as appropriate) following formal system reviews.

4.5 Develop the Asset Register

All assets associated with the organization's information and information processing facilities that will be risk managed need to be recorded in an *asset register*. The person(s) responsible for the business use of each asset needs to be identified and recorded. For a business application, this should be the person responsible for the business process or activity most dependent on the application. In addition to ownership of each asset, the asset register should include (as appropriate) a short description of the asset, an asset ID, and the type of asset in question (e.g., information asset, software asset, physical asset, or service). Moreover, the register should reflect each asset's classification relative to confidentiality, integrity, and availability, based on the implementation of a structured classification scheme. Finally, a determination will need to be made and recorded as to the asset's value (e.g., low, medium, or high) expressed as a product of the assets' confidentiality, integrity, and availability criteria.

4.6 Establish the Risk Criteria

Risk criteria provide a reference against which the significance of a risks are evaluated. These are developed consistent with the organization's risk frame (context), and derived from standards, contractual, legal and regulatory requirements that are applicable to the organization's activities, and/or policies and other sources. In short, the risk criteria are defined having considered a variety of factors, including: *(a)* the nature and types of causes and consequences that can occur and how they will be measured, *(b)* the method through which likelihood of occurrence will be determined, *(c)* the timeframe(s) of the likelihood and/or consequence(s), *(d)* the means through which the level of risk will be determined, *(e)* stakeholder input, *(f)* the level at which risk becomes acceptable or tolerable, and *(g)* whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered (International Organization for Standardization, 2018a).

4.7 Risk Assessment

Prior to commencing the risk assessment, the ISC will need to make use of the asset register and identify and 'map' the organization's process flows, placing emphases on the input-out relations that link the processes together to form a coherent, integrated value stream. The process map should capture the sum of the organization's core processes that are directly associated with actual production and/or service provision results, and the enabling processes that are essential for the achievement of results, which do not, however, necessarily translate directly into products and/or services. Moreover, the process map should reflect information flows and timelines associated the work activities that are carried out, both within and among the organization's different processes, at each recursion level. Thus, the process mapping activity should begin at an organization-wide level, and be repeated incrementally to include the higher resolution layers (lower recursion levels) that are associated with each sub system connected with the organization's structure. Finally, the active entities (decision-makers or agents) need to be identified within each layer, and the overall risks that emerges as a result of their actions and interactions documented and understood.

The explicit objective of the risk assessment stage is to identify: *(a)* sources of risk to the organization's operations, assets, and/or its stakeholders (including those risks associated with not pursuing an opportunity) and sources of risk directed through the organization against others (e.g., clients), *(b)* their root causes (vulnerabilities internal and external to the organization) and their potential consequences, and *(c)* the likelihood that harm will occur given the potential that a threat exploits a vulnerability. In short, through the risk assessment, the ISC should generate a comprehensive list of IS risks (including risks that originate from activities that are not under the direct control of the organization) that is based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of the organization's objectives.

4.8 Evaluate the Risk Level

Levels of risk are typically expressed in terms of the combination of consequences and their likelihood. The purpose of the evaluation is to consider the risk causes and sources, their consequences (positive or negative) and the likelihood of their occurrence. This will assist the ISC in selecting treatment options that are proportional to the risks identified and to prioritize these risk treatments. Each level of risk should be compared with the risk criteria. Decisions made should reflect all contractual, legal, and regulatory requirements that are applicable to the organization and the ISMS.

4.9 Select Treatment Options

Risk treatments should turn uncertainty to the organization's benefit, by restraining threats and taking advantage of opportunities. The ISC should select risk treatment options based on the expected cost of implementation balanced against the anticipated benefits that are sought. Once implemented, treatments should provide or modify controls within the organization's acceptable level of risk exposure. Therefore, decisions relating to risk treatment options should reflect the organization's external and internal context, and be aligned with the organization's strategic, tactical, and operational criteria.

4.10 Determine / Modify IS Controls

The internal and external forces that compose the organization's context may necessitate controls that impact specific information resources within a single operation and level, and/or multi-dimensional controls impacting multiple operations and levels, or the organization as a whole. As previously noted, a control is a measure that modifies a risk that is associated with one or more information resources. Controls vary in nature, and may include administrative processes (e.g., policies, procedures, instruction, and/or guidelines), technical or logical methods (e.g., monitoring software, encryption, network firewalls, passwords), and/or physical measures (e.g., locked doors, file cabinets, cable locks, air conditioners, alarms, access control). In this respect, the organization must strive to achieve a balance between the cost of the controls implemented and the overall value of the information resources that the

controls are intended to protect (International Organization for Standardization, 2013b). Control areas that are specified by the ISO/IEC 27001international standard are outlined in table 1.

Table 1: Control areas that are specified by the ISO/IEC 27001international standard. Source: International organization for standardization (2013a)

Control	Description
Information Security Policies	Provide direction and support for IS in accordance with business requirements and relevant laws and regulations
Organization of IS	Provide sufficient staff, clear roles, responsibilities (segregation of duties), reporting lines, security of teleworking and use of mobile devices
Human resource security	Ensure human resource security, prior, during, and on termination of employment
Asset management	Assure responsibility for assets, information classification, and media handling
Access control	Establish business requirements for access control, user access management, user responsibilities, system and application access control
Cryptographic controls	Ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information
Physical and environmental security	Ensure a safe site, restricted to authorized individuals. Prevent: loss, damage, theft, and/or compromise of assets, and interruption to the organization's operations
Operational security	Establish procedures and responsibilities, protection from malware, data back-up, logging and monitoring, control of operational software, technical vulnerability management, Information systems audit considerations
Communications security	Ensure network security management, information transfer
System acquisition, development & maintenance	Ensure the implementation of security requirements of information systems, security in development and support processes, test data
Supplier relationships	Ensure IS and supplier service delivery management
IS incident management	Ensure effective management of IS incidents and improvements
Business continuity management	Ensure that IS continuity is embedded in the organization's business continuity management systems
Compliance	Ensure compliance with all legal and contractual requirements and IS reviews

4.11 Evaluate Performance

Evaluating performance relates to the structured evaluation of the extent to which the controls implemented have achieved their intended change outcome. A *change outcome* refers to the actual change realized as a result of the control's deployment. In this context, *evaluation* is a broadly used term that covers the entire range of activities designed to verify the tangible results achieved, *and* that the results achieved reflect the intended outcome(s) of the controls implemented. In other words, an important aspect of the evaluation process involves an attempt to explain whether the control is the reason why the change occurred. While the traditional approach to evaluating change outcomes focuses on linear causation, a systems approach concentrates on understanding the *emerging* effects that go beyond the operational boundaries of the isolated assets, structures, processes, and/or work activities that were targeted for treatment. Thus, the ISC needs to evaluate performance metrics regarding the effectiveness of the IS policies, processes, procedures, and functions that protect the organization's information resources, and review trends relating to ISMS's overall performance. (International Organization for Standardization, 2016). The methods and techniques used to evaluate performance should consider what needs to be monitored and measured, how to ensure result accuracy, and the time-frames involved.

4.12 Formulate the Risk Treatment Plan

The objective of the risk treatment plan is to modify risk, which can involve *(a)* avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; *(b)* taking or increasing risk in order to pursue an opportunity; *(c)* removing the risk source; *(d)* changing the likelihood; *(e)* changing

the consequences; *(f)* sharing the risk with another party or parties (including contracts and risk financing); *(g)* retaining the risk by informed choice; or *(h)* any combination of the above (International Organization for Standardization 2018a). The risk treatment plan should define cross-functional responsibilities that create accountabilities relating to the full range of activities that are associated with its implementation. Overall timelines, deliverables, and acceptance criteria need to be specified in relation to each activity, in the context of the budgetary constraints that are established and agreed. Moreover, the risk treatment plan should identify the internal and external stakeholders that are associated with each risk treatment and provide a coherent strategy that mitigates the actual and/or potential barriers to the plan's effective execution. Finally, the risk treatment plan should include the specific outcomes that are sought, the tactical and operational actions through which the outcomes will be achieved, and the means through which to correct deficiencies.

4.13 Implement the Risk Treatment Plan

The success of the ISMS will depend on the effectiveness of the risk treatment plan to balance the necessary controls that assure consistency of purpose in relation to IS, with the required operational elasticity that will allow the affected operations to respond in a manner that is aligned with their individual circumstances, and their respective operational capability. Newly designed or changed processes will require a variety of new skills, knowledge, information processing arrangements, and interactions, reflecting the operational diversity of the operations involved. The organization's staff may not be accustomed to ongoing measurement or performance monitoring, and may perceive such activities as a threat to their existing roles and positions. Prior initiatives that failed to deliver stated objectives can fuel skepticism and distrust. Finally, key ideas may be misinterpreted or lost because they are foreign to (or conflicting with) the organization's culture, and ultimately, succumb to pressures to conform to past behavior(s). Thus, during the implementation phase, a lateral communication network should be established, that enables the various operations to harmonize and coordinate their activities, ensuring that actions taken are not mutually inhibitory (Varsos & Assimakopoulos, 2018). In this context, the knowledge that is generated through incidents, failures, near misses, and successes needs to be captured, preserved, and shared through appropriate education and training programs and adequate plan revisions.

5. CONCLUSIONS AND FUTURE RESEARCH

The ISO/IEC 27000-series of international standards provides organizations with requirements and guidance relative to identifying, managing, and mitigating the risks that are associated with their information resources, with the ultimate goal of ensuring IS and business continuity. In addition to providing IS, a well-structured ISMS is instrumental in augmenting the organization's reputation, which translates to tangible business results. We presented a conceptual structure that can used for the purpose of designing, implementing, maintaining, and continually improving an ISMS. We have argued that an effective system exists when individual elements interact in such a manner that their input-output relationships constitute the operational utility of the unified whole. We have further argued that it is imperative for decision makers (on every organizational level) to be mindful of the type of responses that emerge from feedback mechanisms, which operate to achieve equilibrium following risk treatment. The implication here is that to introduce a risk treatment that modifies an isolated part while ignoring the structural and behavioral relationships that exist between the parts, only serves to preserve the very condition that will undermine the objective of the treatment. We will present a quantitative monitoring scheme that constitutes a comprehensive system of 'risk metrics' in a future publication. This scheme transcends conventions that rest on unidirectional cause-effect assumptions, focusing on the network of feedback structures that contribute to collective results, accommodating for possible time-lags.

REFERENCES

Ackoff, R.L. (1971). "Towards a system of systems concepts". *Management Science*, 17(11): 661-671.

Ackoff, R.L. (1974). *Redesigning the Future: A Systems Approach to Societal Problems*. John Wiley & Sons, New York.

Ackoff, R.L. (1999). *Recreating the Corporation: A Design of Organizations for the 21st Century*. Oxford University Press, New York, NY.

Assimakopoulos, N.A., & Varsos, D.S. (2015). "A methodological systemic scheme using causal loops for the design and control of organizational change (DCSYM-2)". *Int. J. of Applied Systemic Studies*, 6(1): 1-25.

Flood, R.L. & Carson E.R. (1988). *Dealing with complexity: an introduction to the theory and application of systems science*. Plenum Press, New York.

Forrester, J.W. (1968). *Principles of Systems.* Productivity Press, Cambridge, MA.

Information. (n.d.). In Business Dictionary web. Retrieved September 12, 2018, from http://www.businessdictionary.com/definition/information.html

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (2018a). *ISO 31000:2018: Risk management – Guidelines.* Geneva, Switzerland.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (2018b). *ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary.* Geneva, Switzerland.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (2018c). *ISO/IEC 27005:2018: Information technology - Security techniques - Information security risk management.* Geneva, Switzerland.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (2017). *ISO/IEC 27003:2017 - Information technology - Security techniques - Information security management systems - Guidance.* Geneva, Switzerland.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (2016). *ISO/IEC 27004:2016: Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation.* Geneva, Switzerland.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (2013a). *ISO/IEC 27001:2013 - Information technology - Security Techniques - Information security management systems - Requirements.* Geneva, Switzerland.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (2013b). *ISO/IEC 27002:2013 – Information technology - Security techniques - Code of practice for information security controls.* Geneva, Switzerland.

Varsos, D.S., & Assimakopoulos, N.A. (2016). "A systems approach to alternative paradigms for organization and organizational change". *Int. J. of Applied Systemic Studies*, 6(4): 302-326.

Varsos, D. S., & Assimakopoulos, N. A. (2018). "Viability and change in the 21st century organization: a cybernetic perspective". *Int. J. of Applied Systemic Studies*, 8(2): 119-150.

von Bertalanffy, L. (1950). "An outline of general system theory". *The British Journal for the Philosophy of Science*, August, 1(2): 134-165. Wiley & Sons, New York.