Advisera

Integration of Information Security, IT and Corporate Governance

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

WHITE PAPER

February 11, 2016

Introduction

When we talk about corporate governance, we are talking about a set of practices to help build an environment of trust, transparency, and accountability necessary for fostering long-term investment, financial stability, and business integrity. This supports stronger continuity and sustainability for an organization and its products and services.

Today's environment is increasingly connected and dependent on information processing speed, which adds a new threat and risk landscape. In order to maintain an effective relevance, it is essential that corporate governance practices are adapted to deal more directly with assets such as information, and the information technologies they depend on.

The purpose of this white paper is to present how the principles and models of corporate governance can be applied to information security and information technology governance, and how these two aspects of governance can be integrated, considering some standards and frameworks already available on the market.

This integration, both horizontal and vertical, can prove to be very valuable through ensuring a proper top-down development and control of the organizational objectives and goals that are supported by information security and information technology, as well as the optimization of resources. This increases the chances that the success of information security and information technology can add value to the main organizational objectives.

Why should I care about governance?

Organizations are under constant and strong pressure to achieve results, and managers make their best effort to accomplish those. But sometimes the actions taken and short-term results achieved may not be in the long-term best interest of the organization. When this happens, key organizational assets, like credibility and public image, can be damaged.

To avoid such situations, governance takes its place as a control mechanism to ensure management actions are geared toward stakeholders' best interests.

As R. Ticker once said: "If management is about running the business, governance is about seeing that it is run properly."

Corporate governance principles and models

According to the Organization for Economic Cooperation and Development (OECD), a global forum where governments, businesses, trade unions, and other representatives of civil society work to promote economic growth, prosperity, and sustainable development, there are six principles of corporate governance that symbolize the general rules and regulations by which the financial and non-financial institutions are expected to operate in proper authority. These are as follows:

Right of shareholders: in organizations that have shareholders, e.g., financial institutions, it is essential, even when not mandatory by law, to ensure that management decisions are made on the behalf of shareholders, to preserve their investments and their trust in the organization.

Accountability: when top management, or the board of directors, is held accountable for the organization's results, there is an additional incentive for proper control over the general executives of the entity, strengthening the preservation of the interests of shareholders and stakeholders.

Responsibilities of the board: clearly defined responsibilities make it easier for the board to focus on what is expected from them, and the definition and acquisition of skills and knowledge needed to maintain leadership over the management body.

Alliance and ethics: ethical standards should be established and enforced to avoid biased and/or unethical choices and decisions, because even if they can bring short-term benefits, the long-term negative impacts and conflicts can bring serious problems for the members of the board.

Rights of other stakeholders: workers, suppliers, distributors, regulators, and customers also have some rights through the organization, which should be preserved and respected to increase the chances of fulfilling organizational objectives both in the short and long term.

Transparency: the disclosure of relevant information and clarification of responsibilities to interested parties is a great trust transmitter of an organization, improving its good image with stakeholders.

By following these principles, an organization has a better chance to build strong relationships between its various departments and external parties, and with that achieve its planned results.

To fulfill these principles, some models are available that consider orientation and organizational structure.

In terms of orientation:

- Market-oriented corporate governance: emphasizes the interests of shareholders.
- Network-oriented corporate governance: includes the interests of other parties, like workers, managers, suppliers, customers, and the community.

In terms of organizational structure:

- One-tier system: the management is assigned to a single board, and among its members a control committee is appointed.
- Two-tier system: the administration is divided into two different bodies, the management body and the supervisory board.

Because the implementation of corporate governance greatly depends on the reality in which an organization performs its activities, there is no general model agreed upon for corporate governance processes beyond the presented principles and models.

However, as we look deeper into the internal process of organizations, we can perceive certain processes, procedures, and activities that recur (e.g., HR, acquisition, etc.) that can be met by common governance practices, such as information security governance and federal law that governs information technology.

For example, the Sarbanes-Oxley Act (SOX) is a United States law that seeks to strengthen the confidence of investors in organizations that must report to the Securities and Exchange Commission (SEC). One of its issues deals with the strengthening of corporate governance, which unfolds in information integrity protection (an information security governance domain), and effectiveness of implemented internal controls (some of which are in the information technology governance domain, like controlled changes, backup, access control, etc.).

Governance of information technology and information security

In an Internet search you can find a lot of definitions for information security governance and information technology governance, but all can be related to the proper use and control of resources to achieve proposed results – in these cases, the protection of information and the provision of IT services.

Although the information security and information technology governance can be treated and developed as separate aspects (you can find a lot of frameworks, standards, and independent literature available), they naturally have many common aspects with corporate governance, only applied in more specific scenarios.

In the following tables you will see comparative information of the corporate governance aspects already presented against two ISO standards:

- ISO/IEC 38500:2015 - Information technology — Governance of IT for the organization, which provides principles, definitions, and a model for governing bodies to use when evaluating, directing, and monitoring the use of information technology (IT) in their organizations.
- ISO/IEC 27014:2013 - Information technology — Security techniques — Governance of information security, which provides guidance on concepts and principles for the governance of information security, by which organizations can evaluate, direct, monitor, and communicate the information security-related activities within the organization.

These standards will be used in the next section, when we will explain the integration of governance of information security and information technology.

For complementary information, you can read this short article: IT Governance – the basics.

In Figure 01 you can see the broader objectives of corporate governance in comparison with the specificities of information security governance and information technology governance objectives.

Figure 01 - Comparisons between governance objectives

Corporate Governance (OECD)	Information Security Governance (ISO 27014:2013)	Information Technology Governance (ISO 38500:2008)
• Long-term investment • Financial stability • Business integrity • Organizational continuity and sustainability	• Provide alignment between information security objectives and strategies and business objectives and strategies • Add value to the board of directors and interested parties • Ensure that information risks are being properly treated	• Balance risks and encourage opportunities arising from the use of IT • Mitigate the risk of directors not fulfilling their obligations • Ensure the conformance with obligations concerning the acceptable use of IT • Ensure that IT use contributes positively to the performance of the organization

Obs.: The order in which the objectives are presented does not mean that there is a specific or stronger link between certain objectives. As sub-sets of corporate governance, the objectives of information security governance and information technology governance are related to all objectives of corporate governance.

In Figure 02 you can see the that principles of corporate governance are more people-oriented (what is expected from management on behalf of the interested parties), in comparison with the principles of information security governance and information technology governance, which are more organization-oriented (what it should do to enforce corporate governance principles).

Figure 02 - Comparisons between governance principles		
Corporate Governance (OECD)	**Information Security Governance (ISO 27014:2013)**	**Information Technology Governance (ISO 38500:2008)**
• Rights of shareholders • Accountability • Responsibilities of the board • Alliance and ethics • Rights of other stakeholders • Transparency	• Establish organization-wide information security • Adopt a risk-based approach • Set the direction of investment decisions • Ensure conformance with internal and external requirements • Foster a security-positive environment • Review performance in relation to business outcomes	• Strategy to attend to actual and ongoing IT business needs • Acquisition made for valid reasons and proper analysis and transparent decision making • Responsibility for supply of and demand for IT • Conformance with all mandatory legislation and regulations • Performance of services according to service levels and service quality required by the business • Human behavior respected in policies, practices, and decisions

Obs.: The order in which the principles are presented does not mean that there is a specific or stronger link between certain principles.

In Table 01, you can see the adoption by the standards of a more complex governance model, the two-tier system, as a way to increase the reliability of the governance process by segregation of functions. With proper authorities and responsibilities defined, the one-tier model can work with the same reliability, too. The size of the management body in the organization is the main factor to define which model to adopt.

Table 01 - Comparisons between governance models		
Corporate Governance (OECD)	**Information Security Governance (ISO 27014:2013)**	**Information Technology Governance (ISO 38500:2008)**
One-tier system (single board with appointed control committee)	-	-
Two-tier system (management body and supervisory board)	Two-tier system (executive management and governing body)	Two-tier system (management body and board of directors)

In Table 02 it is easy to see that in terms of processes to be performed, there are many similarities, considering the processes defined by ISO standards 38500 and 27014:

Table 02 - Comparisons between governance processes	
Information Security Governance (ISO 27014:2013)	**Information Technology Governance (ISO 38500:2008)**
Evaluate achievement of security objectives and determine adjustments	Evaluate the use of IT, including strategies, proposals, and supply arrangements
Direct security objectives, strategies, resources, prioritizations, and approvals	Direct preparation and implementation of plans and policies, including transition of projects to operational status, and submission of proposals for approval to address identified needs
Monitor the achievement of strategic objectives	Monitor the performance of IT, and its compliance with external obligations and internal work practices
Communicate information security to governing body and stakeholders	Although there isn't an explicit communication process in ISO 38500 IT governance, there are aspects related to the responsibility of directors that require managers to provide timely information

Assure by independent and objective audits, reviews, and certifications the validity of objectives and actions related to information security governance and operations	-

Integration of information security governance and information technology governance

Thanks to the similarities previously presented, integrating the governance of information security and information technology is not only possible, but very desirable, as a way to optimize resources, align efforts, and facilitate communication.

Another reason you should consider to encourage integration is the fact that a significant part of the security measures to protect information and services today requires the use of information technology (e.g., VPN, backup, cryptography, etc.).

But, how do you proceed with integration? The recommended approach is doing it through a project management methodology, given its characteristics of result uniqueness (you won't be implementing such integration often) and limitation in terms of resources and time (the smaller the spending the better). Agile, PRINCE 2 and Waterfall are examples of methodologies that can be applied. Of course, if your organization already has its own methodology, this can also be evaluated as a possible choice.

However, regardless of the chosen methodology, some items required will be common to them:

1. Identification of and buy-in from stakeholders

To increase the chances of success, the person (e.g., a senior executive or any organization employee) with the vision of an integrated governance of information security and information technology must have in mind from the beginning the entities who may affect, or be affected by, the integrated governance, in a positive or negative way, and how these effects occur. These entities are called "interested parties." By the nature of governance, some of these are the top management, middle management, investors, and owners (others can exist, both people and organizations, according to the type of organization).

By knowing who these interested parties are, this person can have a perception of how this integration proposal has to be presented in order to gain their buy-in for project execution. A well-designed **business case** will reinforce positive expectations (e.g., raising investors' interest and reducing legal risk), minimize fears and uncertainties (e.g., increased costs and bureaucracy), and document objectives to be achieved (e.g., which parts are to be integrated). See this article: "ITIL Business Case – How to justify the implementation of the IT service" for more details about developing a business case.

2. Definition of the sponsor and project manager

The sponsor is a senior executive who has great interest in the success of the project and has enough power, authority, and influence to overcome obstacles in the path of the project that cannot be solved by the project manager. If this integrated governance vision is a top-down initiative (e.g., started by the CEO or board of

directors), you won't have much problem choosing a sponsor. If it is not, the business case used to obtain the stakeholders' buy-in can help the CEO or board of directors to choose one.

As for the project manager, this person should be carefully chosen by top management or the sponsor, considering knowledge, technical and interpersonal skills, and experience. The project manager is the one who will be responsible for the main planning and controlling of the activities and resources needed for the success of the governance integration project.

To learn more about the selection of a project manager, please see these articles: Who should be your project manager for ISO 27001/ISO 22301? and How to choose a project manager for your ISO 9001:2015 implementation.

3. Assessment of current governance situation

Once the idea of the integration of information security and information technology governance has been sold to the top management and main interested parties, and the sponsor and project manager have been chosen, the task of the project manager is to identify the organization's current governance situation. Using this information, the project manager can validate whether the proposed integration objectives are achievable and determine the effort and resources required.

This assessment can be tricky, because an organization may have a heterogeneous governance environment (remember that we are talking about the central corporate governance and its sub-sets information security governance and information technology governance), where different governance models are being used and each one may be at a different level of maturity in terms of its processes.

To help you with this assessment, you can use Figures 01 and 02, as well as Tables 01 and 02, of this white paper as basic checklists.

Organizations that already have implemented information security and information technology management, especially in compliance with the ISO 27001 and ISO 20000 standards respectively, will find it easier to perform this assessment, by using use these gap analysis tools provided by Advisera:

- ITIL Gap Analysis Tool
- ISO 20000 Gap Analysis Tool
- ISO 27001 Gap Analysis Tool

If your organization does not have information security and/or information technology management implemented, or any previous knowledge at all, you can access this material to learn more:

- What is ISO 27001?
- ISO 27001 implementation checklist
- Diagram of ISO 27001:2013 Implementation
- ISO 27001:2013 Foundations Course
- What is ISO 20000?
- ISO 20000 implementation diagram

From the reading material, you can reach one of these two conclusions:

- My organization already has information security and information technology practices implemented that allow the integration of governance practices. In this case, you can proceed with the assessment.
- My organization does not have information security and information technology practices implemented that allow the integration of governance practices. If this is your case, the recommendation is to take a step back and prepare the field with the minimal practices required, so your organization won't suffer trying to implement practices without the proper environment or maturity.

If you do decide to proceed with the assessment, and use the gap analysis tools to perform it, the main results you should look for are:

Table 03 – Aspects for governance processes integration

Information Security Governance	Information Technology Governance	ISO 27001 clause	ISO 20000 clause	ITIL
Evaluate	Evaluate	4.1 – Understanding the organization and its context	7.1 – Business relationship management	Service portfolio management
		4.2 – Understanding the needs and expectations of interested parties		
		9.3 – Management review	4.5.4.3 – Management review	
Direct	Direct	6.1 – Actions to address risks and opportunities	4.5.2 j – approach to risk management and risk acceptance criteria	Service portfolio management Release and deployment management
			4.5.3 d – services risks identification, evaluation and management	
			6.6.1 c – approach to information security risk management and risk acceptance criteria	
		6.2 – Information security objectives and planning to achieve them	6.6.1 b – information security management objectives	
Monitor	Monitor	9.1 – Monitoring, measurement, analysis and evaluation	4.5.4.2 – Internal audit 6.2 - Service reporting	Service level management Availability management
Communicate	-	7.4 – Communication	-	-
Assure	-	9.2 – Internal audit	4.5.4.2 – Internal audit-	-

For assessment of a process maturity, you can find more detailed information in this article: Achieving continual improvement through the use of maturity models.

4. Adjustment of governance elements

Once your assessment is complete, you should have a view of what needs to be changed/adapted so you can use the governance processes in an integrated way. The elements you should consider, as well the changes/adjustments to be made, are:

Governance model: If possible, try to use the same model for all of them (e.g., all one-tier or all two-tier). If it is not possible, make sure to establish a proper integration in the item "roles and responsibilities" (examples are presented later in this paper).

Processes and guidelines: If your organization already has processes in use, or at least follows a set of guidelines (documented or not), try to unify as many processes as possible. Document them and make the singularities of each one being documented a specific operational procedure. If your organization does not have processes or guidelines in use, you may consider the processes and guidelines defined by ISO 27014 and ISO 38500 (see Table 04) to set all your governance environments (corporate, information security, and information technology). Because the processes and guidelines in the standards are very similar, it will make the integration effort easier (see examples of documentation at the end of the paper).

Roles and responsibilities: The establishment of a proposal for roles and responsibilities is quite easy for governance processes following ISO standards:

Table 04 – Governance roles and responsibilities integration

Process	Roles	Responsibilities	Rationale
Evaluate	CEO / Board of directors	Evaluate the achievement of security and IT objectives, including the suitability of strategies, the effectiveness of security controls and the use of IT, and the proposals and supply arrangements. Determine adjustments on objectives and/or strategies. Approval of proposals and arrangements that support the business' and interested parties' best interests.	Evaluation is a top management duty, so it must be assigned to the CEO / Board of directors according to the governance model adopted (see Table 01). The integrated responsibilities should cover all those defined in the standards (see Table 02). Applicable to all processes.
Direct	Business unit managers	Direct security / IT objectives, strategies, resources, prioritizations and approvals Direct preparation and implementation of plans and policies, including transition of projects to operational status, and submission of proposals for approval to address identified needs	While CIOs (Chief Information Officers) and CISOs have the duty to make information technology and information security work for the organization, the business managers are those who have to point out the objectives and approve the strategies that will support their operations.

Monitor	CEO / Board of directors	Monitor the achievement of strategic objectives, the performance of IT, and their compliance with external obligations and internal work practices	As guardians of the interested parties' best interests, the CEO / Board of directors should be the ones with the duty to verify and validate the results achieved by the business units.
Communicate	Business unit managers / CIO / CISO / CEO	Communicate information security and information technology to governing body and stakeholders	The responsibilities here must cover multiple points of view to ensure reliable information: corporate view (CEO), business view (unit managers), security view (CISO), and technological view (CIO).
Assure	Audit committee	Assure by independent and objective audits, reviews and certifications the validity of objectives and actions related to information security and information technology governance and operations	Not evaluating one's own work and results is essential to ensure the reliability of the results and proper applications of policies and procedures.

Schedule: Now that you have detailed information about the current situation and the resources and effort required, it is possible to create a schedule defining who will be performing the required tasks and when, and how many resources should be available. In general, these types of tasks are included in a project schedule: elaboration (creation of a deliverable), implementation (deployment to the site of use), validation (verification that the deliverable meets specifications and can deliver the expected results), and training (preparation of personnel to use the deliverable).

Budget: As important as the schedule, a budget must be created so the organization can have control of the project expenditures (how much and when the financial resources will be used). This can prevent the project from coming to a halt because of a lack of money, or from becoming costlier than expected.

For more information about managing a project, try this Free Tutorial: How To Set Up ISO 27001 Project – Writing the Project Plan.

Integrated governance helps cope with complexity

In today's dynamic and complex environments, to fulfill interested parties' best interests, and to demonstrate that fulfillment, requires a precise set of variables to be controlled (e.g., financial, technological, informational, etc.). But, it does not necessarily require different methods. Organizations must achieve an "internal simplification" to remain competitive.

By integrating its governance processes, an organization can create a beneficial cycle where an increase in business integrity and shareholders' and stakeholders' confidence leads to an improvement in its competitive position, ensuring long-term investments and financial stability. This supports business integrity and interested parties' confidence, a recipe for a strong and sustainable organization.

And, this integration task can be made easier by the adoption of standards, already proven practices adopted worldwide, and documentation models, which can help you start adjusting the best practices to your business environment.

Complementary material

As for documentation support, here are some examples of documents available at Advisera:

Information Security / Technology Governance process	Document name
Evaluate	List of Legal, Regulatory, Contractual and Other Requirements List of Services Management Review Minutes
Direct	Risk Assessment and Risk Treatment Methodology
Monitor	Internal Audit Procedure
Communicate	Communication Procedure
Assure	Management Review Minutes

So, with some adjustments, these documents can be used as the basis for an integrated governance of information security and information technology.

References

ADVISERA – 27001Academy (http://advisera.com/27001academy/)

ADVISERA – 20000Academy (http://advisera.com/20000academy/)

OECD (2015), G20/OECD Principles of Corporate Governance, OECD Publishing, Paris. (http://dx.doi.org/10.1787/9789264236882-en)

ISO/IEC 38500:2015 - Information technology — Governance of IT for the organization

ISO/IEC 27014:2013 - Information technology — Security techniques — Governance of information security

Advisera

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

EPPS Services Ltd.
for electronic business and business consulting
Zavizanska 12, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
Phone: +1 (646) 759 9933
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Fax: +385 1 556 0711

EXPLORE THE ACADEMIES

9001 Academy
ISO 9001 Online Consultation Center

14001 Academy
ISO 14001 Online Consultation Center

20000 Academy
ITIL and ISO 20000 Online Consultation Center

18001 Academy
OHSAS 18001 Online Consultation Center