ISACA®
Trust in, and value from, information systems

Internal Control Using COBIT® 5

Abstract

Internal controls are often not well understood in business. They may even be shunned in enterprises that perceive them as onerous rules that exist primarily to make work more difficult or cumbersome. Instead, they should be recognized as the policies, procedures, practices and organizational structures that ensure desirable positive outcomes and mitigate potential negative consequences. In both cases, they contribute to the enterprise's ability to deliver value to stakeholders. Like any significant business element, controls can be complex. There are multiple types of controls addressing a variety of objectives, and numerous standards and frameworks that can be consulted for guidance. Many questions surround internal control, such as who owns it within the business, who are its stakeholders, and what role IT plays. This white paper addresses those questions, and more, and provides a case study illustrating the selection and application of internal controls in an information security environment. Given that internal controls can help the enterprise realize benefits, optimize risk and resources, and minimize disruption, their mastery is a business asset and enabler.

COBIT® 5
AN ISACA® FRAMEWORK

What Is Control?

The concept of control, both in general and in business terms, can sometimes be difficult for practitioners to understand, usually due to inconsistencies in how the term is applied across different industries. This is true within professional discourse (i.e., one practitioner to another), in publications and guidance, and sometimes in a regulatory context. Therefore, when writing a guidance publication about internal control, it is important to be very clear about what is meant by the term—and to differentiate from other very specific usage as appropriate.

Generally, the term "control" refers to guidance, regulation, restraint and oversight. Within a business context, the term (earliest use by assurance and compliance practitioners) usually refers to the mechanisms by which specific business activities are monitored and directed. To operate effectively, any given business unit or area must ensure that it is following the optimal course of action, i.e., the course of action that realizes the most business value, optimizes risk (realizing the most value within a risk that is acceptable to the organization and its stakeholders) and best supports the mission of the organization. This can be challenging because, without a holistic view, the goals of individual business units might be at odds with one another. In the absence of a mechanism for central oversight, decisions made at the individual business-unit level might counteract or adversely impact other areas. This is the essence of internal control: specifically, to provide that oversight and (if done well) the holistic viewpoint.

In this context, internal control is established by providing visibility into what individual operational units are doing. Why are they acting in a certain way? Why do they consider those actions to be most efficient and effective? What measures are they taking to prevent undesired outcomes? While there are many ways to phrase the responses to these—and other—questions, and many subtle nuances can be added along the way, addressing these issues is what internal control is all about.

What Are the Components of Internal Control?

ISACA defines internal controls as the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.[1] In the past, a control was usually understood from a risk management point of view only (e.g., a mechanism to mitigate risk). In fact, some regulatory guidance and even some legislation limit discussion of controls to risk specifically—in some cases, the subset of risk related just to financial reporting (e.g., US Sarbanes-Oxley Act of 2002).

Looking at internal control from the perspective of risk only limits the potential of how organizations might employ the concept. Just as controls can be used to mitigate potential negative consequences (i.e., risk), they can also be used to ensure desirable positive outcomes. In other words, controls can be used to ensure that value is created in the same way that they can work to minimize risk. Therefore, internal controls are those specific structures, tools, processes or other mechanisms that are used to ensure an outcome. Note that this can be applied to any aspect of business activity that ties back to value creation, including benefits realization, risk optimization, resource optimization, disruption minimization, business enablement, and potentially any other element of an organization and its operation.

Enterprises exist to create value for their stakeholders, and internal controls are an integral part of this process.

[1] ISACA Glossary, www.isaca.org/pages/glossary.aspx

ISACA identifies as stakeholders anyone who has a responsibility for, an expectation from or some other interest in the enterprise.[2] This is an intentionally broad definition because an enterprise can be a public corporation, not-for-profit association, government entity or other type of organization. These enterprises have a variety of interested parties and stakeholders. Great care must be exercised when identifying an enterprise's stakeholders because this list will drive all further strategic, risk and internal control activities.

Some examples of stakeholders include boards of directors, who execute and oversee control of an enterprise's operations; internal audit and assurance departments; business process management; IT; and external parties such as auditors, governmental regulators and other supervisory bodies.

Internal Control in COBIT

In COBIT® terms, a control can be any enabler that supports the achievement of one or more objectives (control objectives). These objectives are the desired result or purpose from the implementation of a relevant process, practice, principle, tool, organizational unit, symbol or other capability. A control practice is a key mechanism that supports the achievement of control objectives through responsible use of resources, appropriate management of risk and alignment of IT with business requirements. Control activities are distinct, documented activities dedicated to reduce the risk to the accuracy, completeness, timeliness or consistency in financial reporting and the supporting general controls (primarily access control, change approval and resolution of incidents) of relevant IT systems. As an example, US Generally Accepted Accounting Principles (GAAP) formalizes these requirements by defining five financial statement assertions that must be supported in order for financial statements to be relied on.[3] Control activities are periodically and formally assessed by financial and IT auditors and, taken as a whole, provide the control environment that generates the assurance that enterprise objectives are met and relevant financial statements are reliable.

Control Systems

It is necessary to bring all of the controls and the control activities together into a systematic structure that clearly identifies the risk being managed and the objectives being served. Having such a structure permits identification of gaps in control objective coverage and facilitates internal audit planning that supports the achievement of overall enterprise objectives. This structure is called the internal control environment.

The internal control system is the ecosystem that organizations establish to ensure that enterprise enablers are being used efficiently and effectively.

It is a collection of integrated processes designed to deliver value to stakeholders and provide reasonable assurance regarding the achievement of specified objectives. These objectives include effectiveness; efficiency and economy of operations; reliability of management; and compliance with applicable laws, regulations and internal policies.

This structure can include awareness of specific measures (i.e., individual controls) the organization puts in place to manage and meet specific goals and the value that the organization places on the importance of those measures, as well as the other supporting structures the organization has established to ensure the sufficiency, efficacy and efficiency of those measures. Enterprise leadership must confirm that an effective internal control system is designed and operating and periodic monitoring uncovers any changes necessary to continue this assurance. A well-designed internal control system will ensure that objectives are met efficiently and effectively, resources are used appropriately, legal compliance occurs, and financial information and reporting are reliable and free of material misstatement. The difference between a control and a control activity is that a control is a means to create value or manage risk. Controls are processes, tools, templates, etc., that cannot be audited, whereas a control activity is a distinct activity that can be audited, such as approvals, reviews, etc.

[2] ISACA Glossary, www.isaca.org/pages/glossary.aspx

[3] American Institute of Certified Public Accountants (AICPA), *Statements on Auditing Standards (SAS) No. 106, Audit Evidence,* 2006

Control Practice Areas

The internal control environment permits the operation of various control practice areas such as controlling, risk management, quality management, audit and assurance, and information security. These areas cover functions such as IT, enterprise risk management (ERM) and finance. The practice areas set the tone for the enterprise for effective and efficient internal control. The following sections outline these areas in additional detail.

CONTROLLING

Risk management depends on the appropriate definition of risk, identification of risk elements within the enterprise and decisions as to how those risk elements will be handled. The internal control environment provides the means and processes through which reliable risk information can be developed and monitored. The practice of controlling provides the objectives and benchmarks for comparison and ultimate measurement of performance. Controlling then permits the identification of corrective actions.

RISK MANAGEMENT

Risk is described by the International Organization for Standardization (ISO) in the *ISO Guide 73:2009* as the combination of an event and its consequence.[4] Risk management requires identifying risk, assessing and understanding that risk's potential for business disruption and identifying specific actions that can be used to reduce that risk to acceptable levels. Disruption to business can take many forms; it includes situations that impact the enterprise at a very low level or to a negligible degree and those that impact it at a very high level, possibly threatening the ongoing viability of the enterprise. Risk management must take into account and understand the needs of the enterprise stakeholders, how the enterprise intends to deliver value to those stakeholders, and what actions must be taken for their needs to be met and value to be delivered. Any risk that could potentially prevent those goals from being realized must be recorded and managed as part of ongoing risk management activities.

Part of the risk management process involves determining the priorities of risk and outlining the courses of action that need to take place to avoid the risk, mitigate the risk's impact on the enterprise should it materialize, transfer or share the risk (e.g., insurance), or simply accept the risk. Risk assessment is a subset of a broader risk management process; it includes the activities that determine what risk exists and what impact it could potentially have. This part of the process should inform the enterprise what controls are needed to bring the risk to an acceptable threshold. Each organization should determine its risk appetite, which is the amount of risk, on a broad level, that the organization is willing to accept.

QUALITY MANAGEMENT

The reliability of information is a function of quality management. The internal control environment must be designed such that quality of information is considered and managed to a sufficient degree. Audit and assurance requires reliable risk information to demonstrate that business systems and the information they handle are secure and enterprise assets are appropriately safeguarded. When this is true, the audit function can form a reliable opinion on the state of compliance with legal and operational requirements.

AUDIT AND ASSURANCE

Audit and assurance services provide a level of assurance or comfort that a requirement, either regulatory or contractual, is being met. Enterprises may secure these services from outside assurance professionals or internal staff. The control environment provides the means by which the assurance function can base its reliance on any and all underlying information and systems.

INFORMATION SECURITY

Information security seeks to safeguard the confidentiality, integrity and availability of enterprise systems and data. This protection is accomplished by using an information security management system (ISMS) or information security program to establish, monitor and maintain the technical, procedural and administrative safeguards that support those goals. An ISMS must have reliable data to effect the required control as determined by the enterprise. The section in this publication titled "Control Selection Example: Internal Control for Information Security" gives an illustrative example showing the importance of control in information security and the control selection process.

[4] International Organization for Standardization (ISO), *ISO Guide 73:2009 Risk Management—Vocabulary,* 2009

How COBIT 5 Can Help

COBIT 5 facilitates a systematic approach to establishing a control environment. Further detail on how COSO and COBIT 5 relate is offered in ISACA's publication *Relating the COSO Internal Control—Integrated Framework and COBIT,*[5] which presents the COSO components in framework terms.

The initial step in understanding stakeholder requirements is to go through the COBIT 5 goals cascade, shown in **figure 1**. Based on stakeholder requirements, the cascade will draw out from the enterprise the actions that each level of the enterprise must take to deliver value to the stakeholders. Once complete, the cascade will detail enterprise goals, IT-related goals and enabler goals. Goal setting contributes to the definition of the enterprise internal control environment and assists with future risk assessments and assurance activities. Specifically, by understanding in a systematic way what the goals of the enterprise are, appropriate internal controls—and the supporting internal control environment—can be established.

Figure 1—COBIT 5 Goals Cascade Overview

ADAPTED FROM: ISACA, COBIT® 5, 2012, figure 4

Systems of Internal Control

In the United States, the term "system of internal control" has a very specific and precise meaning for publicly traded organizations, as mandated by the Public Company Accounting Oversight Board (PCAOB). The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines internal control and control systems as the specific measures that provide assurance that an enterprise's operations are effective and efficient, its financial reporting is reliable, and the enterprise is in compliance with all regulatory requirements. COSO describes these objectives further and provides detail on control components (risk assessment, control environment, control activities, information and communication, and monitoring) that are used to accomplish them.[6]

Being aware of the precise usage of the term is important, but it is equally important to note that the term itself can be a valuable concept even when used more generally, especially as it relates to stakeholder requirements and risk assessment. Stakeholder requirements provide the basis for deciding what activities should be pursued. A risk assessment will determine what must happen to deliver value to stakeholders and subsequently details what risk the enterprise faces, i.e., what might jeopardize the objectives of the enterprise. The results obtained from the risk management process enable a comprehensive control environment to be designed. This control environment will define and detail what control activities are required, who owns and operates them, and how issues are managed. The control environment will generate information that will be communicated throughout all pertinent levels of management, and monitoring of these issues will determine what, if any, changes should be made to the control environment. **For tips on using COBIT 5 to build an effective internal control environment, see "How COBIT 5 Can Help."**

[5] ISACA, *Relating the COSO Internal Control—Integrated Framework and COBIT*, USA, 2014, www.isaca.org/COSO-and-COBIT

[6] COSO, *Internal Control—Integrated Framework*, 2013, www.coso.org/IC.htm

Who Owns Internal Control?

Stakeholders delegate their needs to the governing body, who then take ownership of those requirements. The governing body remains accountable, and directs management to plan, build, run and monitor the controls required. Management instructs and aligns operations to execute those controls and report their results. The results are monitored by the governing body, who then reports on their accountability to the stakeholders. This relationship among stakeholders, governing bodies, management and operations is shown in **figure 2.**

Ownership is a multitiered proposition. Several layers within an enterprise have responsibilities within the design and execution of the control environment. COBIT 5 provides a resource to manage this mapping of goals and responsibilities in process RACI charts. RACI charts illustrate, within an organizational framework, who is:

- **Responsible**—Who is getting the task done?
- **Accountable**—Who accounts for the success of the task?
- **Consulted**—Who is providing input?
- **Informed**—Who is receiving information?

RACI charts can assist in the design of the control environment and enable evidence gathering to support goals accomplishment and other assurance reporting needs.

Information Technology in Internal Control

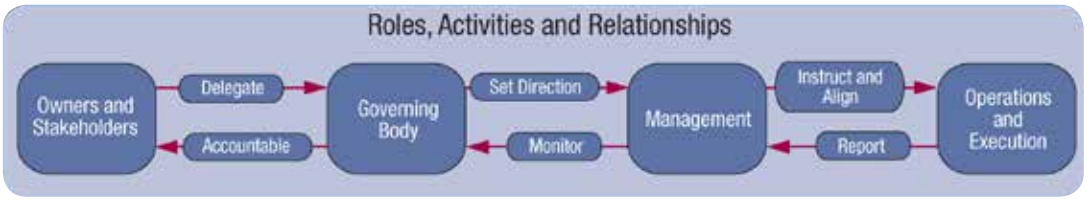
Technology is ubiquitous in enterprises, being used to conduct every imaginable task, from data creation to manufacturing to financial reporting. Technology can also be exploited by internal or external parties to perpetrate a crime against the enterprise. Not only is technology used to effect internal control, it is also the subject of controls and is used in control testing and reporting.

The controls that organizations use to ensure the proper, expected and efficient operation of technology are very often automated. However, they can also be manually executed on an as-needed basis, i.e., manual controls. When to use and perform a manual control is an *ad hoc* or periodic decision. An example of a manual control is the review by a qualified person of a log of all superuser accounts that have accessed a particular server. Manual controls are used in areas where activity is expected to be low and/or automation of that control might be expensive or not feasible.

Another type of technology control is automated controls, which are set up to run without intervention, triggered by either the passage of time or specific events. One example is data analytics, in which insights are extracted from large sets of data generated to report on specific metrics of the enterprise.

Business process controls are also often automated controls. They include controls on the applications themselves, which consist of all relevant systems used within the enterprise. Examples of such systems include general ledger (enterprise resource planning [ERP]), shop floor control (manufacturing resource planning [MRP]) and payroll. ISACA defines such application controls as the policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved.[7] Application controls ensure completeness, validity and accuracy of transactions processed within them.

Figure 2—Key Roles, Activities and Relationships



SOURCE: ISACA, COBIT® 5, 2012, figure 9

[7] ISACA Glossary, www.isaca.org/pages/glossary.aspx

Financial reporting requires the determination of very specific objectives. The PCAOB provides resources on internal control over financial reporting such as:

- Staff Audit Practice Alert No. 11, "Considerations for Audits of Internal Control Over Financial Reporting," http://pcaobus.org/Standards/QandA/10-24-2013_SAPA_11.pdf
- "A Layperson's Guide to Internal Control Over Financial Reporting (ICFR)," http://pcaobus.org/News/Speech/Pages/03312006_GillanCouncilInstitutionalInvestors.aspx

COBIT 5 Enablers for Internal Control

COBIT 5 discusses the enablers available to enterprises to accomplish their goals and deliver value to their stakeholders. Those enablers are:

1. Principles, Policies and Frameworks
2. Processes
3. Organizational Structures
4. Culture, Ethics and Behavior
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies

Principles, policies and frameworks should include policies that inform employees what is expected of them and offer guidance on actions to take if they become aware of a control deficiency or fraudulent act. These policies should address information protection, a code of conduct and whistleblower processes. While policies such as these may be fairly generic, other policies are likely to be quite specific to the enterprise.

When appropriate principles, policies and frameworks are in place, internal control is made a part of the fabric of the enterprise and controls become embedded in daily operations.

A great deal of focus is placed on processes within internal control, and rightly so. Most business operations are communicated in terms of processes, and it is through these processes that operations are conducted and controlled. ISACA defines processes as a collection of activities influenced by the enterprise's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs and produces outputs.[8] In fact, internal control itself is a process.

The process reference model in the ISACA publication *COBIT® 5: Enabling Processes* provides two processes that can be used in the definition and execution of a control environment: MEA01 *Monitor, evaluate and assess performance and conformance* and MEA02 *Monitor, evaluate and assess the system of internal control.* These processes detail the relevant practices and their related inputs, outputs and activities to design an effective system of monitoring the internal control environment. Without effective monitoring, the enterprise might not have timely notice of problems with the design and operating effectiveness of the internal control environment. The publication also includes RACI charts for each process. These charts can be used to link accountabilities within processes to internal controls. For example, the RACI chart for the MEA02 process is shown in **figure 3.**

If an employee becomes aware of an issue with internal controls, the culture, ethics and behavior of the organization influence the employee's reaction. An organization with a culture that is transparent about its needs and expectations and an ethical tone created by the governing body can encourage communication and facilitate the easy and quick resolution of issues. The ability of an enterprise to create a culture of transparency can be influenced by its size, history, national area of primary operation and hierarchy.

Organizational structures are used to create arrangements of resources in such a manner that the accomplishment of specific goals is facilitated. The alignment of resources can, therefore, be manipulated to best advantage to provide controls functions and satisfy stakeholder requirements. In larger enterprises there can be many organizational structures. For example, a large automobile manufacturer might produce several brands. Each of these brands will have separate organizational structures dedicated to accomplishing its requirements. At the parent enterprise level, this can result in an amalgamation of structures that might not easily satisfy higher-level needs while still accomplishing what was needed within the division itself.

ISACA defines information as an asset that, like other important business assets, is essential to an enterprise's business. It can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by

[8] ISACA Glossary, *www.isaca.org/pages/glossary.aspx*

Figure 3—RACI Chart for MEA02 *Monitor, evaluate and assess the system of internal control*

MEA02 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
MEA02.01 Monitor internal controls.		I	C	I	C	R			R		R					R	R	A	I	R	R	R	R	R	R	R
MEA02.02 Review business process controls effectiveness.	I	I	R	I	A	R	I				I	I				R	R	C			C		C	C	C	
MEA02.03 Perform control self-assessments.		I	C	I	C	R			R		R					R	R	A	I	R	R	R	R	R	R	R
MEA02.04 Identify and report control deficiencies.		I	C	I	C	R			R		I	I				R	R	A	I	R	R	R	R	R	R	R
MEA02.05 Ensure that assurance providers are independent and qualified.						R										A	A	R								
MEA02.06 Plan assurance initiatives.		A			C	R			C							C	C	R	C	C	C	C	C	C	C	C
MEA02.07 Scope assurance initiatives.				R	R	R			C							C	A	R	C	C	C	C	C	C	C	C
MEA02.08 Execute assurance initiatives.	I	I			C	R			C		I	I				C	A	R	C	C	C	C	C	C	C	C

SOURCE: ISACA, *COBIT® 5: Enabling Processes*, 2012, page 208

post or electronic means, shown on films, or spoken in conversation.[9] In general, information is data made relevant to the user. This necessarily includes all documentation related to internal control. How these data and reports are stored and transmitted can influence reliability. If it is possible for an unauthorized user to gain access to compliance reports and alter them, then the enterprise may face regulatory sanctions. Information is key to internal control and must be safeguarded accordingly.

The Services, Infrastructure and Applications enabler is made up of all of the relevant enterprise technology assets. The internal control process could be based, or housed, within a specialized application. The architecture surrounding that application will create security and risk concerns that must be managed if reliable internal control reporting can be expected. Advanced auditing tools and governance, risk and compliance (GRC) solutions also reside within enterprise architecture, giving further evidence to the importance of designing appropriate internal controls around architecture and its security.

The People, Skills and Competencies enabler includes specifying the skills needed not only to perform basic job tasks but also to adequately conduct risk activities and interpret risk and control information. All employees have responsibility for safeguarding enterprise assets and, therefore, they must have the awareness and skills to appropriately respond to incidents as they arise. Pertinent certifications are a good way for employees to expand and demonstrate their knowledge and skills. For example, ISACA's Certified in Risk and Information Systems

[9] ISACA Glossary, www.isaca.org/pages/glossary.aspx

Control™ (CRISC™) certification provides evidence of training and relevant professional experience in skills that are integral to ERM.

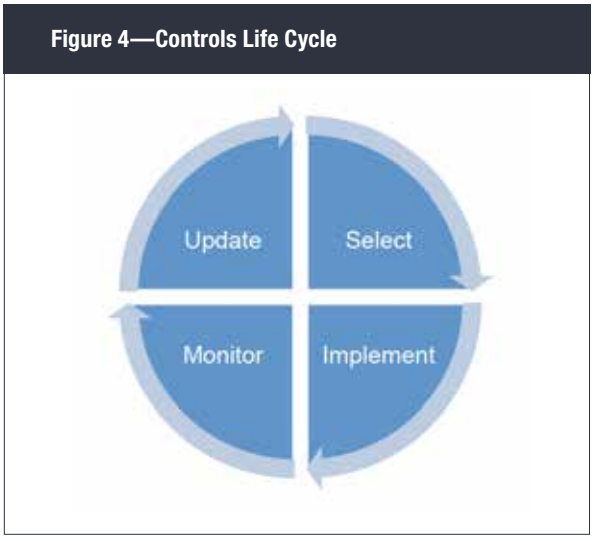
Control Life Cycle

It is important to note that controls, like everything else in business, change over time. Because controls map directly (or, in some cases, indirectly) to business goals, they will, of necessity, change as business goals evolve and change. Likewise, other factors that influence the control landscape change, such as technology, business processes and organizational structures.

As a consequence, controls have a life cycle, as illustrated in **figure 4**, and they require periodic reevaluation to ensure that they continue to meet their original purpose.

Note that this life cycle is roughly analogous to the Shewhart cycle (i.e., Plan, Do, Check, Act such as that found in ISO/International Electrotechnical Commission (IEC) 27001:2013), and it also maps roughly to the phases of the COBIT 5 implementation cycle (shown in figure 17 of the COBIT 5 framework). The similarities show there is a natural process of selecting controls (based on requirements and goals), implementing them, monitoring their effectiveness, and updating (or even removing them) based on changes.

Figure 4—Controls Life Cycle



Control Selection

Practitioners should have an understanding of what internal controls are and the value that they provide before selecting the appropriate controls for their environment. It should be noted that COBIT 5 provides an exhaustive description of this process: how to select the controls that fit within the goals of the organization, how to ensure that the controls tie directly to business objectives and goals, etc. Therefore, for more detailed guidance about control selection, the COBIT 5 framework and other publications, especially *COBIT® 5: Enabling Processes*, might be an ideal place to start and would provide a more thorough reference.

At a high level, the process of control selection consists of three phases:

- **Phase 1: Identify goals**—Determine the end state that should be achieved. Specifically, what is the scope of the control selection? Are controls being selected for risk reduction or compliance, or is there a broader goal?
- **Phase 2: Determine opportunity/risk gaps**—Conduct a gap analysis between the target state and the current state. Keep in mind that no organization works in a vacuum; there are likely dozens (or even hundreds) of controls in use that have been selected over the years for various purposes. Understanding what these are and where they fit into the current plan is important. Note that this might take some investigation internally (such as a discovery activity) to fully understand.
- **Phase 3: Define coverage**—Based on the goals, select the specific controls that address the gaps. Document what the gaps are and identify success criteria, budget, success metrics and other factors that will govern operation.

Control Selection Example: Internal Control for Information Security

This section illustrates the control selection steps in action, using information security as an example of an area in which controls are required and can have tremendous value. It discusses one approach to selecting specific security countermeasures based on materials and concepts covered in this and other ISACA publications.

In the context of this publication, all enablers are also internal controls. The purpose of internal controls is ultimately to safeguard value generation for the organization and optimize risk taken to realize that value. Selection of internal controls can be done systematically with consideration of business value, but internal controls can also form the basis for technical, administrative, procedural, physical or other safeguards, such as those within an information security program, ISMS or other security ecosystem.

USE OF TERMS

There are a number of different terms used to refer to the universe of controls, countermeasures, and management and governance activities used for information security. For example, ISMS and security program might be used interchangeably in the literature in aggregate, even though they each have a precise meaning depending on context and the publication within which each is used.

For the purposes of this section, to reduce confusion and remain consistent with material presented elsewhere in this publication, security control selection activities will be referred to within the context of an internal control system for information security, or ICS-IS. Specifically, the term refers to the selection of countermeasures, tools, activities, processes, enablers and anything else designed to ensure that information security goals such as confidentiality, integrity and availability are met.

STAKEHOLDERS FOR SECURITY CONTROL/ COUNTERMEASURE SELECTION

The primary stakeholders of the ICS-IS are:

- **Board of directors** (executive and nonexecutive), who need to have oversight on the risk exposure and assurance on the adequacy of controls in place
- **Internal and external auditors**, who need to provide assurance on the completeness, effectiveness and efficiency of the controls
- **IT professionals**, who need to design, develop, operate and maintain information systems. Their primary stake is the adequacy and efficiency of the controls in place.
- **End users**, who use information systems and technology. The priority lies in the efficiency of the controls—the seamless integration of mechanisms without any negative impact on the operational processes.
- **Customers**, who rely on the quality of information provided and the protection of their privacy. A complete and effective set of controls needs to be in place.

Other stakeholders (e.g., regulators, suppliers and providers of services, legal or media) are not further elaborated as their stake is highly dependent on the organization's environment.

CONTROL/COUNTERMEASURE SELECTION

There is no shortage of standards, frameworks, regulation, advice, and other recommendations outlining technical, operational and other steps that organizations can consider for protection of digital assets. ISACA's *COBIT® 5 for Information Security*, for example, outlines topical areas and provides guidance, as do ISO/IEC 27002, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, and numerous other publications. Almost universally, this guidance is intended to be customized and adapted to the organization within which it will be used. Control sets are not meant to be "one size fits all" but are instead designed to be tailored to the organization's risk in a particular area, the context in which that operation exists, the risk tolerances of the organization and other factors.

Forethought is required when adapting the extant guidance to the organization. Utilizing the internal control selection concepts and principles outlined in this and other ISACA publications is one way to systematically (with an eye to stakeholder needs and business value) perform that contextualization and adaptation.

THE CONTROL UNIVERSE

The first step in the example control selection process is to define the "universe" of possible areas to evaluate, to establish the topical areas for further discussion and analysis. Guidance such as that described previously is helpful to this process—many of the regulatory guidance documents, frameworks and standards identify core topics that the organization should address from a security point of view.

The list of areas being used must be credible, complete and reputable. For the purposes of this example, the ISACA publication *COBIT® for Information Security*, which contains a topical list of areas aligned to international standards, is used. Note that this is not intended to imply that other guidance cannot be used to create this list; organizations must choose what works for them.

The list of topical areas outlined by the guidance forms the initial universe of areas within which the control selection and documentation occur. This is a starting point only; there will almost certainly be other areas and considerations that will need to be addressed based on environmental factors, industry-specific factors or factors unique to the organization.

These topics contain different types of security capabilities, concerns and areas of focus, which can be used to identify the universe of possible controls that the organization may wish to consider during control selection. This includes: process descriptions, inputs and outputs, and goals and metrics, which provide further guidance and are also considered as potential controls. One such process might involve breaking larger control areas or programmatic goals into smaller, manageable subcontrols. For example, an organization might identify a high-level control area such as "user and system activity monitoring," which might include a wide array of specific ways to accomplish this (e.g., log aggregation, intrusion detection or privileged identity management tools). Therefore, breaking that control area down into the specific parts that will form the basis for selection of individual controls can make the process of control selection much more manageable.

High-level guidance and frameworks (e.g., COBIT, ISO/IEC 27001) define generic high-level practices and capabilities that (to be relevant and useful) need to be adapted to the organization within which those practices and capabilities will be used. Likewise, not all systems and processes will be managed, maintained and supported in a uniform manner throughout the organization. This means that control selection and operation need to be informed by the context within which they will operate. In addition, context should be monitored postimplementation so that the control continues to stay relevant over time. In the internal control for information security example, the following COBIT 5 processes might be implemented:

- EDM03 Ensure Risk Optimization
- APO12 Manage Risk
- APO13 Manage Security
- DSS05 Manage Security Services

ASSIGNING OWNERSHIP

Once high-level goals are broken down into individual components, e.g., vulnerability management (VM), the next step is to find an owner for each. There are different IT environments that have to be taken into account when selecting an owner:

- The "classic" supportive IT environment around ERP and supply chain systems, e.g., the office infrastructure with mail and file services
- Digital media, where the enterprise maintains its digital footprint in the form of web pages, apps and other tools
- Production environment, where goods are actually produced and tested

Each of these sectors has its own culture and regulatory requirements (e.g., financial reporting regulation for an ERP system or industry-specific standards for production, as in health care, the automotive industry or online gaming). In some organizations these areas might overlap (e.g., financial reporting might be combined with production in a financial institution) or other areas might be defined. The most important aspect here is the different ownership because the system operations (and consequently significant parts of VM) are owned by different units. Consequently, these areas are treated separately.

The owner of the ICS-IS identifies, together with the owner of the topic, the key controls for the topic.

In the example of VM for ERP and office environment, the following controls might be included:

- Use current versions of systems and minimize the impact for the end user.
- Per VM, assess the infrastructure on a periodic basis.
- Assess the capabilities of the team in place to test the system on behalf of the end user.
- Configure system to enforce segregation of duties among test, approval and deployment roles and to maintain documentation and traceability.
- Require management reports on the timeliness of patches and their application to the operational environment.
- Assess key performance indicators (KPIs) such as the number of vulnerable systems and the time lapse from identification to confirmation of deployment.

These key controls are documented in a central repository, together with the current and the future status of those controls. Some organizations maintain a long list of controls; some identify the top five only. This, again, needs to be aligned with the corporate culture and the stakeholders' needs. It is the duty of the owners of the ICS-IS and VM to assess the completeness, adequacy, effectiveness and efficiency of the controls and identify areas for improvement when necessary. The guidance contained in COBIT 5 can serve as a valuable input.

If an independent assessment of the controls needs to be obtained (e.g., due to mandatory compliance checks), it is recommended to identify and define relevant control activities. For example, a control activity might be, "An automated check of the system environment is performed on a daily basis and any deviation to the defined baseline (which is drawn from a vulnerability database) is reported to the owner of VM." Also, it is advisable to document the rationale why this activity is considered required (effectiveness), provide evidence on implementing and enforcing the control (e.g., procedures defined or training instructions), and document the execution of control. For some control activities it is also important to closely monitor their operational execution and act on any deviation. Evidence of those monitoring activities should be provided.

For the operation and maintenance of the ICS-IS, there are several activities recommended:

- **Close cooperation with the owners**—This is to ensure the consistency of a virtual team, which will facilitate the ongoing support of the ICS-IS and the currency of owners and their operational duties.
- **Periodic check on the content**—The key controls and the enablers in place permanently evolve and plans for improvement sometimes are optimistic. The list of key controls should reflect reality and highlight the primary means to keep the topic under control.
- **Periodic assessment of the control**—With or without independent resources, such as auditors or assessors, periodic assessment of the control needs to be completed. The frequency of such assessments and the approach are, of course, dependent on the control's nature and its inherent importance, but assurance and reporting requirements mandated by the stakeholders are often key factors in determining when, how often and how assessments are done. Whatever the driver is, assessing the control not only from the perspective of the owner but also from the stakeholders' view is important because the control is ultimately in place to meet their needs.
- **Learning and improvement of the controls should be identified and implementation should be overseen**—A key duty of the ICS-IS owner is not only completing the improvements identified and agreed on with a topic owner, but also providing input and guidance to other owners. Whether the guidance is passed along to the owner of a related topic (e.g., the VM in the production system) or to owners of other topics (e.g., an input to the development environment and project delivery teams to apply proper architecture principles), the important thing is that lessons learned are shared.
- **Monitoring and reporting**—This is another—often time-consuming—accountability of the ICS-IS owner, but it is necessary to ensure that topic owners identify and document the key controls, assess their adequacy on a periodic basis, and define and track KPIs. ICS-IS owners must also assess the balance among preventive, detective and corrective controls; automated and manual controls; deficiencies; improvement pace per topic or organizational unit; and other areas that help to improve the ICS-IS.

Conclusion

Internal controls are the policies, procedures, practices and organizational structures that provide central oversight so that individual business units can work together to follow optimal courses of action to minimize risk and provide value to stakeholders. An internal control system should be designed that includes control practice areas that are integral to the organization's success. This system should identify risk, but it should not be used only as a risk management tool—internal controls can be used to mitigate risk, but they also can be used to create value. Responsibility for internal controls is owned by many different levels in an enterprise. Controls should be selected after identifying goals, determining opportunities/gaps and defining coverage. Tools such as COSO, COBIT 5, and ISO/IEC 27001 can greatly assist in the selection. When a successful internal control system is in place, an organization can gain reasonable assurance that business objectives will be achieved and risk will be prevented or detected and corrected.

ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

This is an educational resource and is not inclusive of all information that may be needed to assure a successful outcome. Readers should apply their own professional judgment to their specific circumstances.

ISACA®
Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: info@isaca.org

Website: www.isaca.org

Provide feedback:
www.isaca.org/internal-controls

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Follow ISACA on Twitter:
www.twitter.com/ISACANews

Join ISACA on LinkedIn:
www.linkd.in/ISACAOfficial

Like ISACA on Facebook:
www.facebook.com/ISACAHQ

ACKNOWLEDGMENTS

Development Team

Jimmy Heschl
CISA, CISM, CGEIT,
Red Bull, Austria

Peter Tessin
CISA, CRISC, CGEIT,
ISACA, USA

Expert Reviewers

Sushil Chatterji
CGEIT,
Edutech Enterprises, Singapore

Nancy A. Cohen
CPA, CIPP/US,
ISACA, USA

Joanne De Vito De Palma
CISM, The Ardent Group, USA

James Doss
CGEIT, ITIL Expert, PMP,
TOGAF 9, EMCCA,
ITvalueQuickStart.com, USA

Ed Moyle
ISACA, USA

Andre Pitkowski
CGEIT, CRISC, APIT
Consultoria De Informatica Ltd., Brazil

Abdul Rafeq
CISA, CGEIT,
WINCER Infotech Limited, India

Paras Shah
CISA, CGEIT, CRISC,
Vital Interacts, Australia

Alok Tuteja
CGEIT, CRISC,
Mazrui Holdings, UAE

Board of Directors

Christos K. Dimitriadis
Ph.D., CISA, CISM, CRISC,
INTRALOT S.A., Greece,
Chair

Rosemary M. Amato
CISA, CMA, CPA,
Deloitte Touche Tohmatsu Ltd.,
The Netherlands, Director

Garry J. Barnes
CISA, CISM, CGEIT, CRISC, MAICD,
Vital Interacts, Australia, Director

Robert A. Clyde
CISM,
Clyde Consulting LLC, USA,
Director

Theresa Grafenstine
CISA, CGEIT, CRISC, CPA,
CIA, CGAP, CGMA,
US House of Representatives,
USA, Director

Leonard Ong
CISA, CISM, CGEIT, CRISC, CPP,
CFE, PMP, CIPM,CIPT, CISSP
ISSMP-ISSAP, CSSLP, CITBCM,
GCIA,GCIH, GSNA, GCFA,
Merck & Co., Singapore, Director

Andre Pitkowski
CGEIT, CRISC, OCTAVE,
CRMA, ISO27kLA, ISO31kLA,
APIT Consultoria de Informatica Ltd.,
Brazil, Director

Eddie Schwartz
CISA, CISM, CISSP-ISSEP, PMP,
WhiteOps, USA, Director

Gregory T. Grocholski
CISA,
SABIC, Saudi Arabia,
Past Chair

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA,
Queensland Government, Australia,
Past Chair

Robert E Stroud
CGEIT, CRISC,
USA, Past Chair

Zubin Chagpar
CISA, CISM, PMP,
Amazon Web Services, UK, Director

Matt Loeb
CGEIT, CAE,
ISACA, USA, Director

Rajaramiyer Venketaramani Raghu
CISA, CRISC,
Versatilist Consulting India, Pvt., Ltd.,
India, Director

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, FACS CP,
BRM Holdich, Australia, Director