Selected COBIT 5 Processes for Essential Enterprise Security

Selected processes from the COBIT® 5 framework can improve the effectiveness of enterprise security in an organization. The objective here is to develop a security strategy with technical processes, controls and tools for security across an enterprise. This is a risk-based strategy to defend critical enterprise resources against a wide range of threats and vulnerabilities.²

The risk component of this strategy includes a coherent, well-thought-out approach to identify, inventory, analyze, manage and respond to key risk factors. Using this risk approach, security efforts can be focused to defend networks, end points and data against malware and other threats.

The assumption here is that much of the IT governance, organization structure, policies and skilled talent are in place.

The threat landscape appears very intimidating at the moment. High-profile organizations including banks, government agencies and retailers are recent victims of exploits and attacks. What is even more intimidating is that these organizations have the resources to defend themselves, yet even they have fallen victim. The security posture of small and mid-sized businesses (SMBs) and other sectors of the global economy appears to be vulnerable.

Threats may include cybercrime (e.g., fraud, theft, destruction of IT resources, blackmail, extortion), social or political hacktivism, or advanced persistent threats (APTs) with national or commercial objectives. Threats may come from foreign governments, organized crime syndicates, hacktivists with an agenda, and employees or consultants from within the organization.

STRATEGY TO IMPROVE SECURITY

What is a smart strategy and what specific steps can be taken to quickly improve enterprise security?

COBIT 5 provides guidance on best practices for enterprise security. Other sources of best practices to consider include: ISO 27001 (information security),³ ISO 27032 (guidelines for cybersecurity),³ the US National Institute of Standards and Technology (NIST) SP 800-53 (recommended security controls),³ NIST Framework for Improving Critical Infrastructure Cybersecurity⁴ and SANS Critical Security Controls⁷ (top 20).

COBIT 5 includes a set of seven enablers for the governance and management of enterprise IT (GEIT), one of which is processes. Of the 37 COBIT 5 processes, this article focuses on three core security processes:

• APO12 Manage risk
• APO13 Manage Security
• DSS05 Manage security services

APO12 MANAGE RISK

This Align, Plan and Organize (APO) process is a prerequisite for any set of security controls and is referenced by virtually every framework or standard on information security. A risk assessment process is essential to identify an organization’s “crown jewels” and to focus resources on the most critical, sensitive, threatened and vulnerable areas.

Specific practices that make up the Manage risk process follow. Data should be collected from all relevant sources (e.g., systems, applications, networks, databases) in multiple categories (e.g., access, configurations) to support the understanding of risk (APO12.01); these data should be considered in the risk analysis, especially for business impact analysis (what is important to the enterprise), estimating the probability of different threats and identifying the mitigating controls in place (APO12.02).

Risk profiles should be maintained on an inventory of business processes and the supporting IT systems, applications, infrastructure, data, facilities and capabilities (APO12.03). This inventory should be used to identify the IT elements/assets that are most critical (highest risk)
and that require the strongest controls. Risk indicators or factors (internal/external) used to maintain this inventory should be reviewed and validated periodically.

Key stakeholders should be kept informed through the articulation of risk status, including worst-case and most-probable scenarios (APO12.04). A risk management action portfolio should be defined and maintained for the control activities to manage, avoid, prevent or transfer (insurance) risk (APO12.05).

Response to risk events should be timely and effective based on formal test plans (APO12.06). Such plans should be prepared, maintained and tested periodically for responding to IT-related incidents that may impact business operations.

**APO13 MANAGE SECURITY**

This APO process consists of defining, operating and monitoring an information security management system (ISMS). This is an essential link to translate the risk process into effective security services. To build this ISMS, risk and security professionals should consider and document risk appetite, security requirements and security solutions.

Specific practices that make up the Manage security process follow. An ISMS (APO13.01) should be established as a standard, formal and continuous approach to IT security. This approach should be aligned with business requirements and business processes.

To formalize this approach, an information security risk treatment plan should be defined based on realistic business cases and implemented as part of strategic objectives and enterprise architecture (APO13.02). The overall ISMS should be monitored and reviewed regularly (APO13.03) through management reviews and security audits. An underlying theme here is a culture of security and continual improvement.

**DSS05 MANAGE SECURITY SERVICES**

This Deliver, Service and Support (DSS) process covers technical security controls to defend the most critical, vulnerable and sensitive resources including information (data), network and communications infrastructure, network end points (e.g., users, PCs), and systems access.

Specific practices that make up the Manage security services process follow. Protection against malware (viruses, worms, spyware, scanning tools, remote access tools) should be implemented through threat (malware) detection systems (e.g., Next Generation firewalls), intrusion detection/prevention systems (IDS/IPS), searchable event (log) repositories (e.g., security information and event management [SIEM] systems), forensic capabilities (tools) and the maintenance of security patches. Malware should be prevented, detected and removed at all layers of the IT environment including applications, operating systems, networks, shared resources (e.g., directories) and hardware (e.g., USB ports) (DSS05.01).

Network security should be actively managed with an integrated strategy and set of tools across network layers and topology (e.g., switch/router access control lists [ACL], firewalls, IDS/IPS). Controls should be deployed at all points of entry including email, web applications, file transfer protocols, social networking, messaging, cloud applications/storage and hardware (USB) ports (DSS05.02).

End-point security (antivirus/antimalware software, web/email security, firewalls) should be deployed and managed to ensure that laptops, desktops, servers and mobile devices are adequately secured (as measured against value of information). High-value targets (e.g., crown jewels) should be protected with stronger security and controls (DSS05.03).

User identity and logical access should be managed on business need-to-know and least-privilege bases. A good practice is to strengthen controls around authentication (i.e., user ID, password) and authorization to sensitive resources. One must ensure that privileged or administrator access (e.g., “keys to the kingdom”) is especially well-controlled and monitored (DSS05.04).

Physical access to IT assets should be managed with procedures to grant, limit and revoke physical access to

---

Enjoying this article?

- Read COBIT 5 for Information Security.  
  www.isaca.org/cobit

- Learn more about, discuss and collaborate on COBIT 5, risk management and cybersecurity in the Knowledge Center.  
  www.isaca.org/knowledgecenter

---
organization sites based on business need. Access should be justified, authorized, logged and monitored (DSS05.05).

Sensitive documents (e.g. special forms, negotiable instruments) should be safeguarded with appropriate controls. Output devices (e.g. security tokens) should also be controlled with an accurate accounting (DSS05.06).

Security monitoring of IT infrastructure is a key component of the control environment. A set of robust controls and tools such as a searchable repository (e.g., SIEM system), centralized and secure log aggregator systems, forensic tools and processes, and malware detection software (event correlation, rule based, pattern recognition) should be considered. Integration with incident management and escalation processes (DSS05.07) should be ensured.

**CONCLUSION**

The three essential COBIT 5 processes for information security—Manage risk (APO12), Manage security (APO13) and Manage security services (DSS05)—offer a risk-based approach to defend enterprise resources against a wide range of threats and vulnerabilities. The risk process is the prerequisite to any security process—first to understand and assess risk before managing and controlling risk. The logical next step is to manage a coherent security program with appropriate controls focused on the highest risk assets and resources.

As the threat landscape gets more complex, these processes represent the critical path toward effective security.

**COBIT® 5 for Information Security**, an extension of the core framework with a focus on information security, includes practical guidance on information security processes in an enterprise environment along with a wealth of supporting detail including service capabilities, policies, principles, security-specific organizational structures, security skills and competencies.

**ENDNOTES**

1 ISACA, COBIT 5, 2012, www.isaca.org/cobit
7 SANS Institute, Critical Security Controls, www.sans.org/critical-security-controls/