# Integrating MITRE With COBIT

## Goals Cascading From the Strategic to Tactical Levels

Protecting enterprises from malicious code and software requires that governance and cybersecurity practitioners take a comprehensive approach. Many people believe that governance, risk and compliance (GRC) is a path to cybersecurity. Others believe that GRC is a part of cybersecurity. However, based on 56 years of scientific research in audit, expertise theory, schema theory, judgment and decision-making (JDM), and human capital theory, it is clear that governance professionals should leverage design factors such as enterprise strategy, enterprise goals, risk profile and current IT issues (pain points) to determine which cybersecurity practices and controls are necessary rather than aligning governance to cybersecurity practices that might not be warranted. In other words, without inherent risk, there is no need for cybersecurity practices, frameworks or tools.

Cybersecurity efforts must be commensurate with an enterprise's risk appetite and tolerance levels. So, the question is, how can a practitioner assess and articulate risk from the board level to the code level using industry models such as the COBIT®[1] and MITRE ATT&CK frameworks?[2]

### Strategies for Addressing Malicious Code From the Strategic Level

Risk must be communicated from the board level in business terms that stress the importance of implementing and maintaining detective, preventive and corrective controls via security baselines (benchmarks), patch management, endpoint detection/response and virus control. To accomplish these aims, GRC professionals need to understand the enterprise's strategy (business plan) and vision and identify which enterprise archetype the business has chosen to adopt. Conducting a risk assessment at the strategic level to evaluate which portfolio items are at the greatest risk helps the assessor understand which governance and management objectives are ideal for reducing risk to acceptable levels. Identifying the organization's current IT issues (pain points) enables GRC professionals to understand which processes and controls can help address conflicts between various IT entities and business departments, and service delivery problems related to IT outsourcing.

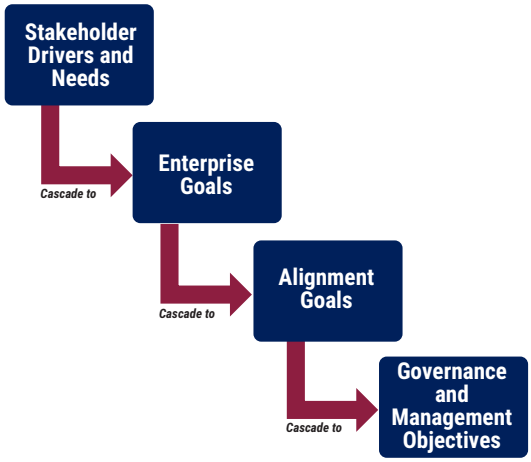
The COBIT goals cascade (**figure 1**) and design factors are helpful in assessing an enterprise's current and future state with respect to reducing

**BLAKE CURTIS** | SC.D, CISA, CRISC, CISM, CGEIT, CDPSE, COBIT 2019 FOUNDATION, DESIGN AND IMPLEMENTATION, CISSP, NIST CSF

Is a cybersecurity governance advisor with more than 13 years of experience in engineering, networking, virtualization and IT service management. He creates global information assurance programs for the government, commercial, international and healthcare sectors. Currently, he assesses various aspects and latitudes of risk and audits information systems to assure compliance with applicable state, federal and regulatory requirements. In addition, he leverages a comprehensive amalgamation of cybersecurity, governance and control frameworks to develop tailored assurance programs for enterprises. Curtis is also a research scientist who specializes in quantitative correlational research, measuring cybersecurity expertise, task performance and technical competency for IT; governance, risk and compliance; and cybersecurity professionals. He also mentors students and advises on strategies to help them earn their master's degree in cybersecurity or pass difficult IT certification exams. He can be reached at *www.linkedin.com/in/reginaldblakecurtis/*.

**FIGURE 1**

## COBIT Goals Cascade

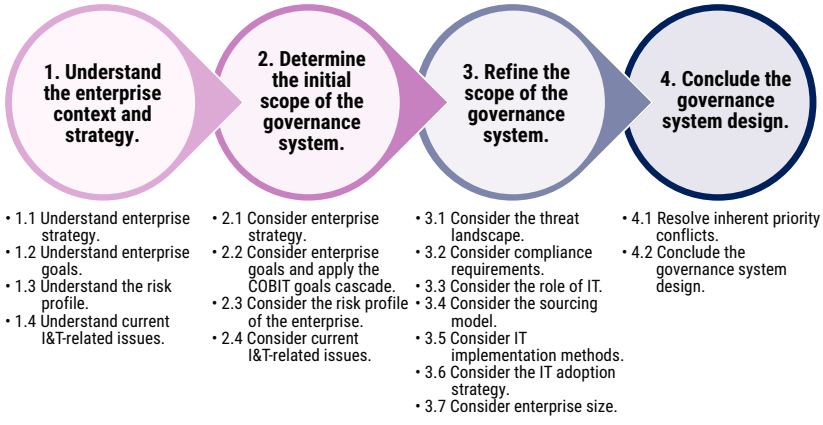



Source: ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, USA, 2018, *https://www.isaca.org/resources/cobit.* Reprinted with permission.

the threat of malicious code and other types of significant risk. For example, the goals cascade enables enterprises to take internal and external stakeholder needs and hierarchically map them to the enterprise's goals and objectives. Subsequently, through strategic alignment and equal representation in both IT and the business, the enterprise can further cascade the enterprise goals into IT alignment goals and governance and management objectives (e.g., COBIT processes and industry framework security controls).

**FIGURE 2**

## Governance System Design Workflow




Source: ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, USA, 2018, *https://www.isaca.org/resources/cobit.* Reprinted with permission.

## Using the Goals Cascade and Design Factors to Identify Cybersecurity Controls

Governance professionals with both declarative knowledge (theoretical) and procedural knowledge (practical) in COBIT understand how to leverage the goals cascade and design factors to identify relevant governance and management objectives and their components. Once the appropriate governance and management objectives are mapped onto the governance design canvas, they should be prioritized, as shown in step 4 of **figure 2**.

In the governance design workflow, the first step is to identify the organization's context, goals, objectives, mission and strategy through intake processes, questionnaires and other types of assessments. Next, the governance practitioner should determine the initial scope of the governance effort by using the goals cascade, conducting risk assessments and identifying common IT pain points. Then, the practitioner should refine the scope of the governance systems by considering other design factors such as the threat landscape, regulatory and contractual obligations, and IT implementation methods (e.g., Agile, DevOps, traditional, hybrid). Lastly, the practitioner must conclude the governance system design by identifying redundancies, prioritizing governance and management objectives, and agreeing on the final system design with the appropriate stakeholders. Typically, there will be conflicting and duplicative governance and management objectives; therefore, governance practitioners must be diligent and tailor each objective to meet their organization's specific needs.

## Leveraging Strategies and Goals to Meet Governance and Management Objectives

Enterprise goals can be identified using a questionnaire or survey. For this example, consider a mature yet risk-averse organization that not only is focused on growth and acquisition, but also wants to minimize business risk. In this case, the COBIT framework recommends governance and management objectives, as shown in **figure 3**, and indicates how to rank them by importance.

The goals cascade process can be used to map enterprise goals (EG) to their corresponding IT alignment goals (AG). The AGs are then used to identify their related governance and management objectives and processes (controls). Mapping AG01, AG02, AG05, AG07 and AG11 generates approximately 35 unique governance and management objectives, including Deliver, Service and Support (DSS). For this example, it is helpful to focus on only one—in this case, DSS05 *Managed Security Services*—to understand how to map it to MITRE (**figure 4**). However, it is important to note that the alignment goals shown in the second column of **figure 4** will map to many governance and management objectives.

## Mapping DSS05 Processes to Industry Control Frameworks

Governance and management objectives comprise more than processes (controls). COBIT is one of the only frameworks that stresses the importance of its components (enablers) to implement and maintain processes (controls). As shown in **figure 5**, processes are the practices and activities (also known as security controls in other frameworks) that organizations leverage to meet specific objectives by implementing safeguards and countermeasures. The organizational structures represent the responsible, accountable, consulted and informed (RACI) parties for a given objective and its components.

Organizations must consider the following questions:

- Who is responsible for the implementation of the process or control?
- Who is accountable for the overall maturity of the process or control?
- Who has expertise in the relevant domain, and who should be consulted for additional perspective?
- Which individuals are directly or indirectly impacted by the process or control?

**FIGURE 3**

### Goals Cascade: Enterprise Goals to IT Alignment Goals

| Design Factor | Enterprise Goal | Description | BSC Dimension | IT Alignment Goal | Description | IT BSC Dimension |
|---|---|---|---|---|---|---|
| DF2: Enterprise Goals | EG02 | Managed business risk | Financial | AG01 | I&T compliance and support for business compliance with external laws and regulations | Financial |
| | | | | AG02 | Managed I&T-related risk | Financial |
| | | | | AG07 | Security of information, processing infrastructure and applications, and privacy | Internal |
| | | | | AG11 | I&T compliance with internal policies | Internal |
| | EG06 | Business service continuity and availability | Customer | AG02 | Managed I&T-related risk | Financial |
| | | | | AG05 | Delivery of I&T services in line with business requirements | Customer |
| | | | | AG07 | Security of information, processing infrastructure and applications, and privacy | Internal |

Source: ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, USA, 2018, *https://www.isaca.org/resources/cobit*. Reprinted with permission.

**FIGURE 4**

### DSS05 Managed Security Services Example

| Design Factor | IT Alignment Goal | Description | BSC Governance/Management Objective | Description | Priority |
|---|---|---|---|---|---|
| DF2: Enterprise Goals | AG02 | Managed I&T-related risk | DSS05 | Managed security services | Primary |
| | AG07 | Security of information, processing infrastructure and applications and privacy | | | |

Source: ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, *https://www.isaca.org/resources/cobit*. Reprinted with permission.

**FIGURE 5**
COBIT Components of a Governance System


Source: ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, USA, 2018, *https://www.isaca.org/resources/cobit*. Reprinted with permission.

Policies and procedures based on the enterprise's values, principles and guidance inform the day-to-day management of its governance system and the implementation of its individual components. The organization leverages information—including data, evidence, statistics and research—to ensure the effective functioning of the governance system and the implementation of specific processes or controls.

Often neglected is the influence on the overall success of the governance system that may be attributable to the cultural values, ethical principles and behavior of the individuals responsible for implementing and managing the process controls. Many organizations do not have an objective way to assess the people, skills and competencies within the GRC and cybersecurity professions in this context. Therefore, it is paramount to establish a competency framework or program, such as the US National Initiative for Cybersecurity Education (NICE) or the Skills Framework for Information Age (SFIA), to help the enterprise determine whether a professional has the appropriate skills and core values to implement the controls. Lastly, the organization will need the proper services, infrastructure and applications to help implement and maintain the governance and management objectives.

## DSS05 Component Processes (Controls) of Managed Security Services

The goals of DSS05 *Managed Security Services* are to "maintain the level of information security risk acceptable to the enterprise in accordance with the security policy" and to "establish and maintain information security roles and access privileges."[3] These objectives are achieved through its component processes:

- DSS05.01 *Protect against malicious software.*
- DSS05.02 *Manage network and connectivity security.*
- DSS05.03 *Manage endpoint security.*
- DSS05.04 *Manage user identity and logical access.*
- DSS05.05 *Manage physical access to IT assets.*
- DSS05.06 *Manage sensitive documents and output devices.*
- DSS05.07 *Monitor the infrastructure for security-related events.*

It is essential to communicate the importance of each process and control to the stakeholders who can provide the resources necessary to help mitigate the risk. However, they may take some convincing, and an effective way to articulate risk is through the MITRE ATT&CK framework.

MITRE brings awareness to attack methodologies by classifying its framework into tactics, techniques and subtechniques.

## Mapping to MITRE

MITRE developed the MITRE ATT&CK Framework to deconstruct the cybersecurity attack life cycle into distinct phases to help practitioners comprehensively understand how bad actors execute attacks. Specifically, MITRE brings awareness to attack methodologies by classifying its framework into tactics, techniques and subtechniques. GRC, cyber and IT audit

communities can utilize this framework to optimize their existing audit and assurance programs.

In this example, only one of the seven processes—DSS05.01 *Protect against malicious software*—is mapped to MITRE so that the risk can be articulated from the attacker's perspective. DSS05.01 focuses on identifying malicious code and ensuring that the organization monitors its assets for security events and verifies that the appropriate safeguards and countermeasures are in place. **Figure 6** shows examples of MITRE mitigations for addressing malicious code.[4]

After identifying the appropriate mitigations, they can be further broken down into MITRE's relevant techniques. Although this does not create an exhaustive list of MITRE mitigations or techniques, this strategy gives practitioners a comprehensive way to convert vague processes and controls into tactical safeguards and countermeasures. This list provides an example of several techniques that practitioners should consider when optimizing their cybersecurity governance program:

- **M1048 Application Isolation and Sandboxing:**
  - **Examples of associated techniques**—T1175 Component Object Model and Distributed COM, T1189 Drive-by Compromise, T1173 Dynamic Data Exchange
- **M1049 Antivirus/Antimalware:**
  - **Example of associated techniques**—T1215 Kernel Modules and Extensions
- **M1051 Update Software:**
  - **Examples of associated techniques**—T1103 AppInit DLLs, T1017 Application Deployment Software

GRC professionals can help enterprises create bridges between the IT audit, GRC and cybersecurity communities.

- **M1034 Limit Hardware Installation:**
  - **Examples of associated techniques**—T1200 Hardware Additions, T1091 Replication Through Removable Media

## Conclusion

Strategic and tactical mappings generate numerous governance and management objectives, security controls, and MITRE mitigation and associated techniques. GRC professionals can help enterprises create bridges between the IT audit, GRC and cybersecurity communities. For example, practitioners who understand COBIT and MITRE mappings can establish meaningful relationships with the security operation center, incident response, and architecture and engineering teams. This strategy can help organizations implement a comprehensive approach to risk management and cybersecurity. It is worth noting that COBIT and MITRE are not the only frameworks available. If an organization has personnel experienced in US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 5,[5] International Organization for Standardization (ISO) standard 27001/27002[6,7] or the Center for Internet Security (CIS) Critical Security Controls,[8] those individuals can be enlisted to articulate risk at the board level and mitigate it at the code level.

**FIGURE 6**

### MITRE Mitigations Example

| Mitigation ID | Mitigation Name | Mitigation Description |
|---|---|---|
| M1048 | Application Isolation and Sandboxing | Restrict execution of code to a virtual environment on or in transit to an endpoint system. |
| M1049 | Antivirus/Antimalware | Use signatures or heuristics to detect malicious software. |
| M1051 | Update Software | Perform regular software updates to mitigate exploitation risk. |
| M1034 | Limit Hardware Installation | Block users or groups from installing or using unapproved hardware on systems, including USB devices. |

## Endnotes


1 ISACA®, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, *www.isaca.org/resources/cobit*

2 MITRE ATT&CK, *https://attack.mitre.org/*

3 *Op cit* ISACA

4 Center for Internet Security (CIS), CIS Controls Mapping to MITRE ATT&CK Enterprise Mitigations, 2020, *https://workbench.cisecurity.org/*

5 MITRE Engenuity Center for Threat Informed Defense, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 *Controls to ATT&CK Mappings*, USA, 2022, *https://ctid.mitre-engenuity.org/our-work/nist-800-53-control-mappings/*

6 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001 *Information Security Management*, Switzerland, *www.iso.org/isoiec-27001-information-security.html*

7 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27002:2013 *Information Technology—Security Techniques—Code of Practice for Information Security Controls*, Switzerland, October 2013, *www.iso.org/standard/54533.html*

8 Pylant, A.; "18 Is the New 20: CIS Critical Security Controls v8 Is Here!" Center for Internet Security (CIS), *www.cisecurity.org/insights/blog/18-is-the-new-20-cis-controls-v8-is-here*