How to Construct a Governance System From the Board Level to the Code Level

Inventory of Software Platforms and Applications

The concepts involved in promoting a mature structure for software platforms and applications can be quite intricate. Enterprises worldwide face challenges related to managing their critical assets, establishing service definitions and service-level agreements (SLAs), and developing a management system to keep track of all their assets.[1] Therefore, enterprises must be methodical and examine their asset management capabilities from the perspectives of risk optimization, resource planning and benefits realization. Considerations include communicating incidents and issues to stakeholders, managing software licenses, adhering to maintenance schedules, and potentially using remote access services for troubleshooting and diagnostic purposes.[2, 3] Notably, there is a growing dependence on third parties and a need to ensure the existence of security and privacy controls via administrative and technical safeguards and countermeasures. Ultimately, this means that enterprises need to establish mature inventories of their software platforms and applications and tailor their governance systems based on their strategies, goals, risk profiles and current IT issues.[4, 5]

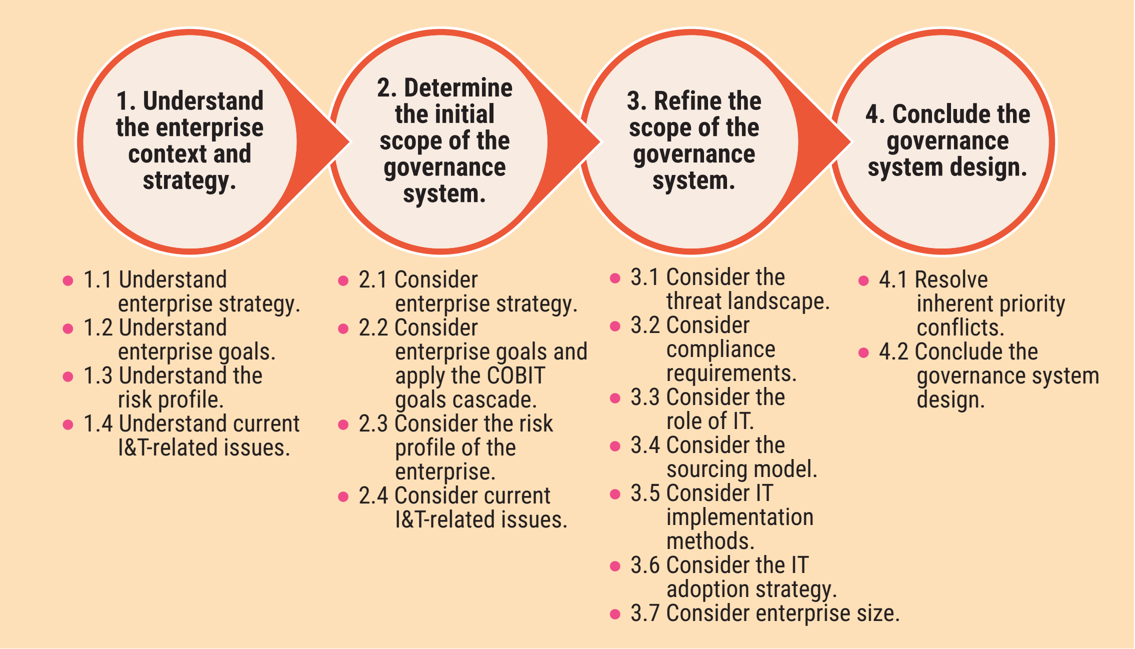
The COBIT® governance framework and the frameworks devised by the US National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO) and the Center for Internet Security (CIS) can be used to address common issues facing enterprises from the vantage point of governance cybersecurity.[6, 7] A combination of strategic, operational and tactical controls can be used to address pain points such as obtaining senior management buy-in and stakeholder engagement and securing business processes via modern technologies and security best practices.[8, 9, 10, 11] Subsequently, COBIT's design factors can be used to replicate real-life scenarios that commonly occur in enterprises.[12]

Starting From the Strategic Level

Before delving too deeply into the governance system's operational and tactical implementation, an enterprise's key stakeholders must be consulted. The goal is to obtain a clear understanding of the enterprise's strategy, goals, risk profile and current IT issues during these working sessions.[13, 14] For this demonstration, only step 1 of the governance system design workflow (**figure 1**) is discussed.

Blake Curtis, CISA, CRISC, CISM, CGEIT, CDPSE, CISSP
Is a global business risk and security engineer for Deloitte Global and a research scientist. He has more than 10 years of experience in engineering, networking, virtualization, IT service management, cybersecurity and risk management and more than 20 industry certifications across diverse disciplines. Curtis is currently completing his Ph.D. in cybersecurity at Capitol Technology University (Washington, DC, USA). He can be reached at *https://www.linkedin.com/in/reginaldblakecurtis/*.

Figure 1—Governance System Design Workflow


1. Understand the enterprise context and strategy.
2. Determine the initial scope of the governance system.
3. Refine the scope of the governance system.
4. Conclude the governance system design.
1.1 Understand enterprise strategy.
1.2 Understand enterprise goals.
1.3 Understand the risk profile.
1.4 Understand current I&T-related issues.
2.1 Consider enterprise strategy.
2.2 Consider enterprise goals and apply the COBIT goals cascade.
2.3 Consider the risk profile of the enterprise.
2.4 Consider current I&T-related issues.
3.1 Consider the threat landscape.
3.2 Consider compliance requirements.
3.3 Consider the role of IT.
3.4 Consider the sourcing model.
3.5 Consider IT implementation methods.
3.6 Consider the IT adoption strategy.
3.7 Consider enterprise size.
4.1 Resolve inherent priority conflicts.
4.2 Conclude the governance system design.

Source: ISACA®, *COBIT® 2019 Framework: Designing an Information and Technology*, USA, 2018. Reprinted with permission.

Understanding the Enterprise Context and Strategy
Questionnaires, interviews, surveys or meetings can be used to determine which archetype best represents the enterprise's strategy. In COBIT's Enterprise Strategy Design Factor, there are four primary archetypes:

1. Growth/acquisition
2. Innovation/differentiation
3. Cost leadership
4. Client service/stability

Each archetype has its own set of prioritized governance and management objectives and controls (**figure 2**). These will become more relevant as the governance system is expanded throughout the operational and tactical levels.

COBIT 2019 in Action

This scenario involves an enterprise that has recently performed an assessment and discovered that its archetype best reflects the growth/acquisition model. The governance professional must now identify the prioritized governance and management objectives and controls associated with this archetype. At the strategic level, controls are known as processes and are geared more toward IT governance stakeholders, senior management and the board of directors (BoD).[15, 16, 17, 18, 19] **Figure 3** reflects only the highest-priority objectives associated with the growth/acquisition archetype.

After determining the enterprise's strategic plan, the practitioner should focus on the primary goals that enable the enterprise to execute that plan. Once these goals are identified, they can be organized based on COBIT's Enterprise Goals Design Factor by considering whether each goal is a financial, customer, internal or growth dimension of the balanced scorecard (BSC). A BSC is used to map an enterprise's goals to IT alignment goals, metrics and actual results.[20, 21] Use this step to cascade the enterprise's goals into IT alignment goals (**figure 4**). For example, an enterprise that focuses on the growth dimension of the BSC would prioritize realizing benefits through its services portfolio, ensuring that IT services are in line with business requirements, and enabling business processes by integrating applications and technology.[22] Next, these IT alignment goals are mapped to COBIT's governance and management objectives (**figure 5**), enabling the practitioner to determine which controls are applicable at the operational and tactical levels. This exercise explains how

Figure 2—Governance and Management Objectives Mapped to Strategy Design Factors

Design Factor Value	Governance and Management Objectives Priority	Components	Focus Area Variants
Growth/ acquisition	Important management objectives[15] include: • APO02, APO03, APO05 • BIA01, BAO05, BAI11	Important components: • Organizational structures – Support the portfolio management role with an investment office – Enterprise architect • Services, infrastructure and applications – Facilitate automation and growth and realize economies of scale	COBIT core model
Innovation/ differentiation	Important management objectives include: • APO02, APO04, APO05 • BIA08, BAI11	Important components: • Organizational structures – Chief digital officer and/or chief innovation officer • Important influence of culture and behavior component for innovation	COBIT core model
Cost leadership	Important governance and management objectives include: • EDM04 • APO06, APO10	Important components: • Skills and competencies – Focus on IT costing and budgeting skills • Important influence of culture and behavior component • Services, infrastructure and applications component (e.g., for automation of controls, improving efficiency)	COBIT core model
Client service/ stability	Important governance and management objectives include: • EDM02 • APO08, APO09, APO11 • BIA04 • DSS02, DSS03, DSS04	Important components: • Important influence of culture and behavior component (client centricity)	COBIT core model

Source: ISACA®, *COBIT® 2019 Framework: Designing an Information and Technology Governance Solution*, USA, 2018. Reprinted with permission.

governance and management objectives and their associated components can satisfy the requirements of enterprise goals and objectives by aligning with IT goals.

By now, the overall approach should start to make sense from a governance perspective. Governance professionals are encouraged to continue with the other steps in the governance design workflow and use design factors such as the risk profile and threat landscape to determine which objectives and controls an enterprise should consider.

Creating a Cybergovernance Design

Once all the relevant design factors have been applied, it is time to begin integrating the governance framework with cybersecurity best practices. Use cybersecurity industry frameworks such as those developed by NIST, ISO and CIS to translate COBIT's strategic governance controls into operational and tactical controls. For example, when developing a cyberresilient strategy for software platforms and application inventory, one should start by highlighting two of the most critical strategic objectives (**figure 6**):

1. Build, Acquire and Implement (BAI) 09.02 *Manage critical assets*
2. BAI09.05 *Manage licenses*

Although the focus here is on process and controls, it is vital to consider other components when selecting governance and management

Enjoying this article?

- *Read COBIT® 2019 Design Guide: Designing an Information & Technology Governance Solution. www.isaca.org/resources/cobit*
- Learn more about, discuss and collaborate on governance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Figure 3—Enterprise Strategy Design Factor Mapped to Governance and Management Objectives

Design Factor	Type	Description	Important Gov/ Mgmt Objective	Gov/Mgmt Objective Description	Important Components	Priority
DF1: Enterprise Strategy	Growth/ Acquisition	The enterprise has a focus on growing (revenues)	APO03	*Managed Enterprise Architecture*	**Important components:** • Organizational structures – Support the portfolio management role with an investment office – Enterprise architect • Services, infrastructure and applications – Facilitate automation and growth and realize economies of scale	4.0
			BAI01	*Managed Programs*	**Important components:** • Organizational structures – Support the portfolio management role with an investment office – Enterprise architect • Services, infrastructure and applications – Facilitate automation and growth and realize economies of scale	4.0
			BAI05	*Managed Organizational Change*	**Important components:** • Organizational structures – Support the portfolio management role with an investment office – Enterprise architect • Services, infrastructure and applications – Facilitate automation and growth and realize economies of scale	4.0

Source: ISACA®, *COBIT® 2019 Framework: Designing an Information and Technology Governance Solution*, USA, 2018. Reprinted with permission.

Figure 4—Goals Cascade Part 1: Mapping Enterprise Goals to IT Alignment Goals

Design Factor	Enterprise Goal	Description	BSC Dimension	IT Alignment Goal	Description	IT BSC Dimension
DF2: Goals Cascade	EG12	Managed digital transformation programs	Growth	AG03	Realized benefits from I&T-enabled investments and services portfolio	Financial
				AG05	Delivery of I&T services in line with business requirements	Customer
				AG06	Agility to turn business requirements into operational solutions	Customer
				AG08	Enabling and supporting business processes by integrating applications and technology	Internal
				AG09	Delivering programs on time and on budget and meeting requirements and quality standards	Internal
				AG13	Knowledge, expertise and initiatives for business innovation	Learning and Growth

Source: Adapted from ISACA®, *COBIT® 2019 Framework: Designing an Information and Technology Governance Solution*, USA, 2018.

Figure 5—Goals Cascade Part 2: Mapping IT Alignment Goals to Governance and Management Objectives

Design Factor	IT Alignment Goal	Description	Governance/ Management Objective	Description	IT BSC Dimension
DF2: Goals Cascade (Part 2)	AG06	Agility to turn business requirements into operational solutions	APO03	*Managed enterprise architecture*	Primary
			APO04	*Managed innovation*	Primary
			APO08	*Managed relationships*	Primary
			BAI02	*Managed requirements definition*	Primary
			BAI03	*Managed solutions identification and build*	Primary
			BAI06	*Managed IT changes*	Primary
			BAI07	*Managed IT change acceptance and transitioning*	Primary
			BAI11	*Managed projects*	Primary

Source: Adapted from ISACA®, *COBIT® 2019 Framework: Designing an Information and Technology Governance Solution*, USA, 2018, *h*

objectives.[23] For example, for each process or control, consider the following:

- **Principles, policies and framework**—Will ISO or NIST be used for operational controls?
- **Organizational structure**—Have the responsible, accountable, consulted and informed (RACI) entities been identified for each process or control?
- **Processes**—What are the controls at the operational and tactical tiers?
- **Information**—Have both inputs and outputs been considered?
- **People, competency and skills**—What skills are necessary to implement these processes and controls? The NICE Cybersecurity Workforce Framework[24] and the Skills Framework for Information (SFIA)[25] can be used to help determine the needed skills.
- **Culture, ethics and behavior**—Could pseudocultures or anticollaboration impede success?
- **Services, infrastructure and applications**—Which services and technologies will be used to implement these processes and controls?

It is important to pay close attention to the supplemental guidance that is available such as industry references including the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) Framework, specifically their components, principles and points of focus.[26, 27, 28]

Tackling Governance at the Operational Level

At the level of operational implementation, enterprises may choose between International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001/27002 and NIST Special Publication (SP) 800-53 Revision 5. It is a good idea to perform a gap analysis between the two to determine the most objective and reasonable set of controls for the enterprise.

ISO/IEC 27001/27002

ISO helps enterprises secure their data, develop robust security and privacy controls, and meet their organizational objectives.[29] For ISO, there are three relevant operational controls (**figure 7**):

1. **A.12.5.1**—Installation of software on operational systems

Figure 6—COBIT Strategic Governance Controls

Implementation Tier	Framework	Control ID	Control Name/ Title	Control Text	Discussion/Guidance
Strategic	**COBIT**	**BAI09.02**	***Manage critical assets***	**Management Practice** BAI09.02 *Manage critical assets* **Description** Identify assets that are critical in providing service capability. Maximize their reliability and availability to support business needs. **Activities** Capability Level 2 1. Identify assets that are critical in providing service capability by referencing requirements in service definitions, service level agreements and the configuration management system. 2. On a regular basis, consider the risk of failure or need for replacement of each critical asset. 3. Communicate to affected customers and users the expected impact (e.g., performance restrictions) of maintenance activities.	• **National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure** Cybersecurity v1.1, April 2018 – ID.AM Asset Management • **NIST Special Publication 800-53, Revision 5 (Draft), August 2017** – 3.13 Physical and environmental protection (PE-20)
	COBIT	**BAI09.05**	***Manage licenses***	**Management Practice** BAI09.05 *Manage licenses* **Description** Manage software licenses to maintain the optimal number of licenses and support business requirements. Ensure that the number of licenses owned is sufficient to cover the installed software in use. **Activities** Capability Level 2 1. Maintain a register of all purchased software licenses and associated license agreements. Capability Level 3 2. On a regular basis, conduct an audit to identify all instances of installed licensed software.	No related guidance for this management practice

Source: Adapted from ISACA®, *COBIT® 2019 Framework: Designing an Information and Technology Governance Solution,* USA, 2018.

2. **A.8.1.1**—Inventory of assets
3. **A.8.1.2**—Ownership of assets

These controls are vital in helping organizations manage their software platforms and applications. They focus on maintaining an up-to-date list of authorized and unauthorized software, establishing clear ownership and accountability, and ensuring that IT-enabled investments are managed throughout their economic life cycle to generate value.[30]

NIST SP 800-53 Revision 5

NIST SP 800-53 is a collection of security and privacy safeguards and countermeasures to defend enterprises, personnel and organizational assets from various types of threats, risk and human

Figure 7—ISO Operational Controls

Implementation Tier	Framework	Control ID	Control Name/Title
Operations	ISO/IEC 27001/27002: 2013	**A.12.5.1**	Installation of software on operational systems
		A.8.1.1	Inventory of assets
		A.8.1.2	Ownership of assets

Source: Adapted from ISACA®, *Implementing the NIST Cybersecurity Framework Using COBIT® 2019*, USA, 2019.

error.[31] At the operational level, NIST recommends the following controls for software platforms and applications (**figure 8**):

- **CM-8**—System component inventory
- **PM-5**—System inventory
- **CM-12**—Information location
- **CM-12(1)**—Information location/automated tools to support information location

NIST suggests implementing centralized system component inventories such as asset management systems and configuration management databases (CMDBs). These types of solutions ensure that the configuration items (CIs) or other related identifiers

Figure 8—NIST Controls

Implementation Tier	Framework	Control ID	Enhancement ID	Control Name/Title	Control Text
Operations	NIST SP 800-53 Rev. 5	**CM-8**	N/A	System Component Inventory	a. Develop and document an inventory of system components that: • Accurately reflects the system; • Includes all components within the system; • Is at the level of granularity deemed necessary for tracking and reporting; and • Includes the following information to achieve system component accountability: (Assignment: organization-defined information deemed necessary to achieve effective system component accountability); and b. Review and update the system component inventory (Assignment: organization-defined frequency).
		PM-5	N/A	System Inventory	Develop and update (Assignment: organization-defined frequency) an inventory of organizational systems.
		CM-12	N/A	Information Location	a. Identify and document the location of (Assignment: organization-defined information) and the specific system components on which the information is processed and stored; b. Identify and document the users who have access to the system and system components where the information is processed and stored; and c. Document changes to the location (i.e., system or system components) where the information is processed and stored.
		CM-12	CM-12(1)	Information Location/Automated Tools to Support Information Location	Use automated tools to identify (Assignment: organization-defined information by information type) on (Assignment: organization-defined system components) to ensure controls are in place to protect organizational information and individual privacy.

Source: Adapted from ISACA®, *COBIT® 2019 Framework: Designing an Information and Technology Governance Solution*, USA, 2018.

track system names, system owners, versioning, licenses, upstream and downstream dependencies, and network-related information. Knowing where assets are located at all times is crucial and sometimes regulated by external mandates.[32, 33, 34] This information enables enterprises to understand where data are being stored, processed and transmitted. It also relates to the critical nature and sensitivity of data and ensuring that the right level of control is present. When implementing NIST controls, practitioners should always reference the supplemental guidance (other publications and documents) provided, which can help with the successful implementation of safeguards and the development of assessment criteria for auditors.

Rolling Up Sleeves and Getting Tactical

Many enterprises stop at the operational level from both an implementation and a review (audit) perspective. Frameworks are prevalent in the cybersecurity and assurance disciplines, yet they require a great deal of technical competence to ensure that professionals interpret them accurately. There are many tactical control frameworks that can empower the enterprise to translate strategic and operational controls into actual configuration parameters for operating systems, applications, networking infrastructure and cloud platforms.

> “MANY ENTERPRISES STOP AT THE OPERATIONAL LEVEL FROM BOTH AN IMPLEMENTATION AND A REVIEW (AUDIT) PERSPECTIVE.”

Center for Internet Security: The Tactical Solution for Governance

CIS 20 is a set of 20 critical security control objectives that enterprises can employ to build secure and resilient infrastructures to prevent threats, reduce vulnerabilities and establish security control baselines.[35] The CIS 20 are divided into subcontrols that can be applied at a more granular level for different types of technologies. These security baselines (benchmarks) enable organizations to comply with international, national, state and local mandates. The CIS framework allows cybersecurity teams to build security into the design instead of bolting it onto the solution later. It can help enterprises build hardened images, applications and networking infrastructure, and support vulnerability management teams by running benchmark compliance scans in conjunction with

Figure 9—CIS Critical Security Controls

Implementation Tier	Framework	Control ID	Control Name/Title	Control Text
Operations	Tactical	Center for Information Security	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.
			Ensure Software Is Supported by Vendor	Ensure that only software applications or operating systems currently supported by the software’s vendor are added to the organization’s authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.
			Track Software Inventory Information	The software inventory system should track the name, version, publisher and install date for all software, including operating systems authorized by the organization.
			Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

Source: Adapted from ISACA®, *Implementing the NIST Cybersecurity Framework Using COBIT® 2019*, USA, 2019.

vulnerability scans. For both implementers and auditors, this is an ideal tool. It frees up time and resources, addresses technical proficiency gaps, and enables enterprises to incorporate security by design earlier in the overall economic life cycle. At the bottom of the hierarchy lie the configuration parameters necessary to implement governance and management objectives and security controls. The following critical security controls (CSCs) enable enterprises to address the tactical issues associated with the proper inventory of software platforms and applications (**figure 9**):

- CSC-2.1—Maintain inventory of authorized software
- CSC-2.2—Ensure that software is supported by vendor
- CSC-2.4—Track software inventory information
- CSC-2.5—Integrate software and hardware asset inventories

Incorporating Controls Into Technology

The CIS Apache HTTP Server 2.4 Benchmark can identify the configurations associated with the controls.[36]

For example, configuration parameter 1.3—Ensure Apache Is Installed from the Appropriate Binaries (**figure 10**)—aims to verify that the enterprise is leveraging vendor-supplied binaries that have been tailored for the operating system's environment, have undergone quality assurance testing and automation, and obtained the latest security updates to reduce the risk of compromise. This configuration parameter within the benchmark also provides instructions on how to implement the control. Moreover, IT auditors who do not have strong technical backgrounds can review controls against CIS benchmarks to gain reasonable assurance that the appropriate configurations are in place.

CIS Apache HTTP Server 2.4 Benchmark Version 7

The following lists the overall objectives of this specific configuration parameter:

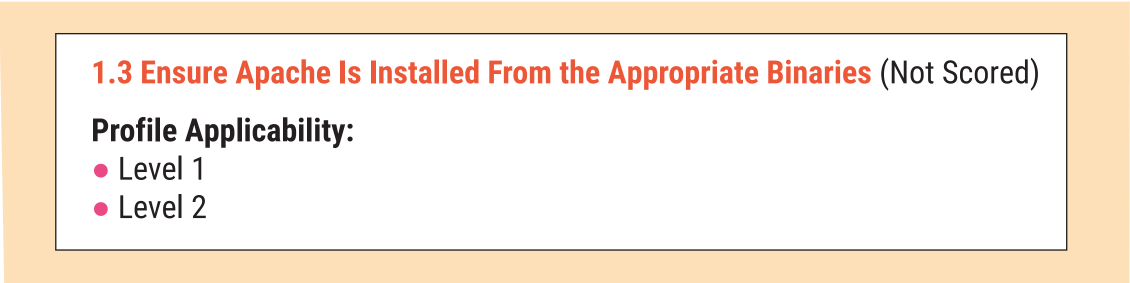
- **Maintain inventory of authorized software**—Maintain an up-to-date list of all authorized software that the enterprise requires for any business purpose on any business system.
- **Ensure that software is supported by vendor**—Ensure that only software applications or operating systems currently supported by the software vendor are added to the enterprise's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.

Notably, CIS offers an automated solution that can be deployed from a centralized server via vulnerability management software. Alternatively, one can simply download the CIS-CAT Pro Assessor and scan the enterprise system's configuration against the benchmark.

Conclusion

There are many ways to take a governance program to the next level and mitigate business and IT communication issues. The proposed guidelines herein should not be viewed as an exhaustive list of controls, as they do not include all the safeguards, design factors and various nuances necessary to build a holistic governance structure. Those interested in building a control framework from a hierarchical perspective must be well versed in

Figure 10—1.3 Ensure Apache Is Installed From the Appropriate Binaries



1.3 Ensure Apache Is Installed From the Appropriate Binaries (Not Scored)

Profile Applicability:

- Level 1
- Level 2

COBIT, ISO, NIST, CIS, and potentially other frameworks such as MITRE ATT&CK, Open Web Application Security Project (OWASP), COSO Internal Controls and COSO ERM.

In many cases, there is a contrived relationship between the business and IT communities because of previous failed initiatives or the perception that IT contributes little to the business's overall success. Establishing a governance framework at the strategic, operational and tactical levels can help the business process owners and IT communities speak the same language and encourage the enterprise to evolve, innovate and compete at a higher level. Furthermore, the business should focus on benefits delivery, a managed portfolio and agreement on the definition of requirements.[37, 38, 39] The governance and control frameworks do not function in isolation. They are inextricably bound and have a cumulative relationship with and a reciprocal influence on each other. For example, if an enterprise is having trouble implementing operational and tactical controls, those controls can be mapped to the COBIT hierarchy to identify common issues and objectives that should be presented to senior management. The next time someone says an enterprise is an ISO or NIST organization, a CIS 20 adopter or a COBIT framework shop, practitioners would be positioned to proudly proclaim to be all of the above.

Endnotes

1. Joint Task Force Interagency Working Group, *Security and Privacy Controls for Information Systems and Organizations: Revision 5*, NIST Special Publication (SP) 800-53, National Institute of Standards and Technology (NIST), USA, 2020, *https://doi.org/10.6028/NIST.SP.800-53r5. doi:10.6028/NIST.SP.800-53r5*
2. ISACA®, *COBIT® 2019 Framework: Designing an Information and Technology Governance Solution*, USA, 2018, *https://www.isaca.org/resources/cobit*
3. *Op cit* Joint Task Force Interagency Working Group
4. Center for Internet Security (CIS), *Cybersecurity Best Practices: CIS Controls and CIS Benchmarks*, USA, 2021, *https://www.cisecurity.org/cybersecurity-best-practices/*
5. *Op cit* Joint Task Force Interagency Working Group
6. ISACA, *Implementing the NIST Cybersecurity Framework Using COBIT® 2019*, USA, 2019, *https://www.isaca.org/bookstore/bookstore-cobit_19-print/cb19nist*
7. International Organization for Standardization (ISO), ISO/IEC 27002, *Information Technology: Security Techniques: Code of Practice for Information Security Controls*, Switzerland, 2013, *https://www.iso.org/standard/54533.html*
8. ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, *https://www.isaca.org/resources/cobit*
9. *Op cit* ISACA, *COBIT 2019 Framework: Designing an Information and Technology Governance Solution*
10. ISACA, *COBIT® 2019 Framework: Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*, USA, 2018, *https://www.isaca.org/resources/cobit*
11. ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, USA, 2018, *https://www.isaca.org/resources/cobit*
12. *Op cit* ISACA, *COBIT 2019 Framework: Designing an Information and Technology Governance Solution*
13. *Ibid.*
14. *Op cit* ISACA, *COBIT 2019 Framework: Implementation Guide*
15. *Op cit* ISACA, *COBIT 2019 Framework: Governance and Management Objectives*
16. *Op cit* ISACA, *COBIT 2019 Framework: Designing an Information and Technology Governance Solution*
17. *Op cit* ISACA, *COBIT 2019 Framework: Implementation Guide*
18. *Op cit* ISACA, *COBIT 2019 Framework: Introduction and Methodology*
19. *Op cit* ISACA 2019
20. Committee of Sponsoring Organizations of the Treadway Commission (COSO), *COSO Enterprise Risk Management: Integrating With Strategy and Performance*, USA, 2017
21. Sobel, P. J.; *Managing Risk in Uncertain Times: Leveraging COSO's New ERM Framework*, Internal Audit Foundation, USA, 2018

[22] *Op cit* ISACA, *COBIT 2019 Framework: Designing an Information and Technology Governance Solution*

[23] *Op cit* ISACA, *COBIT 2019 Framework: Introduction and Methodology*

[24] Petersen, R.; D. Santos; M. C. Smith; K. A. Wetzel; G. Witte; NIST Special Publication (SP) 800-181 Revision 1, *Workforce Framework for Cybersecurity (National Initiative for Cybersecurity Education [NICE] Framework)*, National Institute of Standards and Technology, USA, November 2020, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf*

[25] SFIA Foundation, *Skills Framework for the Information Age 7: The Complete Reference*, UK, 2018

[26] *Op cit* COSO

[27] *Op cit* ISACA 2019

[28] *Op cit* Sobel

[29] *Op cit* International Organization for Standardization

[30] *Ibid.*

[31] *Op cit* Joint Task Force

[32] *Op cit* Center for Internet Security

[33] *Op cit* Committee of Sponsoring Organizations of the Treadway Commission

[34] *Op cit* Joint Task Force

[35] *Op cit* Center for Internet Security

[36] *Ibid.*

[37] *Op cit* ISACA, *COBIT 2019 Framework: Designing an Information and Technology Governance Solution*

[38] *Op cit* ISACA, *COBIT 2019 Framework: Implementation Guide*

[39] *Op cit* ISACA 2019