D4 Data and Ethics

Autumn 2022 | Lecture 3 - Part II

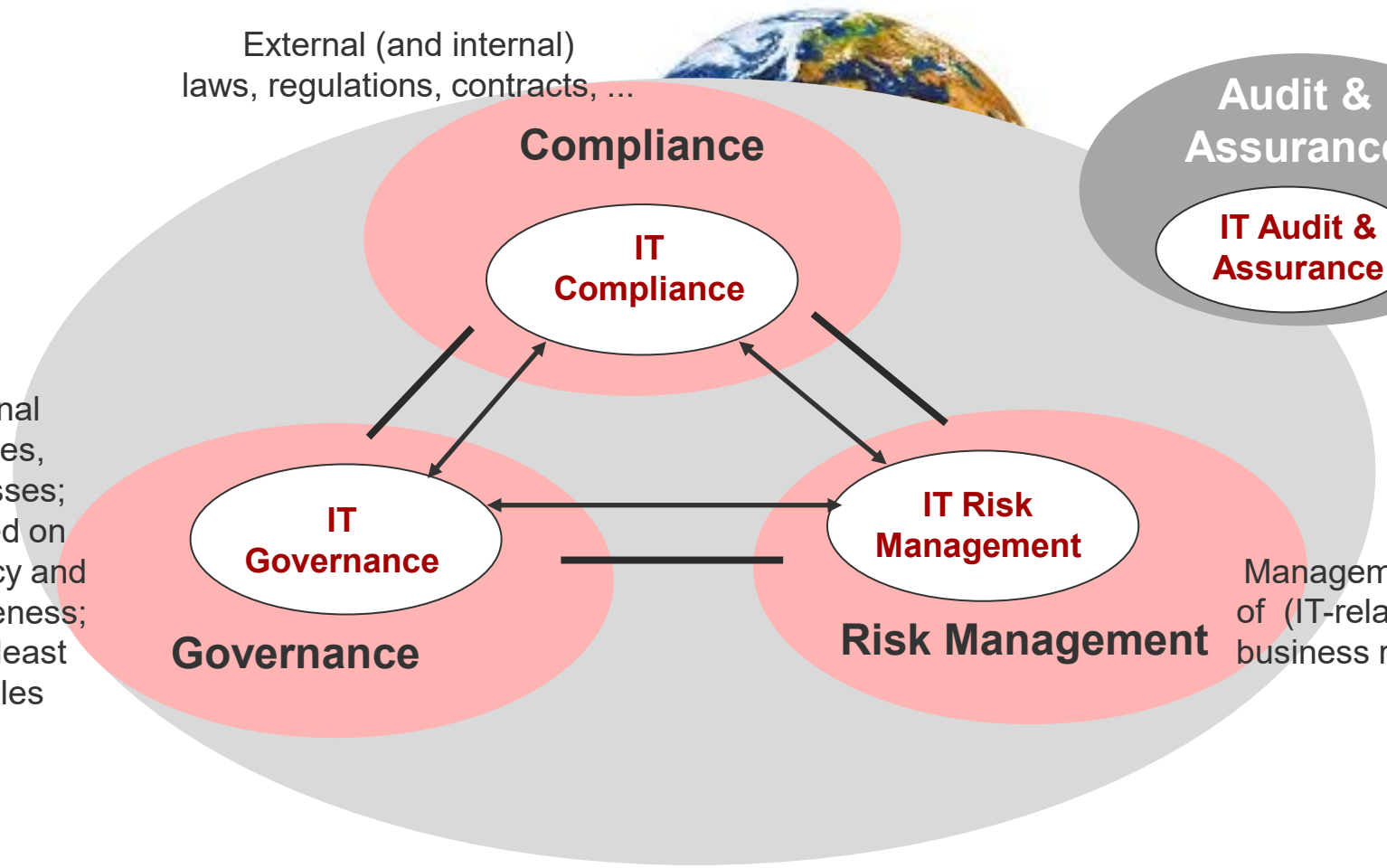
Focus: Information security & cybersecurity | Author: Prof. Dr. Petra Maria Asprion | FHNW

Agenda

Part I -- Repetition L1	→ SD1
Part II -- Organization Layer: Relevant References	→ SD2
Part III -- Organization Layer: First control - IS Policy	→ SD3
Part IV -- Organization Layer: Selective control - GEIGER	→ SD4
Coaching Session #3	→ SD5

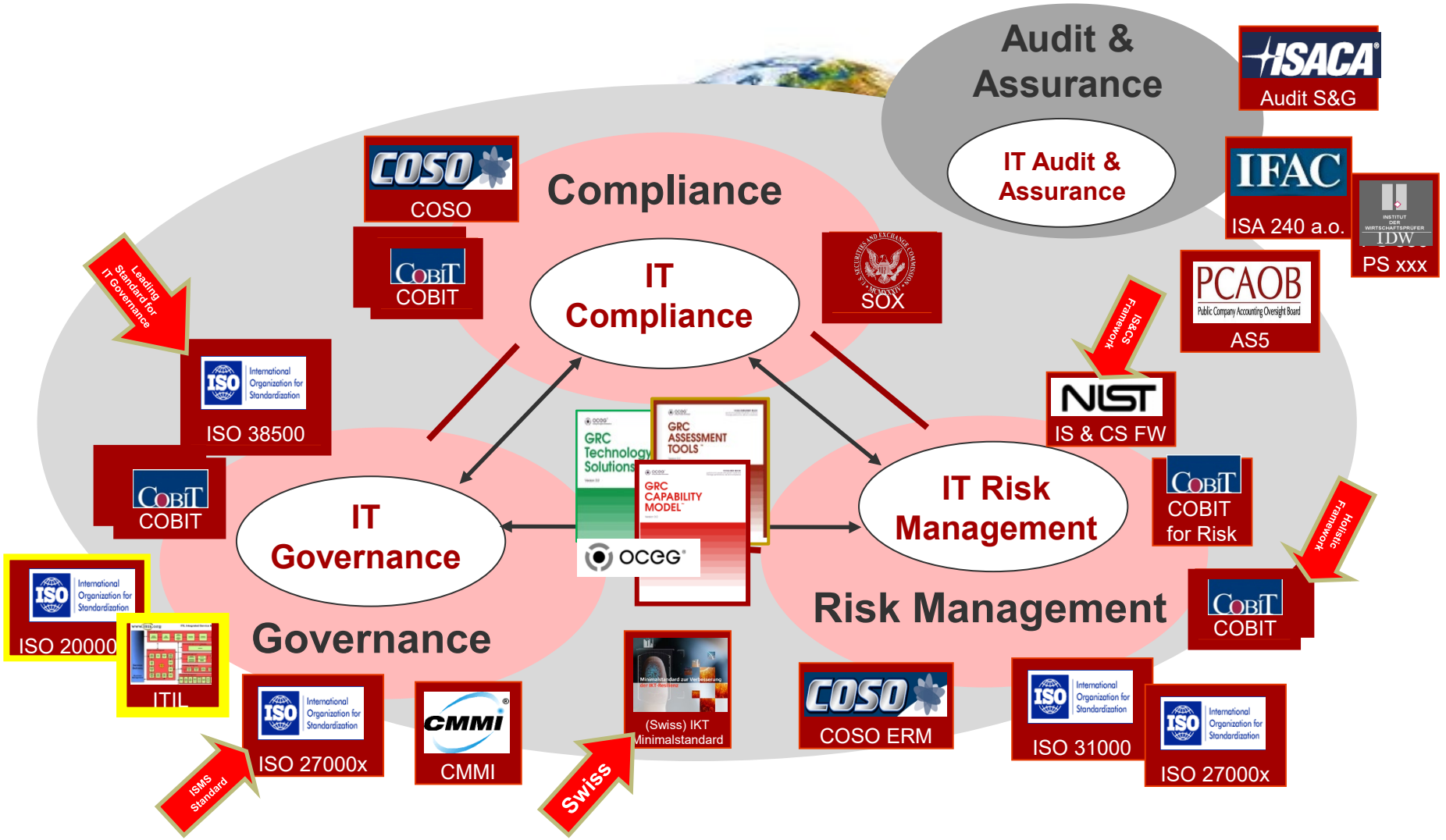
→ SD = Slide Deck

Governance, Risks, Compliance Management -- a holistic approach



Klotz, 2009, p. 11 (adapted)

GRC and related reference models



Add-on

OCEG - Your Source For GRC and Principled Performance®

Principled Performance is the healthy state of being that drives success in any organization. It means being able to reliably achieve objectives while addressing uncertainty and acting with integrity. Taking an integrated approach to how you govern and manage performance, risk and compliance is key to gaining Principled Performance. OCEG, through its GRC Capability Model (OCEG Red Book) and related resources is the only organization that provides you with the guidance necessary to move along the path to Principled Performance.

OCEG is ready to help you address the challenges tha face today. Join the tens of thousands of individuals in OCEG community and stay on the path to Principled Performance

OPTIMIZE YOUR:

Governance
Ensure that sound governance structures are in place "below the board" so that the right information about the right issues is available at the right time.

Risk
Integrate risk management with strategic planning and maintain a 360-degree view of organizational risks and effectively allocate resources to address them.

Ethics & Compliance
Establish practices and a culture to prevent misconduct, inspire desired conduct, detect problems and improve outcomes.

Finance
Reduce costs and optimize how you allocate capital to governance, risk and compliance processes so that GRC is better aligned with the business.

Technology
Address IT compliance issues and the alignment of information technology to general GRC needs in the rest of the business.

Audit
Go beyond financial processes and assess the design and operation of controls for governance, risk management, compliance and ethics efforts throughout the enterprise.

Legal
Identify and establish sound practices to address your legal risks and improve your ability to detect and correct issues; while improving your ability to defend the organization.

Core Processes
Embed sound GRC practices in all lines of business and core processes so that business owners and operators are accountable for GRC success.

RESOURCES AND TOOLS

Resources developed by OCEG, in-house GRC professionals, and other experts, are shared within the OCEG Community:

- Guides and handbooks
- GRC Surveys, research and benchmarking reports
- The GRC Illustrated Series – infographics of key GRC processes
- Topical whitepapers and articles

EXECUTIVE SUPPORT AND SOLUTIONS

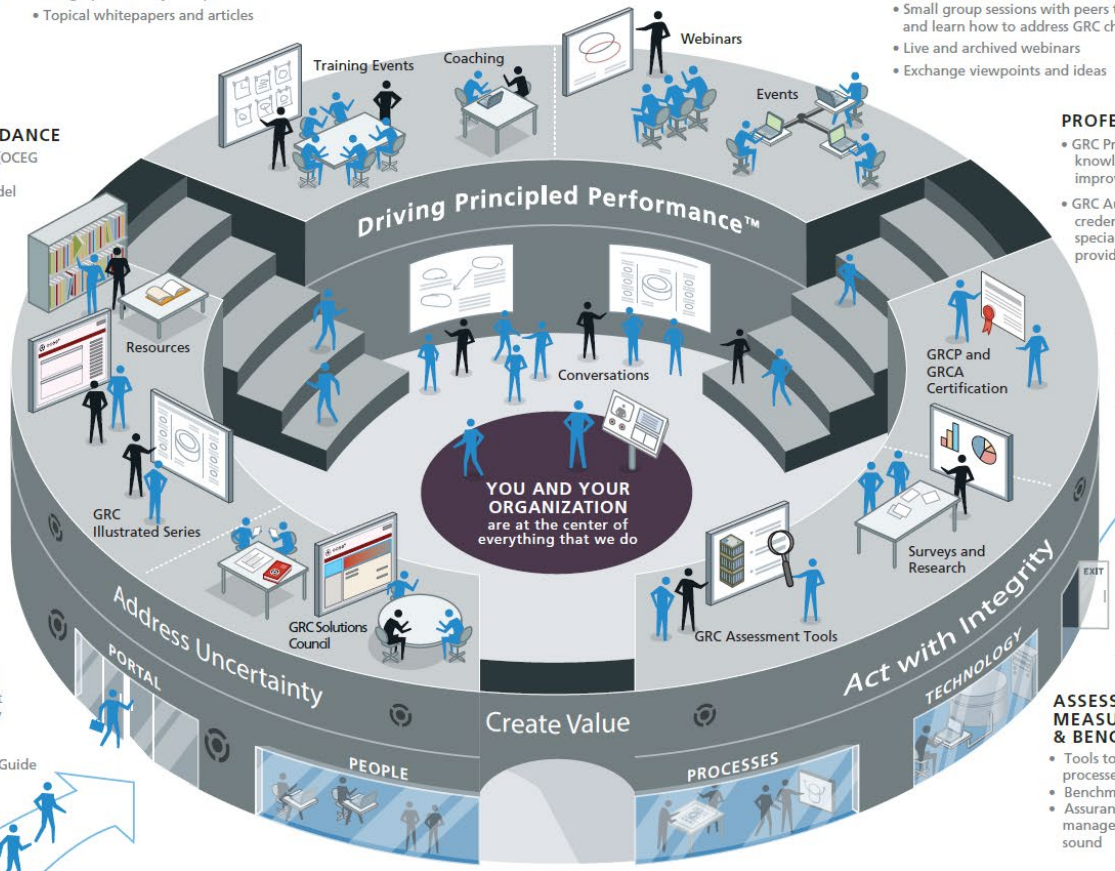
- Participate in the OCEG Executive Council for senior leaders in GRC roles and enjoy small group interaction and exchanges with peers and experts
- Learn how to implement the OCEG Framework in your organization by working with OCEG staff and partners

EVENTS AND NETWORKING

- Small group sessions with peers to discuss and learn how to address GRC challenges
- Live and archived webinars
- Exchange viewpoints and ideas

FRAMEWORKS & GUIDANCE

- The GRC Capability Model (OCEG Red Book), an open source, comprehensive process model developed and vetted by hundreds of experts and reviewed by thousands
- Open Source GRC-XML technology standards
- GRC Assessment Tools (OCEG Burgundy Book) with agreed upon procedures for assessing your GRC capabilities on an enterprise, division or project scale



PROFESSIONAL CERTIFICATIONS

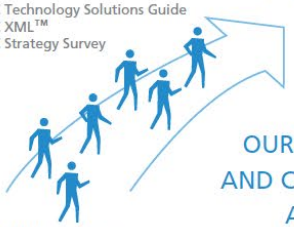
- GRC Professional (GRCP) certification demonstrates your knowledge and ability to drive GRC process improvements
- GRC Audit (GRCA) certification enhances your audit credentials and expertise with understanding of the special requirements for auditing GRC capabilities and providing assurance

Take back tools you can use to help your organization and your career

GRC SOLUTIONS COUNCIL

This group shares member expertise with the OCEG Community and works together to develop strategic and technical resources about the application of technology to GRC. Projects include:

- GRC Technology Solutions Guide
- GRC XML™
- GRC Strategy Survey



Multiple Professions come together in ONE PLACE

ASSESSMENTS, MEASUREMENTS, & BENCHMARKS

- Tools to evaluate your GRC processes and benchmark with peers
- Benchmarking studies and polls
- Assurance to the board and senior management that GRC processes are sound

OUTCOMES

OCEG can assist you on the path to Principled Perfomance™ with tools and resources you can use to:

- Establish an integrated, organization-wide approach to GRC ensuring the flow of consistent information.
- Design and measure your GRC efforts against a business process model developed by hundreds of business, financial, legal and technology experts and publicly vetted by thousands.
- Benchmark your organization's performance against peers and participate in targeted industry research and resource development.
- Join forces with peers who are managing governance, risk and compliance challenges from every angle
- Do your job better, faster, and more economically with the right tools.

OUR APPROACH AND CAPABILITIES ARE UNIQUE

PEOPLE

OCEG brings you the expert executive team that innovated and developed the concept of GRC and the only process model addressing GRC. Team members have backgrounds in business, legal, finance, audit, risk management, technology, research and compliance, and ethics management. Our hands-on experience provides the knowledge and understanding to help you drive to Principled Performance in your organization.

PROCESSES

A collaborative, open process to develop publicly vetted standards and guidance addressing the full scope of governance, risk, compliance and ethics management and measurement.

TECHNOLOGY

An interactive online content portal with cross-referenced and linked resources as well as on-demand video education. Get what you want, how you want, and when you want it.

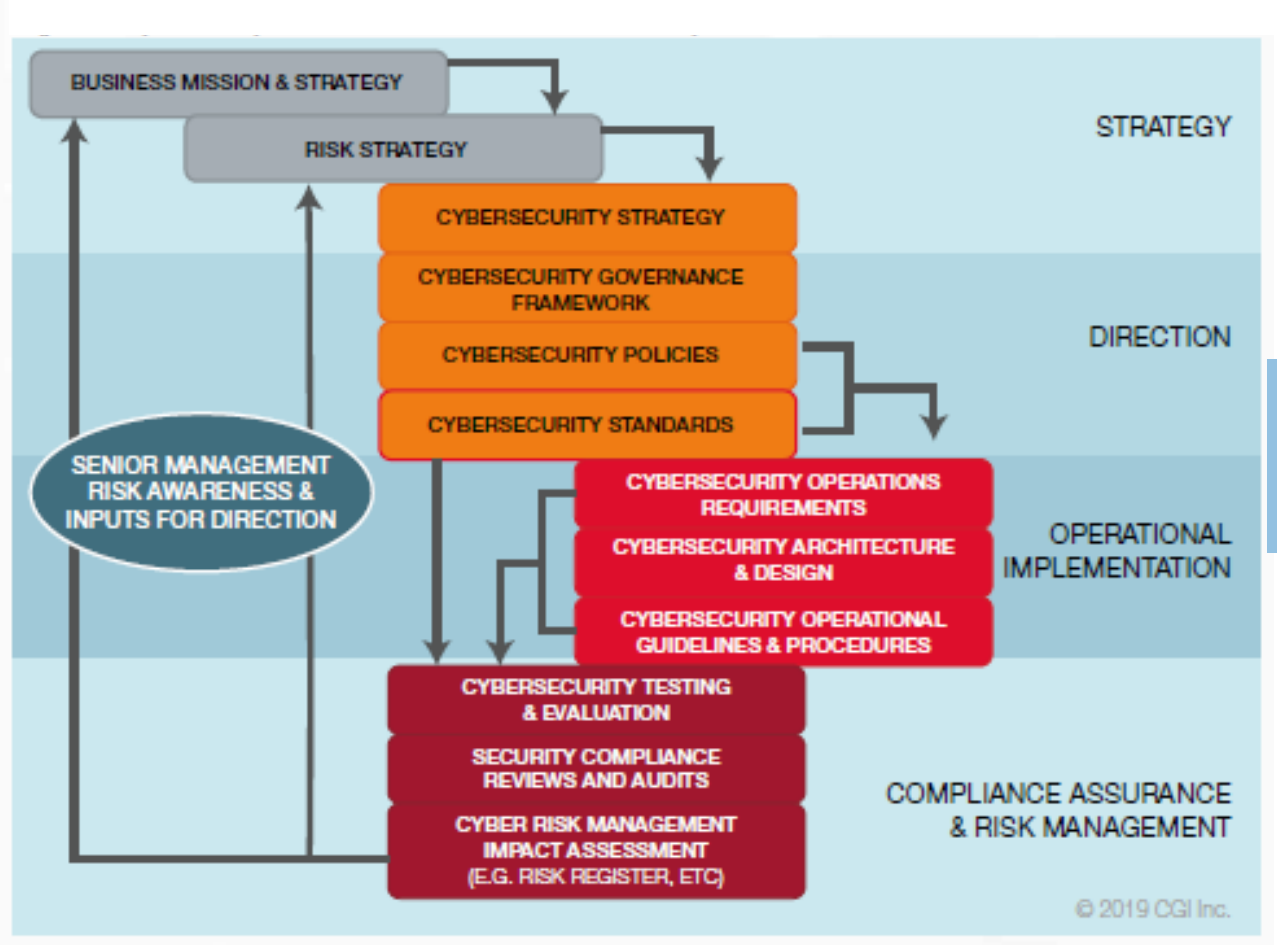
Reference Models – a response to deal with risks …

Depending on the authors „reference models“ refered to as standard (ISO), framework (NIST, ISACA), guideline (OECG), best practice (ITIL), …

- Reference models provide **a common set of reference points** to evaluate whether an organization has controls in place (e.g., processes, procedures, manual activities) that meet an agreed minimum requirement.
- If organizations meet a certain reference model, then it **gives third parties** (e.g., auditors, customers, suppliers) **confidence** to an organization's **ability to deliver to that reference** (could be a competitive advantage).
  E.g., an organization that is compliant with a security standard 27K may have an advantage over a competitor who does not when customers are evaluating their products or services (https://www.itgovernanceusa.com/blog/get-a-competitive-edge-with-iso-27001)
- Regulatory and legal requirements may specify certain references/standards that must be met.
  E.g., if your company processes credit cards then you must be compliant with the PCI DSS Data Security Standard (https://www.baselinemag.com/c/a/Security/TJX-Anatomy-of-a-Massive-Breach). Other regulatory requirements could be e.g., Data Protection Act, GDPR, SOX, HIPAA, …).
- If an organization is not compliant to a recognized reference/standard but victim to a security breach, then it could face potential lawsuits from those customers impacted by that breach.
  For example, TJX (meant to be PCI compliant) suffered a security breach, over 45 million credit card details were hacked; see https://www.bankinfosecurity.com/tjx-hacking-incident-shows-cracks-in-payment-card-systems-a-222)

⇒ **Reference Models help organizations to meet regulatory requirements!**

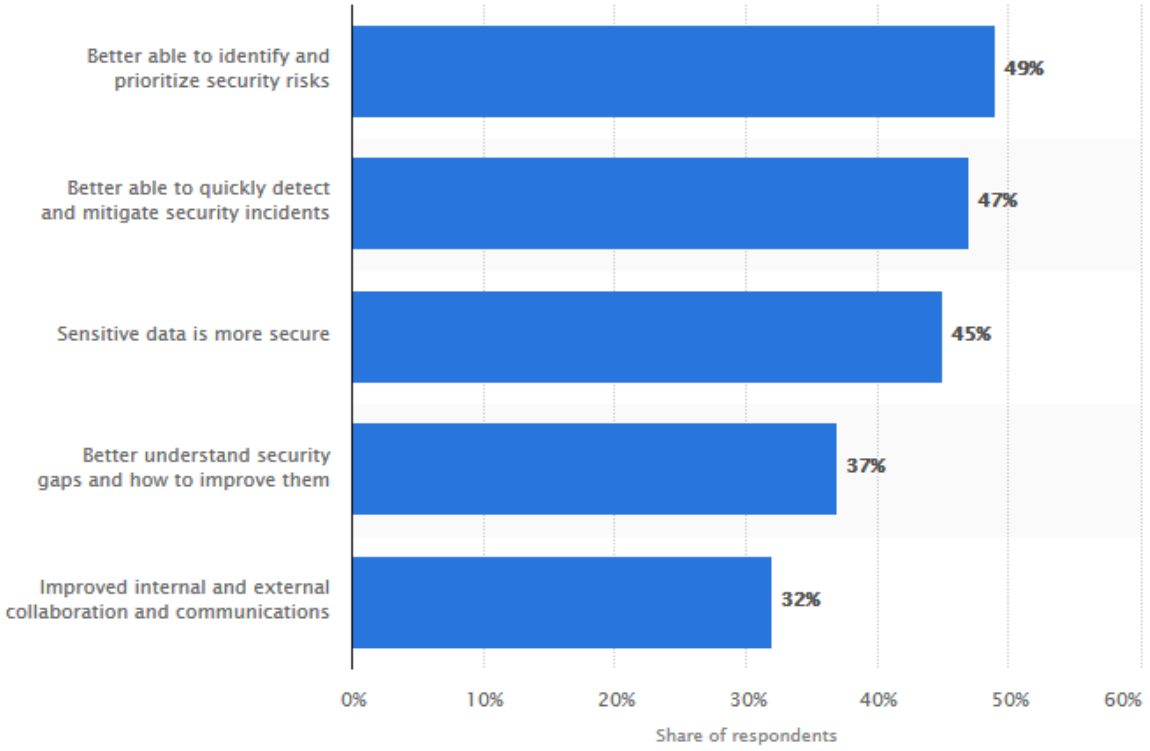
Selection of References -- IT Governance Hierarchy



(Cyber) Security standards sit at the critical interface between the "Direction" elements and the "Operational Implementation" elements.

https://www.cgi.com/sites/default/files/2019-08/cgi-understanding-cybersecurity-standards-white-paper.pdf (2019)

“What impact has the adoption of a risk-based [cyber security] framework had on your organization?”



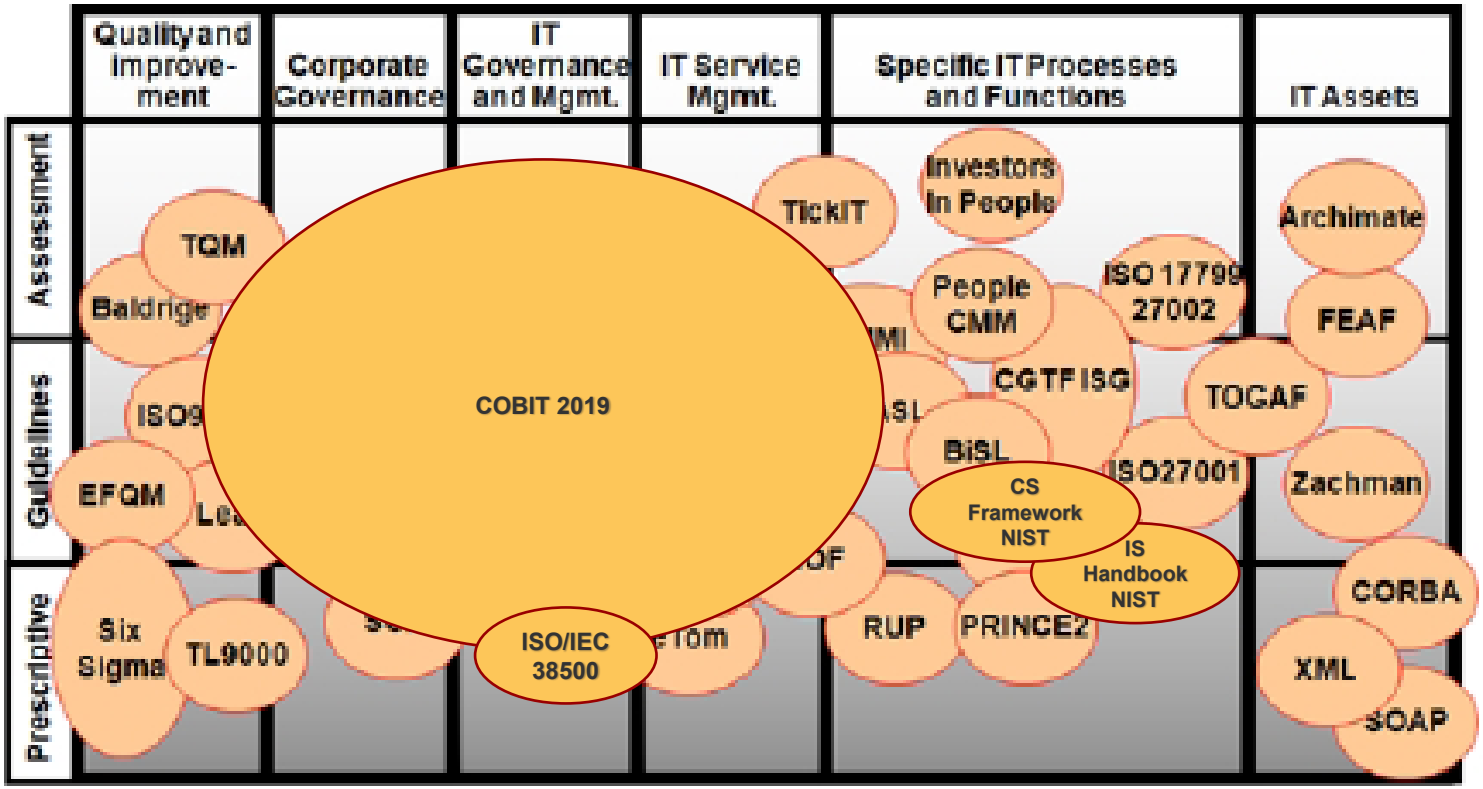
The statistic shows the leading impacts of employing **a risk-based security cyber security framework**, according to respondents to a 2015 information security survey conducted by PwC.

As of the 2015 survey, conducted by PWC, 45% of respondents indicated that risk-based security frameworks **had made their organization's sensitive data more secure.**

https://www.statista.com/statistics/588307/worldwide-information-security-survey-risk-framework-impacts/

Learning Note: You know some positive impact using “reference models”

Gartner: Positioning of International Standards and Industry Frameworks



Adopted from Gartner, Frameworks and Standards to Consider When Evaluating Providers' Delivery Methods, 2010

Have a Look on the Gartner´s website: https://www.gartner.com/en

To ensurethat (cybersecurity) standards are clear and relevant …

10 basic principles should be applied

Source:
https://www.cgi.com/sites/default/files/2019-08/cgi-understanding-cybersecurity-standards-white-paper.pdf

1. **Be linked to policy**. In addition to alignment with business needs, linking a standard to policy also ensures consistent implementation. If your standard is not directly related to the implementation of an approved policy, be prepared for it to be challenged by those who would resist its adoption.
2. **Be collaborative.** Cybersecurity standards can impact many facets of an enterprise. For that reason it is essential to directly engage key stakeholders such as IT operations and business line owners, as well as risk, audit, privacy, and legal departments. Make it a team sport and embrace their inputs. Doing so will make them feel that they have played a role in developing the standard, and they will be less likely to oppose its adoption.
3. **Be approved by an appropriate authority.** Standards must be implemented and supported by more than just IT security. Therefore, it is imperative that standards be "championed" and approved by an overarching authority (e.g. at the C-level). Failure to do so creates a risk that the standard will not be acknowledged and fully implemented across the enterprise.
4. **Be concise.** The wordiness of your description of a standard is inversely proportional to the number of people who will take the time to read it.
5. **Be clear.** Unclear standards lead to ambiguous, inconsistent and interpretive implementations. Standards must clearly state what the objective is in terms that all stakeholders will understand.
6. **Stick to the WHAT.** Standards must clearly state the end-state objective and resist the temptation to delve into how it is to be achieved. Often there are many ways by which a standard can be implemented. This is best left to those who must deploy and execute the standard (as long as it achieves the desired outcome).
7. **Ensure viability.** There is little sense in describing a solution that cannot be achieved in practical business or technical terms. For that reason, those developing the standards must work in partnership with other stakeholders to ensure viability (see Be collaborative).
8. **Ensure auditability.** To be effective, standards routinely must be monitored for compliance. Human nature is such that where monitoring or compliance reviews of a standard are not being done, the standard increasingly will be ignored and its effectiveness will quickly erode. Audit is a key tool in this regard (see Measuring standards compliance, Page 10).
9. **Build in traceability.** Ensuring that standards can be directly traced to an enterprise's policies, as well as external standards, not only demonstrates the importance of the standard, but also assists in updating those standards if the associated policies and external standards change.
10. **Update regularly.** Ensure that cybersecurity standards are regularly reviewed and updated. Policies, technologies and threats are all subject to change, and the standards must also change if they are to remain relevant. Failure to do so will eventually mean that the standard will be considered obsolete and ignored.

Minimum content requirements for a typical standards document:

Source:
https://www.cgi.com/sites/default/files/2019-08/cgi-understanding-cybersecurity-standards-white-paper.pdf

UNDERSTANDING A CYBERSECURITY STANDARD

Cybersecurity standards usually are expressed in written form, especially if they include complex requirements. Having standards created as a document, at least by category (e.g. Access Control standards), also allows standards and associated controls to be reviewed by relevant stakeholders and approving authorities more easily.

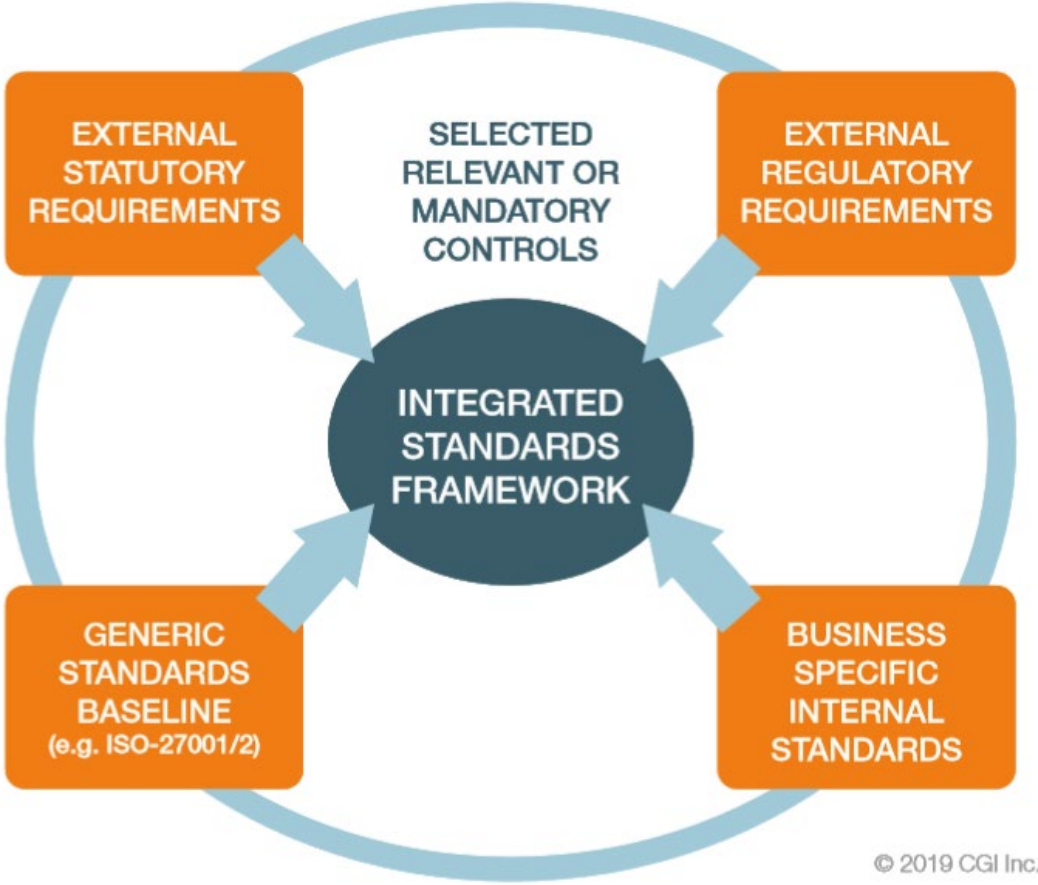
The following are the minimum content requirements for a typical standards document. Bear in mind the need for both clarity and conciseness in each area:

- Catalogue or tracking number of the standard.
- Effective date.
- Approving authority. This should be an executive authority.
- Key references. This should include associated policies.
- Purpose. This is the purpose for which the standard is created.
- Objectives. These are the outcomes that the standard is intended to achieve.
- Scope. Defines what is within the scope of the standard and what is beyond its scope.
- Roles and responsibilities. These assignments can be expressed as a RACI (Responsible, Accountable, Consulted and Informed) matrix. It is important to know who is responsible for what parts of the implementation and who has overall accountability for the standard.
- Requirements. This is the core of the standard. It must include a clear description of what is to be achieved to satisfy the standard. Requirements can include more than one objective and are often referred to as “control objectives.” Any implementation constraints and limitations should also be described.
- Compliance & audit. Describes how the standard is to be monitored and enforced.
- Exception management. Describes the process by which exceptions to the standard are to be approved and by whom.
- Dependencies. Describes related standards upon which there is a dependency. As an example, an Access Control standard may have a dependency on a separate standard for User Authentication or Privilege Management.
- Related external controls. A mapping or cross-reference to external controls or regulatory requirements that are related to this standard.
- Maintenance of the standard. Describes when or how often the standard is to be reviewed and updated and by whom. A revision table should also be provided.

The following is optional, but should be considered to facilitate testing and auditing:

- Testing and audit method. A description of how the effectiveness of the standard (or its integral control objectives) should be tested or compliance with the standard should be measured; this may consist of a brief description of specific tests or audit actions that will demonstrate compliance (see Measuring standard compliance).

Recommendation how to establish a framework



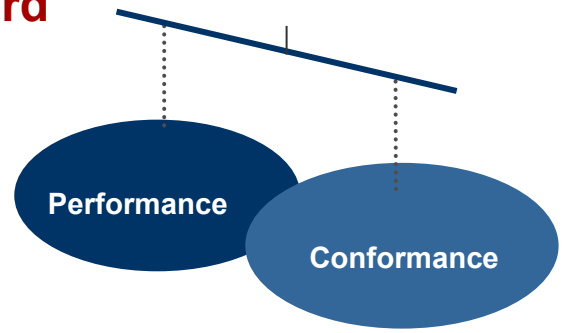
An enterprise should identify all obligatory security and cybersecurity (regulatory) requirements and controls with which it must comply, and build them into a single, integrated enterprise cybersecurity standards framework.

Source: https://www.cgi.com/sites/default/files/2019-08/cgi-understanding-cybersecurity-standards-white-paper.pdf

IT Governance is part of Corporate Governance!

ISO/IEC 38500:2008

Corporate Governance and IT Governance require a balance between conformance and performance goals directed by the board



Conformance -- Adhering to legislation, internal policies, audit requirements, etc.

Performance -- Improving profitability, efficiency, effectiveness, growth, etc.

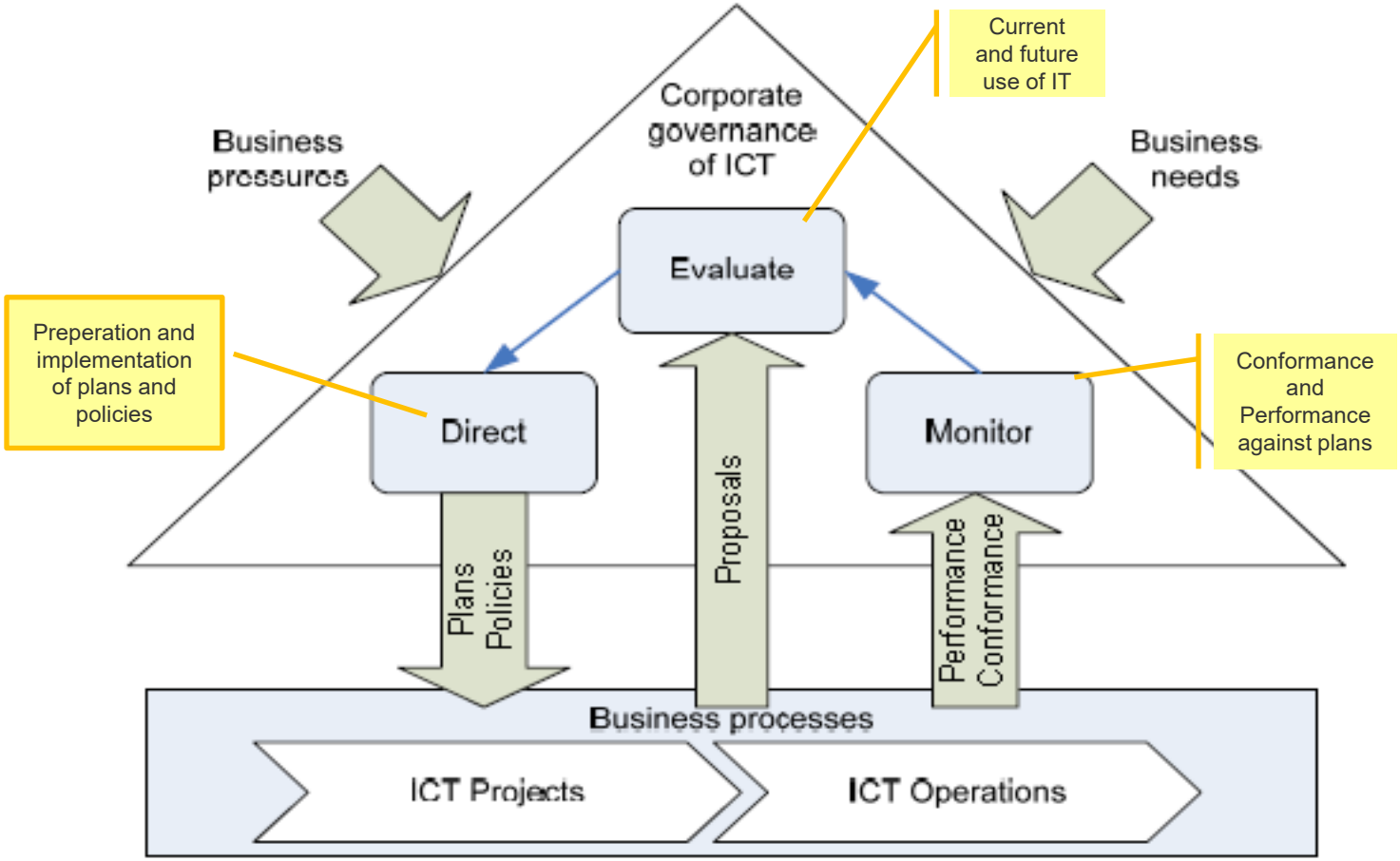
Six principles:

1. **Responsibility**: Responsibility for effective, efficient and acceptable use of IT should be clearly and appropriately allocated and fully understood by all. Business managers should be responsible for business use and performance, including successful outcomes of projects where IT is a major enabling investment.
2. **Strategy**: Business planning should consider and define direction for IT from the highest level, thus providing the basis for proper alignment of IT activity with business requirements.
3. **Acquisition**: Decisions to invest in, and to continue spending on, IT should be made by fully considering the factors that will determine success. These factors go well beyond the basic business case and include the capacity of the organisation to absorb and manage change, the capability of the IT supplier (whether internal or external) to deliver the required services, the feasibility of the required technology solution and the organisation's appetite for risk.
4. **Performance**: Demand for IT service and capability in both current operations and development of new business systems should be moderated in respect of the overall business plan and balanced against the organisation's capacity to obtain or deliver the required service and resources.
5. **Conformance**: All rules, whether external or internal, regarding the use of IT should be formally identified, clearly communicated and appropriately enforced.
6. **Human Behaviour**: Characteristics and the needs of the people in the process (those who plan, control, deliver, implement, operate, use or are otherwise affected by an organisation's decisions regarding the use of IT) should be taken into account in all aspects of planning and using IT.

ISO/IEC 38500:2008 -- https://www.iso.org/standard/62816.html

Model for Corporate Governance of IT

ISO/IEC 38500:2008



Governance view

Management view

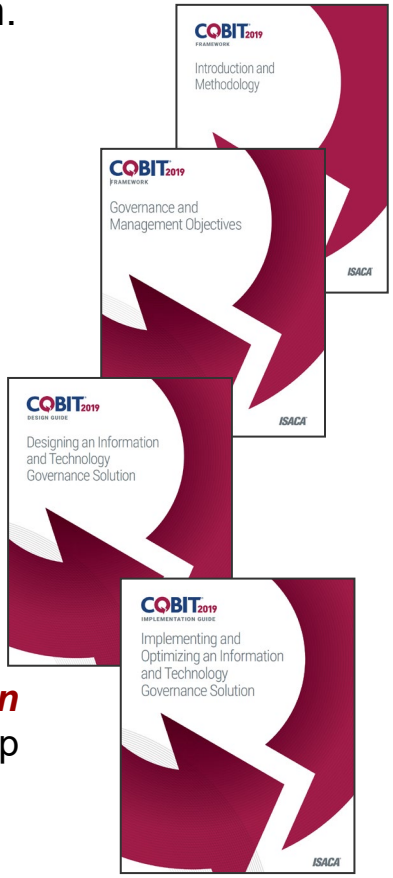
ISO/IEC 38500:2008 -- https://www.iso.org/standard/62816.html

Source: ISACA -- COBIT® 2019, overview 2019 ISACA®

Some Literature – provided from ISACA

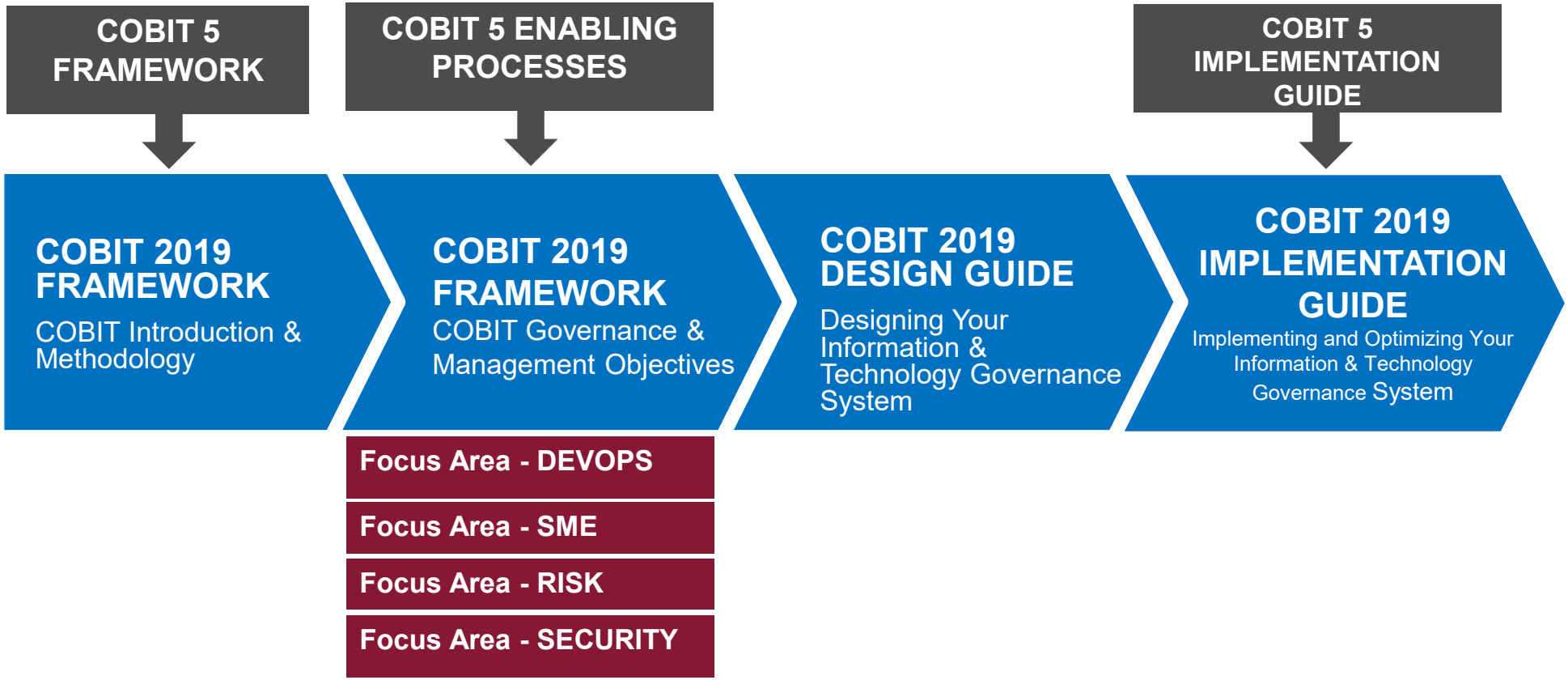
The COBIT® 2019 product family is open-ended and designed for customization.

- ***COBIT® 2019 Framework:***
  Introduction and Methodology introduces the key concepts of COBIT® 2019.
- ***COBIT® 2019 Framework:***
  Governance and Management Objectives comprehensively describes the 40 core governance and management objectives, the processes contained therein, and other related components. This guide also references other standards and frameworks.
- ***COBIT® 2019 Design Guide:***
  Designing an Information and Technology Governance Solution explores design factors that can influence governance and includes a workflow for planning a tailored governance system for the enterprise.
- ***COBIT® 2019 Implementation Guide:***
  Implementing and Optimizing an Information and Technology Governance Solution represents an evolution of the *COBIT® 5 Implementation* guide and develops a road map continuous governance improvement. It may be used in combination with the *COBIT® 2019 Design Guide.*



Have a Look on the ISACA website: https://www.isaca.org/resources/cobit

COBIT 2019 – Overview Products

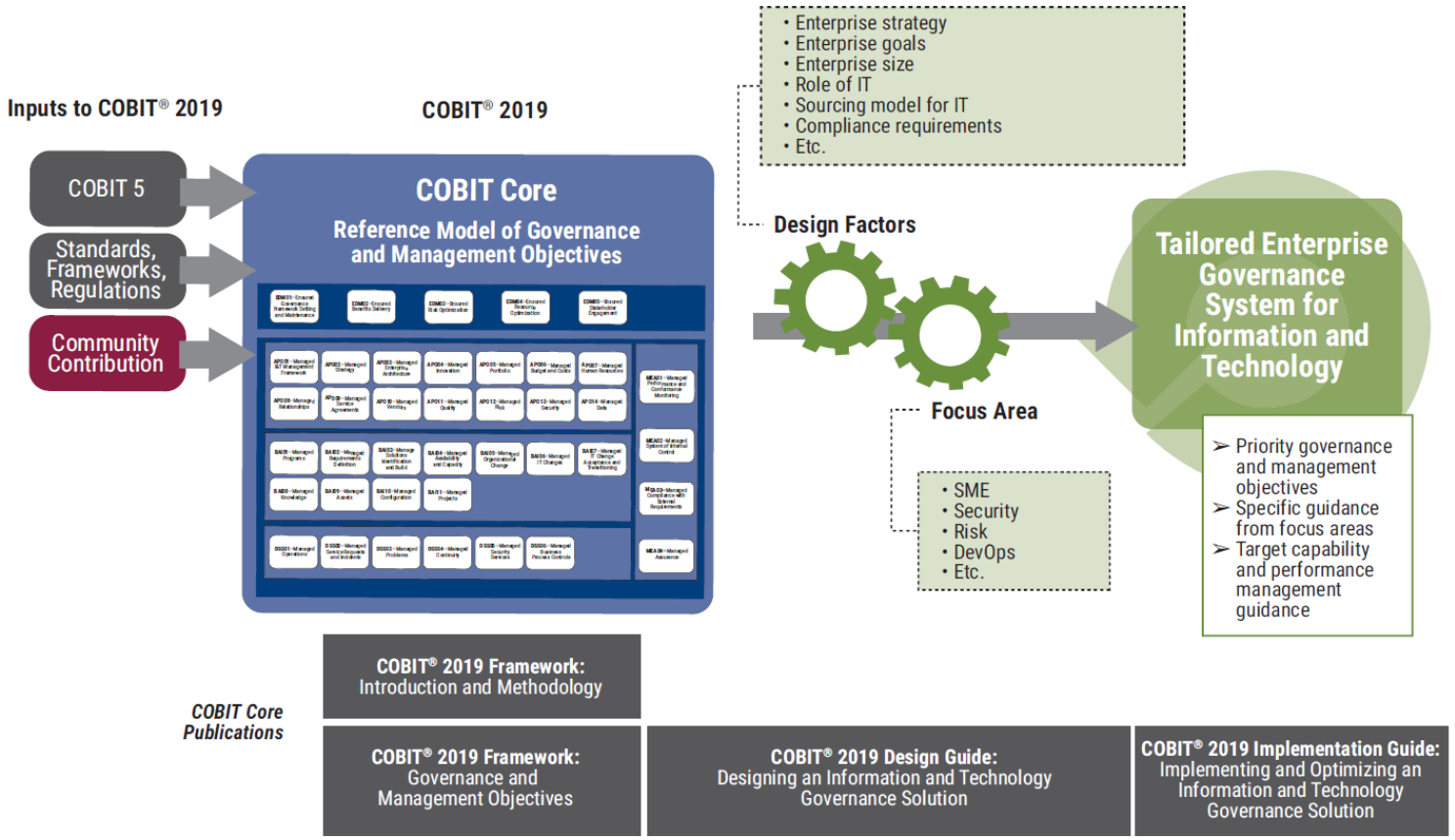


Source: COBIT® 2019, overview 2019 ISACA®

COBIT 2019 – Overview Content

COBIT 2019

Figure 1.1—COBIT Overview



Source: COBIT® 2019, overview 2019 ISACA®

COBIT 2019 – What is COBIT and what is it not …

COBIT IS

- A framework for the governance and management of enterprise IT
- COBIT defines the components to build and sustain a g system
- COBIT defines the design factors that should be considered by the enterprise to build a best fit governance system
- COBIT is flexible and allows guidance on new topics to be added

COBIT IS NOT

- A full description of the whole IT environment of an enterprise
- A framework to organize business processes
- An (IT-) technical framework to manage all technology
- COBIT does not make o prescribe any IT-related decisions

Source: COBIT® 2019, overview 2019 ISACA®

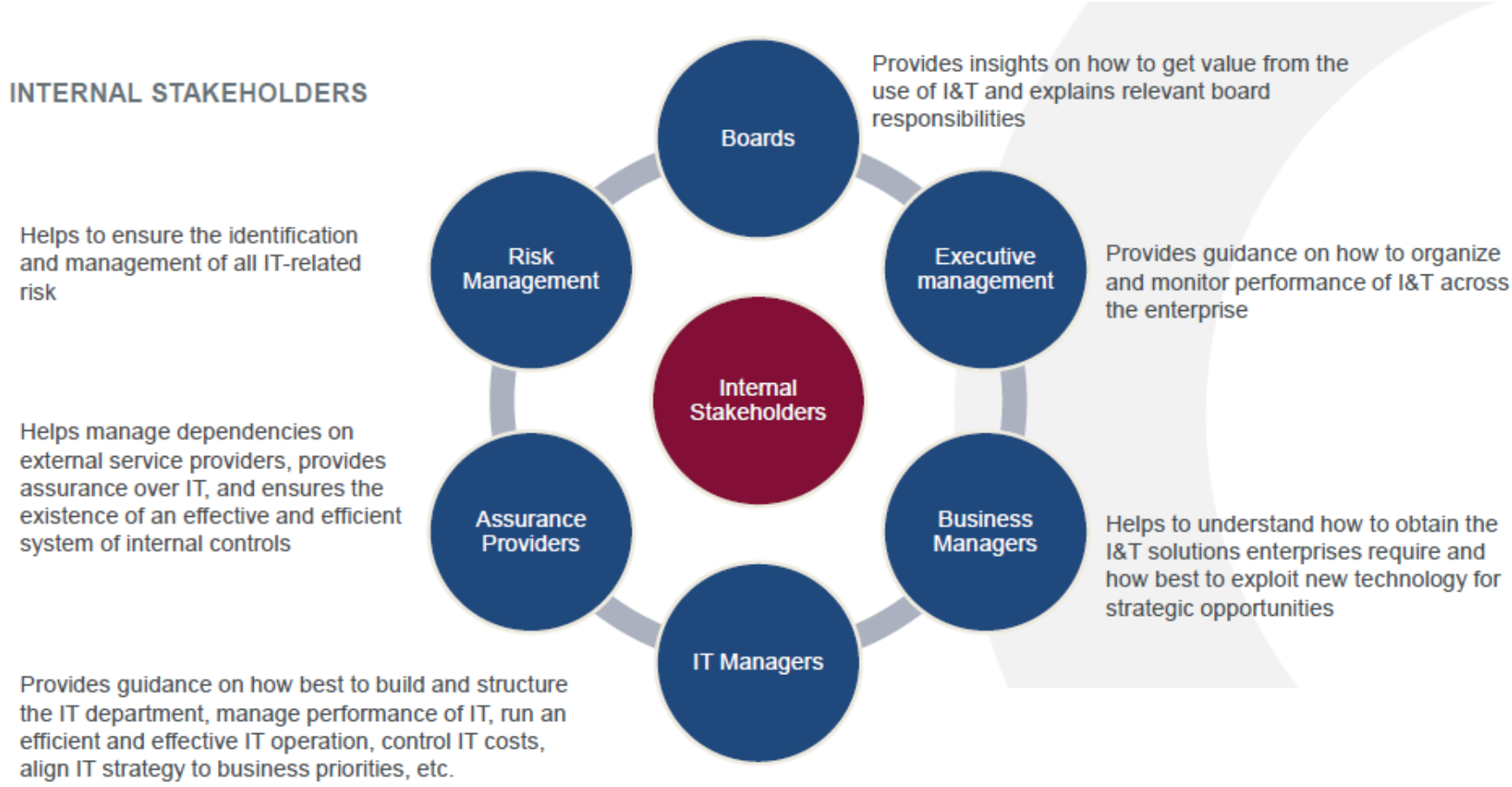
COBIT 2019 – Aligned standards …

- US National Institute of Standards and Technology (NIST) standards:
  - NIST Cybersecurity Framework v1.1
  - NIST SP 800 53 Rev 5
  - NIST SP 800 37 Rev 2 (Risk Management Framework)
- ISO/IEC 20000
- ISO/IEC 27000 family:
  - ISO/IEC 27001
  - ISO/IEC 27002
  - ISO/IEC 27004
  - ISO/IEC 27005
- ISO/IEC 31000:2018
- ISO/IEC 38500
- ISO/IEC 38502
- A Guide to the Project Management Book of Knowledge: PMBOK® Guide, Sixth Edition, 2017
- The TOGAF® Standard, The Open Group
- The Open Group IT4IT™ Reference Architecture, version 2.0
- CIS® Critical Security Controls, Center for Internet Security
- King IV Report on Corporate Governance™, 2016
- Scaled Agile Framework (SAFe®)
- Cloud standards and good practices:
  - Amazon Web Services (AWS®)
  - Security Considerations for Cloud Computing, ISACA
  - Controls and Assurance in the Cloud: Using COBIT® 5, ISACA
- Enterprise Risk Management (ERM)—Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO), June 2017
- The TBM Taxonomy, The TBM Council
- "Options for Transforming the IT Function Using Bimodal IT," MIS Quarterly Executive (white paper)
- ITIL V3
- HITRUST® Common Security Framework, version 9, September 2017
- Change Management Methodology, Prosci
- Skills Framework for the Information Age (SFIA®) V6
- The Standard of Good Practice for Information Security, Information Security Forum (ISF), 2016
- CMMI V2.0
- The CMMI Cybermaturity Platform, 2018
- The Data Management Maturity Model, CMMI Institute, 2014

Source: COBIT® 2019, toolkit 2019 ISACA®

COBIT 2019

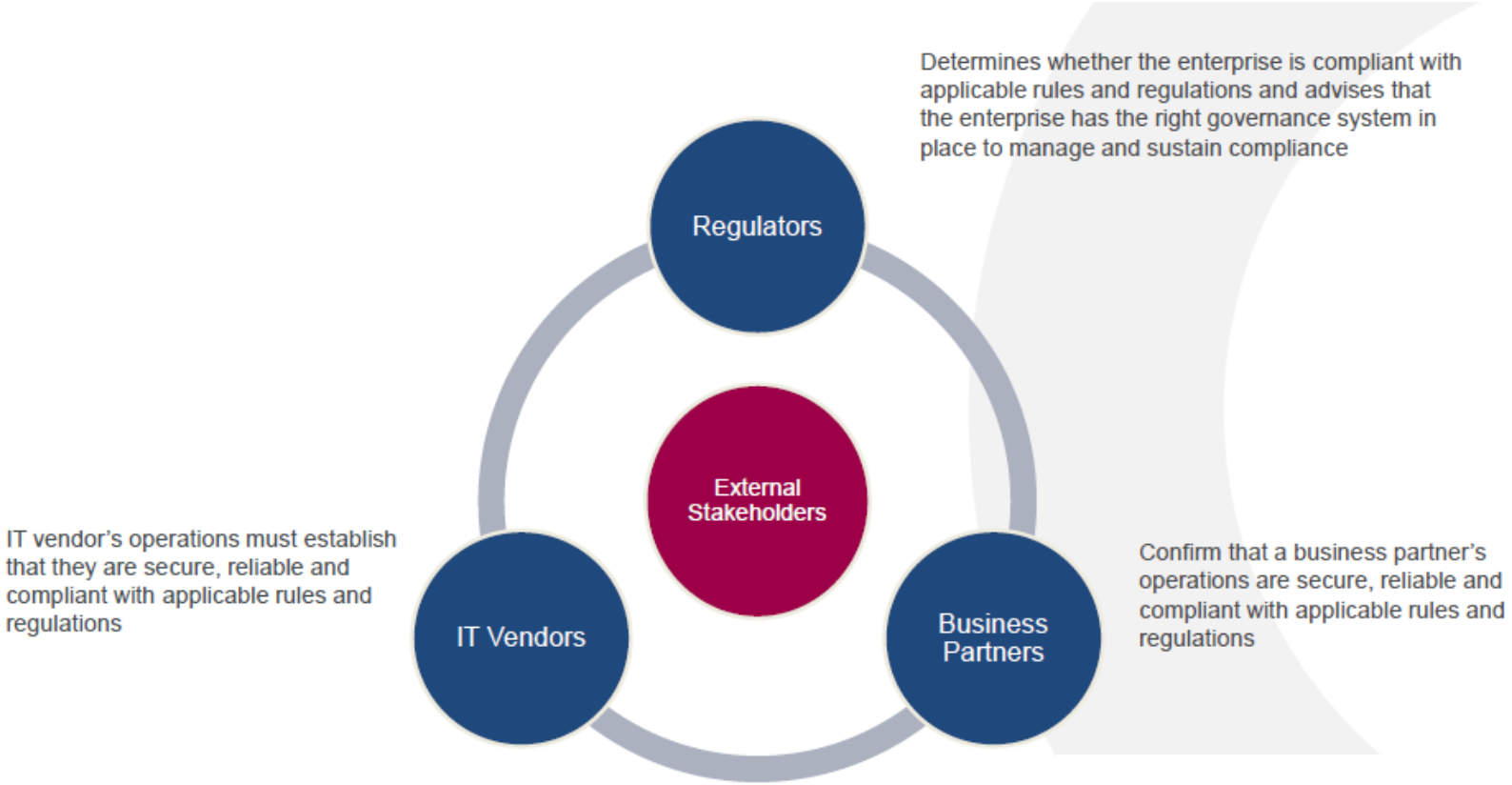
Internal Stakeholders …



Source: COBIT® 2019, overview 2019 ISACA®

COBIT 2019

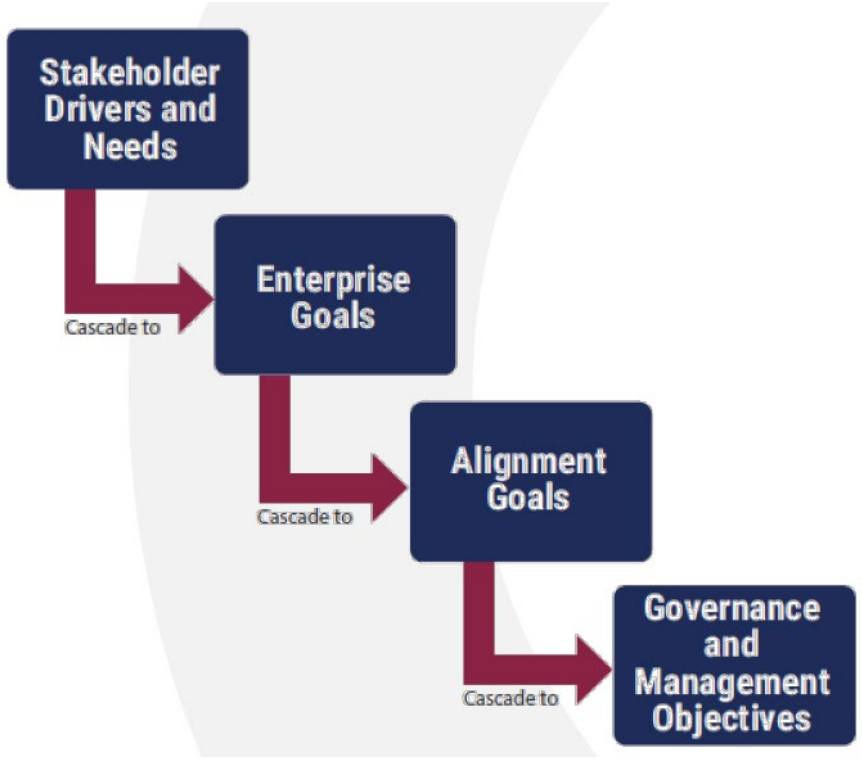
External Stakeholders …



Source: COBIT® 2019, overview 2019 ISACA®

COBIT 2019

Goals Cascade …

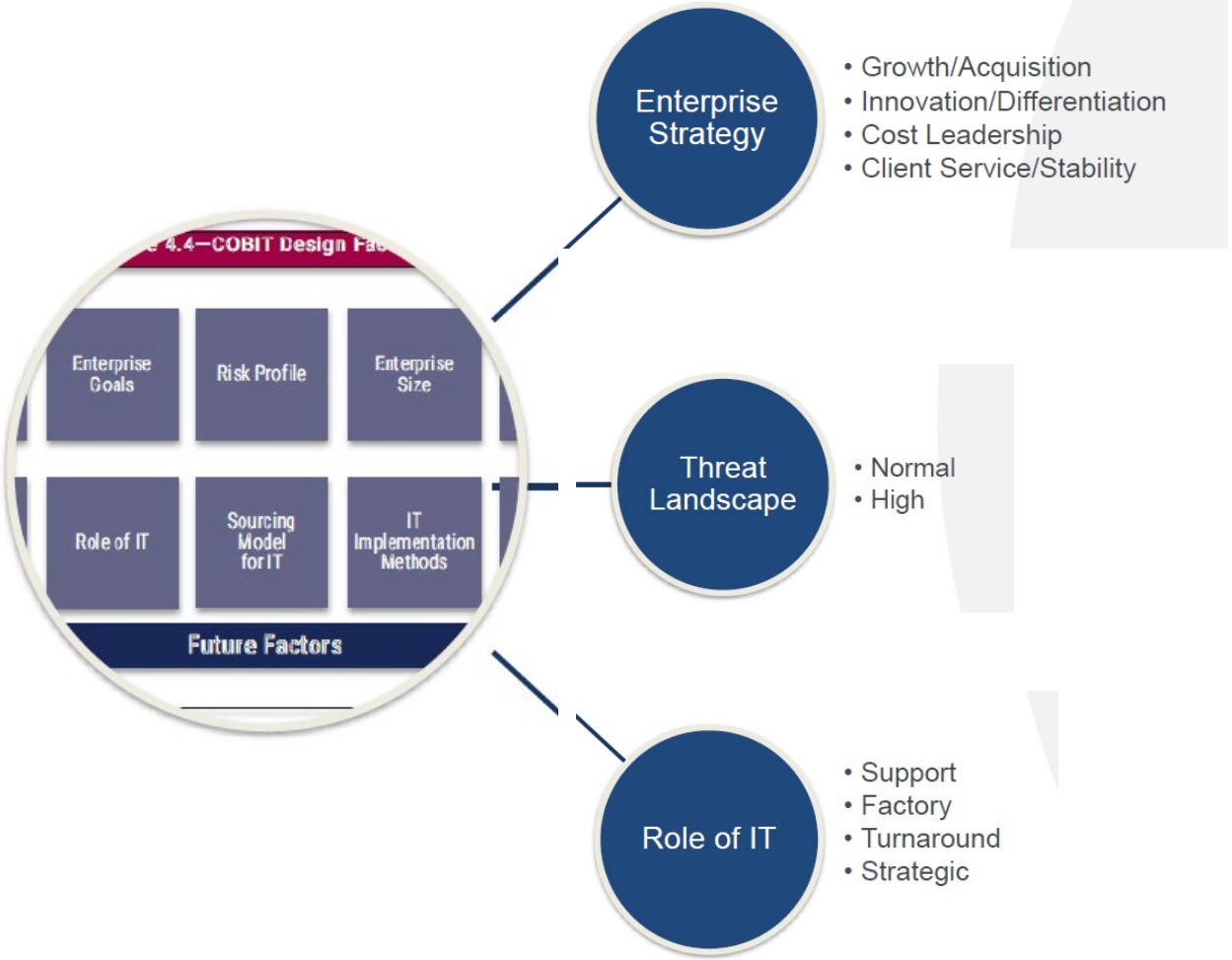


- Enterprise goals have been consolidated, reduced, updated and clarified.
- Alignment goals emphasize the alignment of all IT efforts with business objectives
  - These were IT-related goals in COBIT 5
  - The update seeks to avoid the frequent misunderstanding that these goals indicate purely internal objectives of the IT department within an enterprise
  - Alignment goals have also been consolidated, reduced, updated and clarified where necessary

Source: COBIT® 2019 Framework: Introduction and Meth
Governance Systems and Components, Figure 4.16

COBIT 2019

Design Factors …



Source: COBIT® 2019, overview 2019 ISACA®

COBIT 2019 – Core Model

Reference Model of Governance and Management Objectives
40 processes of relevance!

Figure 4.2—COBIT Core Model

Domain: Align, Plan and Organize Management Objective: APO13 – Managed Security	Focus Area: COBIT Core Model
Description	
Define, operate and monitor an information security management system.	
Purpose	
Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.	
The management objective supports the achievement of a set of primary enterprise and alignment goals:	
Enterprise Goals	**Alignment Goals**
• EG02 Managed business risk • EG06 Business service continuity and availability	AG07 Security of information, processing infrastructure and applications, and privacy
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG02 a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG07 a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment
EG06 a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets	

A. Component: Process	
Management Practice	**Example Metrics**
APO13.01 Establish and maintain an information security management system (ISMS). Establish and maintain an information security management system (ISMS) that provides a standard, formal and continuous approach to information security management, enabling secure technology and business processes that are aligned with business requirements.	a. Level of stakeholder satisfaction with the security plan throughout the enterprise
Activities	**Capability Level**
1. Define the scope and boundaries of the information security management system (ISMS) in terms of the characteristics of the enterprise, the organization, its location, assets and technology. Include details of, and justification for, any exclusions from the scope.	2
2. Define an ISMS in accordance with enterprise policy and the context in which the enterprise operates.	
3. Align the ISMS with the overall enterprise approach to the management of security.	
4. Obtain management authorization to implement and operate or change the ISMS.	
5. Prepare and maintain a statement of applicability that describes the scope of the ISMS.	
6. Define and communicate Information security management roles and responsibilities.	
7. Communicate the ISMS approach.	

COBIT 2019

COBIT 2019 – APO13 Manage Security

APO13 -- 1/5

Source: COBIT® 2019 Framework: Governance and Management Objectives

A. Component: Process (cont.)	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	0.01 Information Security Management program
ISO/IEC 20000-1:2011(E)	6.6 Information security management
ITIL V3, 2011	Service Design, 4.7 Information Security Management
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.3 Selection (Task 1); 3.4 Implementation (Task 1)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-2)
Management Practice	**Example Metrics**
APO13.02 Define and manage an information security and privacy risk treatment plan. Maintain an information security plan that describes how information security risk is to be managed and aligned with enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases, implemented as an integral part of services and solutions development, and operated as an integral part of business operation.	a. Percentage of successful security risk scenario simulations b. Number of employees who have successfully completed information security awareness training

Activities	Capability Level
1. Formulate and maintain an information security risk treatment plan aligned with strategic objectives and the enterprise architecture. Ensure that the plan identifies the appropriate and optimal management practices and security solutions, with associated resources, responsibilities and priorities for managing identified information security risk.	3
2. Maintain as part of the enterprise architecture an inventory of solution components that are in place to manage security-related risk.	
3. Develop proposals to implement the information security risk treatment plan, supported by suitable business cases that include consideration of funding and allocation of roles and responsibilities.	
4. Provide input to the design and development of management practices and solutions selected from the information security risk treatment plan.	
5. Implement information security and privacy training and awareness programs.	
6. Integrate the planning, design, implementation and monitoring of information security and privacy procedures and other controls capable of enabling prompt prevention, detection of security events, and response to security incidents.	
7. Define how to measure the effectiveness of the selected management practices. Specify how these measurements are to be used to assess effectiveness to produce comparable and reproducible results.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	
Management Practice	**Example Metrics**
APO13.03 Monitor and review the information security management system (ISMS). Maintain and regularly communicate the need for, and benefits of, continuous improvement in information security. Collect and analyze data about the information security management system (ISMS), and improve its effectiveness. Correct nonconformities to prevent recurrence.	a. Frequency of scheduled security reviews b. Number of findings in regularly scheduled security reviews c. Level of stakeholder satisfaction with the security plan d. Number of security-related incidents caused by failure to adhere to the security plan

COBIT 2019

COBIT 2019 – APO13 Manage Security

APO13 -- 2/5

Source: COBIT® 2019 Framework: Governance and Management Objectives

COBIT 2019

COBIT 2019 – APO13 Manage Security

APO13 -- 3/5

A. Component: Process (cont.)	
Activities	**Capability Level**
1. Undertake regular reviews of the effectiveness of the ISMS. Include meeting ISMS policy and objectives and reviewing security and privacy practices.	4
2. Conduct ISMS audits at planned intervals.	
3. Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified.	
4. Record actions and events that could have an impact on the effectiveness or performance of the ISMS.	
5. Provide input to the maintenance of the security plans to take into account the findings of monitoring and reviewing activities.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.3 Selection (Task 3)

B. Component: Organizational Structures															
Key Management Practice	Chief Information Officer	Chief Technology Officer	Enterprise Risk Committee	Chief Information Security Officer	Business Process Owners	Project Management Office	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO13.01 Establish and maintain an information security management system (ISMS).	R		R	A						R		R		
APO13.02 Define and manage an information security and privacy risk treatment plan.	R		R	A						R		R		R
APO13.03 Monitor and review the information security management system (ISMS).	R	R		A	R	R	R	R	R	R	R	R	R	R
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**													
ISF, The Standard of Good Practice for Information Security 2016	SG1.2 Security Direction													
ISO/IEC 27002:2013/Cor.2:2015(E)	6.1 Internal organization													

Source: COBIT® 2019 Framework: Governance and Management Objectives

COBIT 2019

COBIT 2019 – APO13 Manage Security

APO13 -- 4/5

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
APO13.01 Establish and maintain an information security management system (ISMS).	Outside COBIT	Enterprise security approach	ISMS scope statement	APO01.05; DSS06.03
			ISMS policy	Internal
APO13.02 Define and manage an information security risk treatment plan.	APO02.04	Gaps and changes required to realize target capability	Information security risk treatment plan	All APO; All BAI; All DSS; All MEA; ALL EDM
	APO03.02	Baseline domain descriptions and architecture definition	Information security business cases	APO05.02
	APO12.05	Project proposals for reducing risk		

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	Inputs		Outputs	
	From	Description	Description	To
APO13.03 Monitor and review the information security management system (ISMS).	DSS02.02	Classified and prioritized incidents and service requests	Recommendations for improving the information security management system (ISMS)	Internal
			Information security management system (ISMS) audit reports	MEA02.01

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.3 Selection (Tasks 1, 3): Inputs and Outputs; 3.4 Implementation (Task 1): Inputs and Outputs

Source: COBIT® 2019 Framework: Governance and Management Objectives

COBIT 2019

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Information security	Skills Framework for the Information Age V6, 2015	SCTY
Information security strategy development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	D. Enable—D.1. Information Security Strategy Development

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Information security and privacy policy	Sets behavioral guidelines to protect corporate information, systems and infrastructure. Given that business requirements regarding security and storage are more dynamic than I&T risk management and privacy, their governance should be handled separately from that of I&T risk and privacy. For operational efficiency, synchronize information security policy with I&T risk and privacy policy.	(1) ISO/IEC 27001:2013/ Cor.2:2015(E); (2) ISO/IEC 27002:2013/Cor.2:2015(E); (3) National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017; (4) HITRUST CSF version 9, September 2017; (5) ISF, The Standard of Good Practice for Information Security 2016	(1) 5.2 Policy; (2) 5. Information security policies; (3) 3.2 Awareness and training (AT-1); (4) 04.01 Information Security Policy; (5) SM1.1 Information Security Policy

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Establish a culture of security and privacy awareness that positively influences desirable behavior and actual implementation of security and privacy policy in daily practice. Provide sufficient security and privacy guidance, indicate security and privacy champions (including C-level executives, leaders in HR, and security and/or privacy professionals) and proactively support and communicate security and privacy programs, innovations and challenges.	(1) ISO/IEC 27001:2013/ Cor.2:2015(E); (2) Creating a Culture of Security, ISACA, 2011	1) 7.3 Awareness; (2) Framework to achieve an intentional security aware culture (all chapters)

G. Component: Services, Infrastructure and Applications
• Configuration management tools • Security and privacy awareness services • Third-party security assessment services

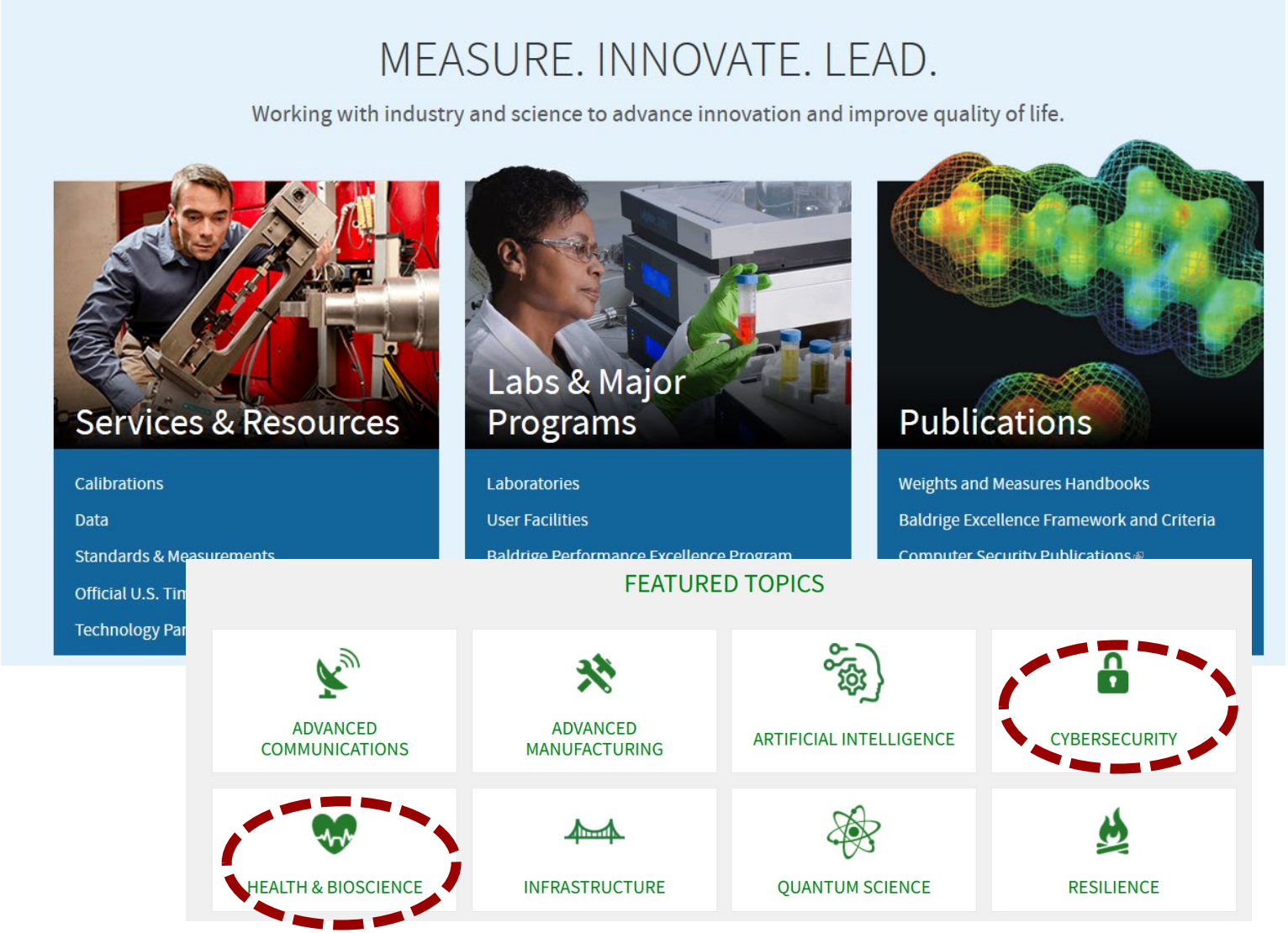
COBIT 2019 – APO13 Manage Security

APO13 -- 5/5

Source: COBIT® 2019 Framework: Governance and Management Objectives

Have a Look: https://www.nist.gov/topics/cybersecurity

NIST – a Leading Organization *www.nist.gov*



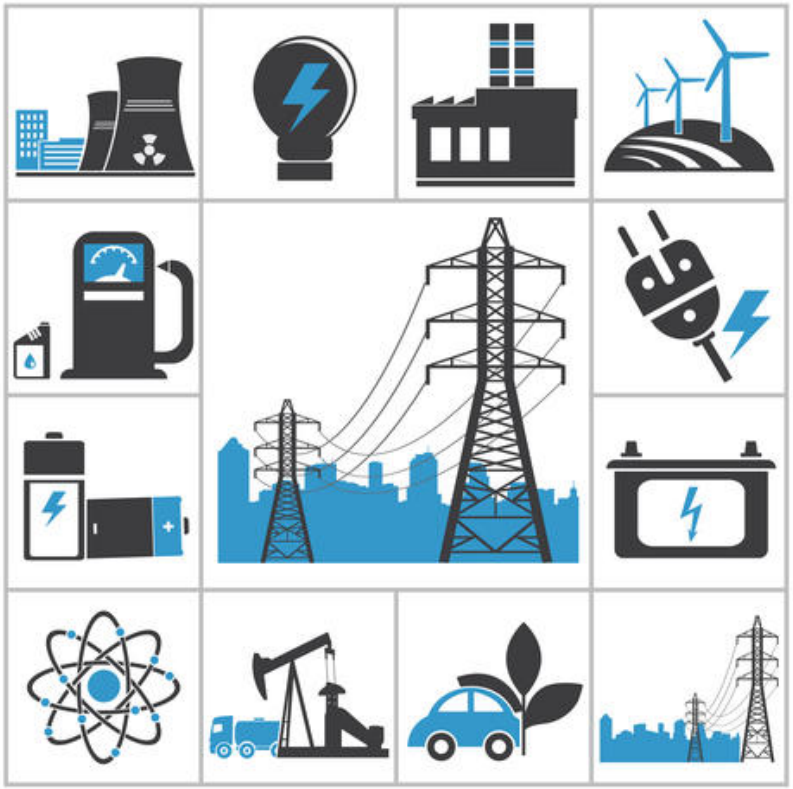
Note:

NIST provides many materials in different fields and technologies.

Innumerable products and services rely in some way on technology, measurement, and standards provided by the NIST.

(Only) one of their featured topics are ‘Cybersecurity».

NIST – Who should use the Framework?



https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework

The Cybersecurity Framework is for organizations of all sizes, sectors, and maturities.

Note:

While the Framework was designed with **Critical Infrastructure** (CI) in mind, it is extremely versatile and can be used by organizations regardless of sector or size.

With built-in customization mechanisms (Tiers, Profiles, and Core are all modifiable), the Framework can be customized for use by any type of organization.

Because the Framework is outcome driven and does not mandate how an organization must achieve those outcomes, it enables scalability.

A small organization with a low cybersecurity budget, or a large corporation with a big budget, are each able to approach the outcome in a way that is feasible for them.

Have a look:
www.nist.gov/cyberframework/new-framework

NIST - Cybersecurity

www.nist.gov/cyberframework/framework

CYBERSECURITY FRAMEWORK

- Framework
  - Version 1.1 (PDF)
  - Version 1.1 (Excel)
- New to Framework
- Perspectives
- Success Stories
- Online Learning
- Evolution
- Frequently Asked Questions
- Events and Presentations
- Related Efforts (Roadmap)
- Informative References
- Resources
- Newsroom
- Related Programs

Study current website material

Framework Documents

Cybersecurity Framework Version 1.1

(April 2018)

- Letter to Stakeholders
- Framework V1.1 (PDF)
- Framework V1.1 (PDF) with markup
- Framework V1.1 Core (Excel)
- Framework V1.1 Downloadable Presentation

Translations

- Arabic Translation of the NIST Cybersecurity Framework V1.1
  (Translated by Ali A. AlHasan, PMP, CISSP,CISA, CGEIT, CRISC, CISM and Ali AlHajj. Reviewed by Schreiber Translations, INC (STI). Not an official U.S. Government translation.)
- Japanese Translation of the NIST Cybersecurity Framework V1.1 (Page not in English)
  (This is a direct translation of Version 1.1 of the Cybersecurity Framework produced by the Japan Information-technology Promotion Agency (IPA).)

ortuguese Translation of the NIST Cybersecurity Framework V1.1
ranslated courtesy of the US Chamber of Commerce and the Brazil-US Business Council. Not an official U.S. Government anslation.)

panish Translation of the NIST Cybersecurity Framework V1.1
he Spanish language Cybersecurity Framework Version 1.1 was translated under government contract.)

NIST - Key Framework Attributes

www.nist.gov/cyberframework/framework

Function
Identify
Protect
Detect
Respond
Recover

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector

NIST – What is the Framework, and what is it designed to accomplish?

The Framework is a voluntary guidance, based on existing standards, guidelines, and practices, for **critical infrastructure organizations** to better manage and reduce cybersecurity risk.

In addition to helping organizations **manage and reduce risks**, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

The framework core and informative requirements are available as separate downloads in three formats: spreadsheet (Excel), alternate view (PDF) , and database (FileMaker Pro).

A companion Roadmap discusses future steps and identifies key areas of cybersecurity development, alignment, and collaboration.

https://www.nist.gov/cyberframework/question-and-answer-pairs#framework

Note:
Main aspects you should know about NIST:

- voluntary guidance
- Developed critical infrastructure organizations , but nevertheless all organizations can establish it
- based on existing standards, guidelines, and practices
- Designed to help organizations to manage and reduce cyber risks
- The framework core and informative requirements are available for free on the NIST website.

NIST – Framework for Improving Critical Infrastructure Cybersecurity

Note: this version 1.1 is available on moodle

Table of Contents

List of Figures

List of Tables

Current Version 1.1
April 16, 2018

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST – Framework Core

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

https://www.nist.gov/cyberframework/online-learning/components-framework

NIST – Tiers

	1	2	3	4
	Partial	**Risk Informed**	**Repeatable**	**Adaptive**
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization: • **monitors and manages supply chain risk**[1.1] • benefits my sharing or receiving information from outside parties			

https://www.nist.gov/cyberframework/online-learning/components-framework

Note:

Tiers do not represent maturity levels.

Organizations should determine the desired Tier, ensuring that the selected level meets organizational goals to reduce cyber risks to levels acceptable to the organization, and is feasible to implement, fiscally and otherwise.

Tiers describe the degree to which an organization's cybersecurity risk management practices. The Tiers range from **Partial (Tier 1)** to **Adaptive (Tier 4**) and describe an increasing degree of rigor, and how well integrated cybersecurity risk decisions are into broader risk decisions, and the degree to which the organization shares and receives cybersecurity info from external parties.

NIST – Watch the Informational Videos

Watch the video

https://www.nist.gov/video/cybersecurity-framework-version-11-overview (1:00:07)

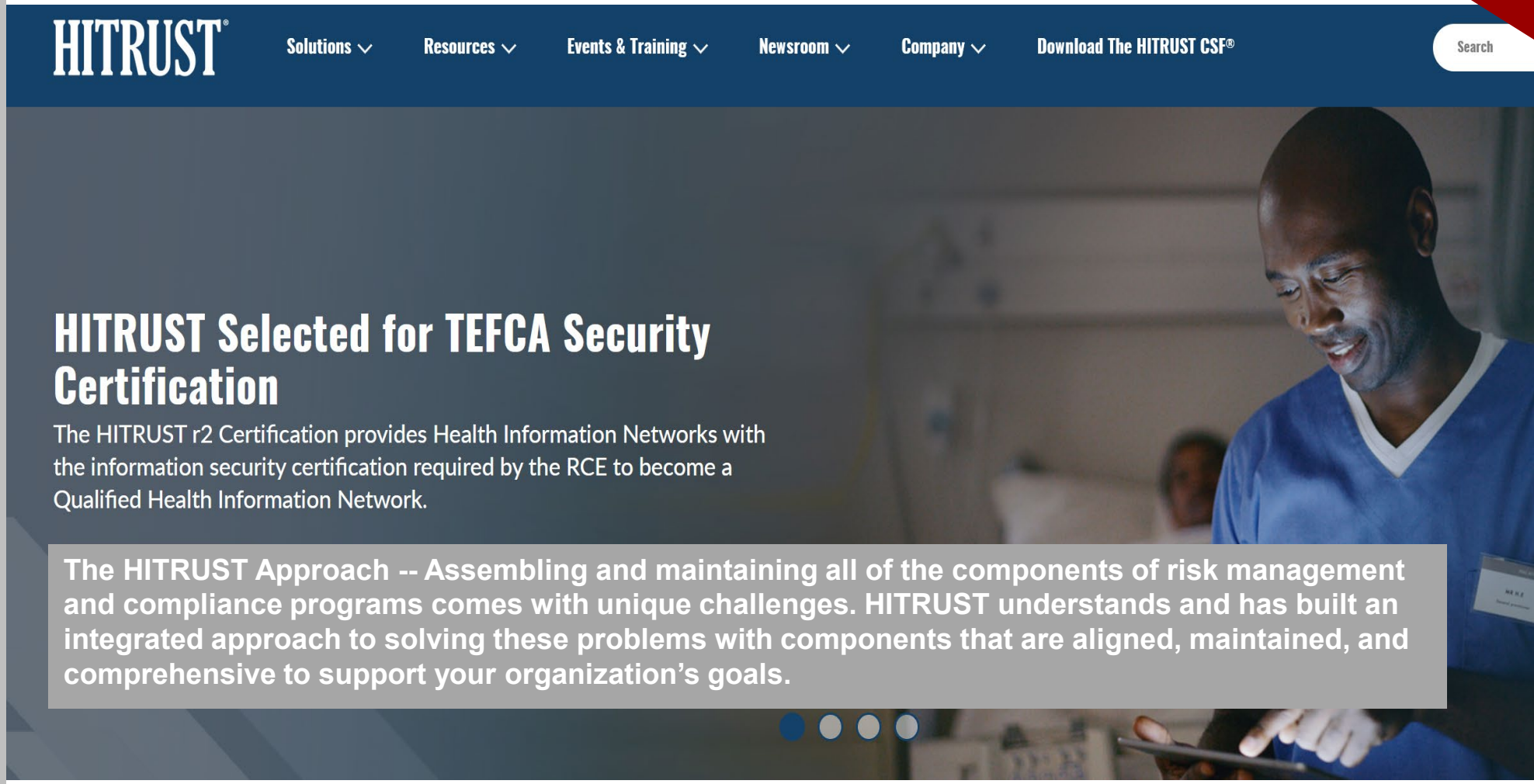
Watch the video

https://www.nist.gov/video/cybersecurity-framework-shared-0 (1:40)

Watch the video

https://www.nist.gov/video/cybersecurity-framework-0 (4:35)

Add-on



Have a Look: https://hitrustalliance.net/

HITRUST CSF

Add-on

a framework that covers many healthcare standards and regulations

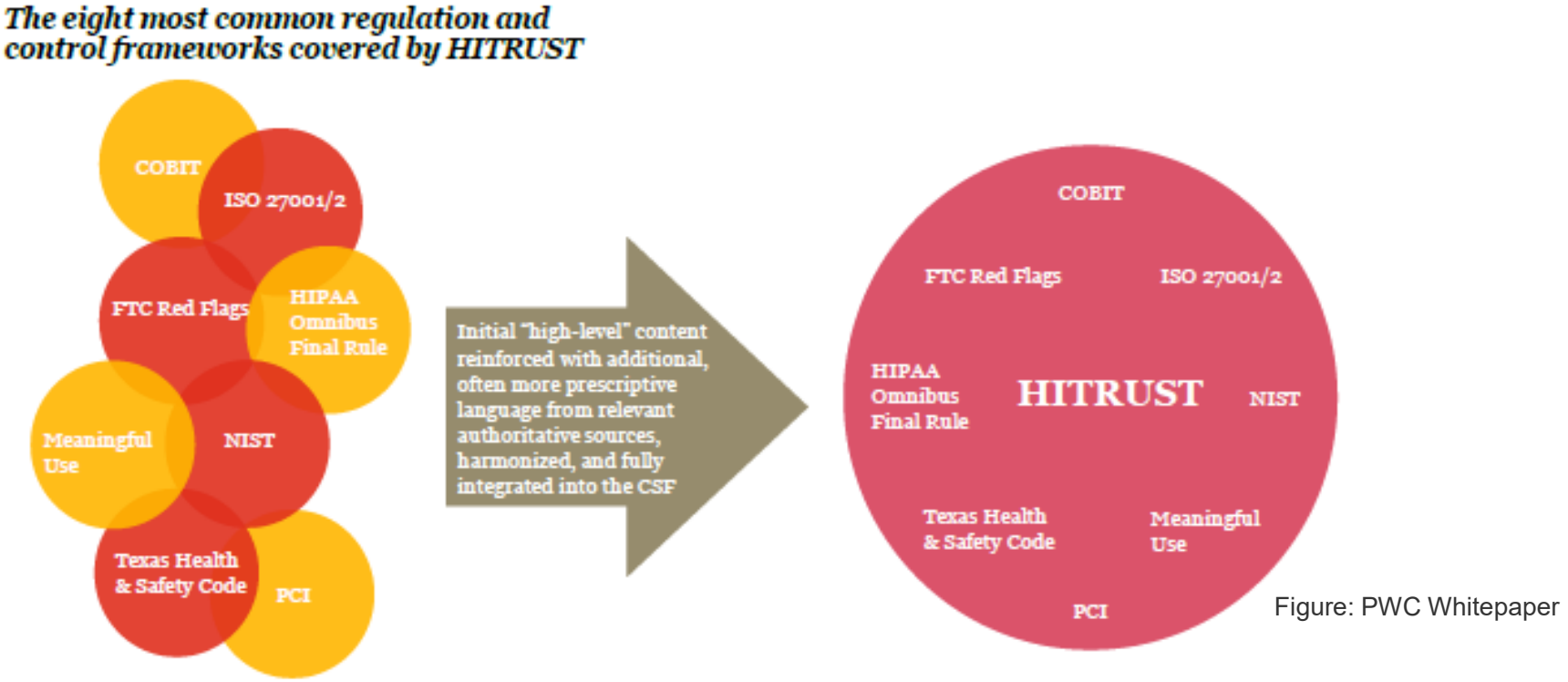


Figure: PWC Whitepaper

The HITRUST CSF is a framework that normalizes security and privacy requirements for organizations, including federal legislation (e.g., HIPAA), federal agency rules and guidance (e.g., NIST), state legislation (e.g., California Consumer Privacy Act), international regulation (e.g., GDPR), and industry frameworks (e.g., PCI, COBIT). It simplifies the myriad of requirements by providing a single-source solution tailored to the organization's needs. The CSF is the only framework built to provide scalable security and privacy requirements based on the different risks and exposures of each unique organization

https://hitrustalliance.net/content/uploads/CSFv9.6.0-Introduction.pdf

HITRUST CSF
Products

HITRUST

Add-on

Designed to leverage the best in class components for a comprehensive information risk management and compliance program.

The HITRUST Approach integrates and aligns the following:

HITRUST CSF®—a robust privacy and security controls framework
HITRUST CSF Assurance Program—a scalable and transparent means to provide reliable assurances to internal and external stakeholders
HITRUST MyCSF®—an assessment and corrective action plan management platform
HITRUST Threat Catalogue™—a list of reasonably anticipated threats mapped to specific CSF controls
HITRUST Assessment XChange™—an automated means of sharing assurances between organizations
HITRUST Shared Responsibility Program—a matrix of CSF requirements identifying service provider and customer responsibilities
HITRUST® Third-Party Assurance Program—a third-party risk management process

Source: (2020) https://hitrustalliance.net/content/uploads/CSFv9.4_Introduction.pdf

HITRUST -- a framework that covers many healthcare standards and regulations

HITRUST

Add-on

A broad base of U.S. federal and international regulations, security and privacy standards and frameworks were used to ensure the HITRUST CSF addresses all areas of data protection governance and control.

The HITRUST CSF integrates and normalizes these different authoritative sources, incorporating key objectives, under one umbrella framework. The CSF v9.4.2 integrates 44 major security and privacy related standards, regulations, and frameworks as the authoritative sources, ensuring appropriate coverage, consistency, and alignment:

- 16 CFR Part 681 –Identity Theft Rules [16 CFR 681]
- 201 CMR 17.00–State of Massachusetts Data Protection Act: Standards for the Protection of Personal Information of Residents of the Commonwealth [201 CMR 17.00]
- American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria: Security, Confidentiality and Availability, 2017 [AICPA TSP 100]
- …
- Cloud Security Alliance (CSA) Cloud Controls Matrix Version 3.0.1[CSA CCM v3.0.1]
- CMS Information Security ARS 2013 v3.1: CMS Minimum Security Requirements for High Impact Data [CMS ARS v3.1]
- COBIT 5: Deliver and Support Sect ion 5 – Ensure Systems Security [COBIT 5]
- Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) version 1.0 [CMMC v1.0]
- …
- HIPAA – Federal Register 45 CFR Part 164, Subpart C: HIPAA Administrative Simplification: Security Standards for the Protection of Electronic Protected Health Information (Security Rule) [45 CFR HIPAA.SR]
- HIPAA – Federal Register 45 CFR Part 164, Subpart D: HIPAA Administrative Simplification: Notification in the Case of Breach of Unsecured Protect ed Health Information (Breach Notification Rule) [45 CFR HIPAA.BN]

… → (next page)

Source: https://hitrustalliance.net/content/uploads/CSFv9.4_Introduction.pdf

HITRUST -- a framework that covers many healthcare standards and regulations

HITRUST

Add-on

- HIPAA – Federal Register 45 CFR Part 164, Subpart E: HIPAA Administrative Simplification: Privacy of Individually
- Identifiable Health Information (Privacy Rule) [45 CFR HIPAA.PR]
- IRS Publication 1075 v2016: Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for protecting Federal Tax Ret urns and Return Information [IRS Pub 1075 (2016)]
- ISO/IEC 27001:2013: Information Technology–Security Techniques–Information Security Management Systems – Requirements [ISO/IEC 27001:2013]
- ISO/IEC 27002:2013: Information Technology Security Techniques Code of Practice for Information Security Controls [ISO/IEC 27002:2013]
- ISO/IEC 27799:2016: Health Informatics –Information Security Management in Health using ISO/IEC 27002 [ISO/IEC 27799:2016]
- ISO/IEC 29100:2011: Information Technology –Security Techniques –Privacy Framework [ISO/IEC 29100:2011]
- ISO/IEC 29151:2017: Information Technology –Security Techniques –Code of Practice for Personally Identifiable Information Protection [ISO/IEC 29151:2017]
- …
- NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1 [NIST Cybersecurity Framework v1.1]
- NIST Special Publication 800-53 Revision 4 (Final), including Appendix J –Privacy Control Catalog: Security Controls for Federal Information Syst ems and Organizations [NIST SP 800-53 R4]
- NIST Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations [NISTSP 800-171 R2]
- …

Source: https://hitrustalliance.net/content/uploads/CSFv9.4_Introduction.pdf

HITRUST CSF

Key Components

HITRUST

Add-on

The CSF contains **14 control categories**, comprised of **49 control objectives** and **156 control specifications**.

The CSF control categories, accompanied with their respective number of control objectives and control specifications for each category, are:

0. Information Security Management Program (1, 1)
1. Access Control (7, 25)
2. Human Resources Security (4, 9)
3. Risk Management (1, 4)
4. Security Policy (1, 2)
5. Organization of Information Security (2, 11)
6. Compliance (3, 10)
7. Asset Management (2, 5)
8. Physical and Environmental Security (2, 13)
9. Communications and Operations Management (10, 32)
10. Information Systems Acquisition, Development, and Maintenance (6, 13)
11. Information Security Incident Management (2, 5)
12. Business Continuity Management (1, 5)
13. Privacy Practices (7, 21)

Source: (2020) https://hitrustalliance.net/content/uploads/CSFv9.4_Introduction.pdf

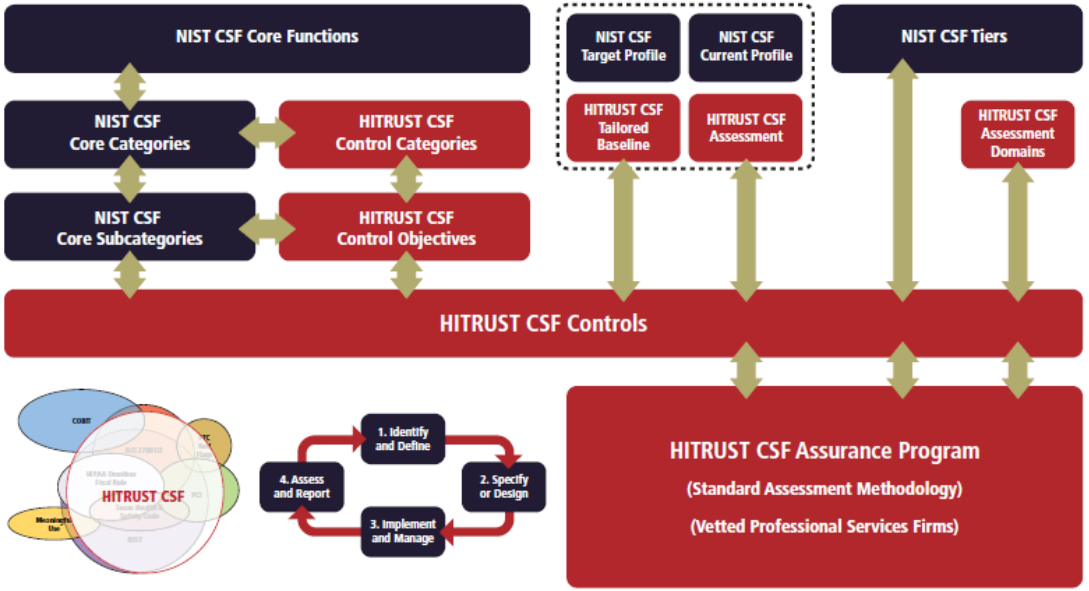
HITRUST

Add-on

A Model Implementation of the NIST Framework

The HITRUST approach meets or exceeds the NIST requirements, fully addresses non-cyber threats, and incorporates a robust assurance program.

- Although scalable, the NIST CSF lacks prescription in:
  - Requirements
  - Assessment methodology
- … and subsequently lacks:
  - Accuracy
  - Transparency
  - Consistency
  - Reliability



The HITRUST CSF provides the foundation needed to implement the NIST Cybersecurity Framework

Source: PWC Whitepaper

What have we discussed so far?

Relevance and positioning of GRCM supporting references/frameworks

Selection criteria of GRCM supporting references/frameworks

ISACA's **COBIT 2019** and its ´family´ resp. related products/books

- Main concepts of COBIT 2019, like separating Governance from Management and how COBIT it interpreted, the core model with its 40 processes, the security process APO13, …

NIST´s Cybersecurity Framework

- Main concepts and its functions, categories and subcategories incl references to other

As Add-on: HITRUST – the (new) Cybersecurity Framework