©ELIA LOCARDI | BLAMETH

PRACTICAL APPROACH ON CYBERSECURITY AUDIT

TAUFIK SN PURBA, CISA, CIA

JAKARTA, DESEMBER 2019

MISSION OF INTERNAL AUDIT

To **enhance** and **protect** organizational value by providing **risk-based** and **objective** assurance, advice, and insight.

The Mission of Internal Audit articulates what internal audit aspires to accomplish within an organization.

Its place in the New IPPF is deliberate, demonstrating how practitioners should leverage the entire framework to facilitate their ability to achieve the Mission.

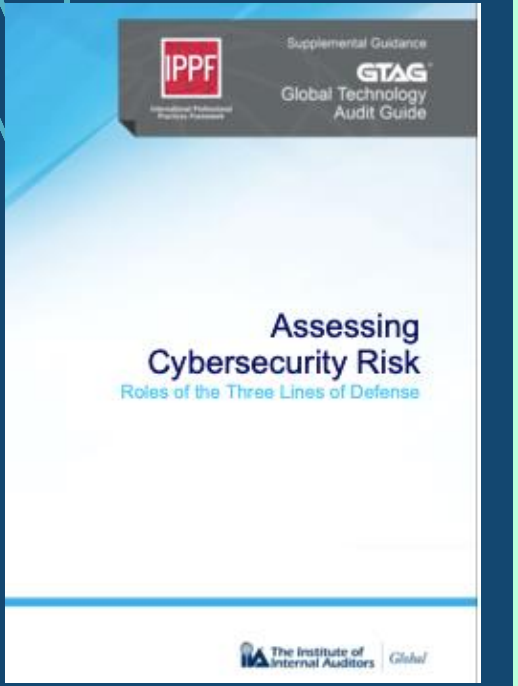
CYBERSECURITY DEFINITION

- Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. - NIST Glossary (https://csrc.nist.gov/glossary/term/cybersecurity)

- The protection of information assets by addressing threats to information processed, stored, and transported by inter-networked information systems – ISACA Glossary (http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf)

- The first known use of cybersecurity was in 1989 – Merriam Webster dictionary

ROLES & RESPONSIBILITIES ON CYBERSECURITY



IPPF

Supplemental Guidance

GTAG
Global Technology
Audit Guide

Assessing
Cybersecurity Risk

Roles of the Three Lines of Defense

The Institute of Internal Auditors | Global

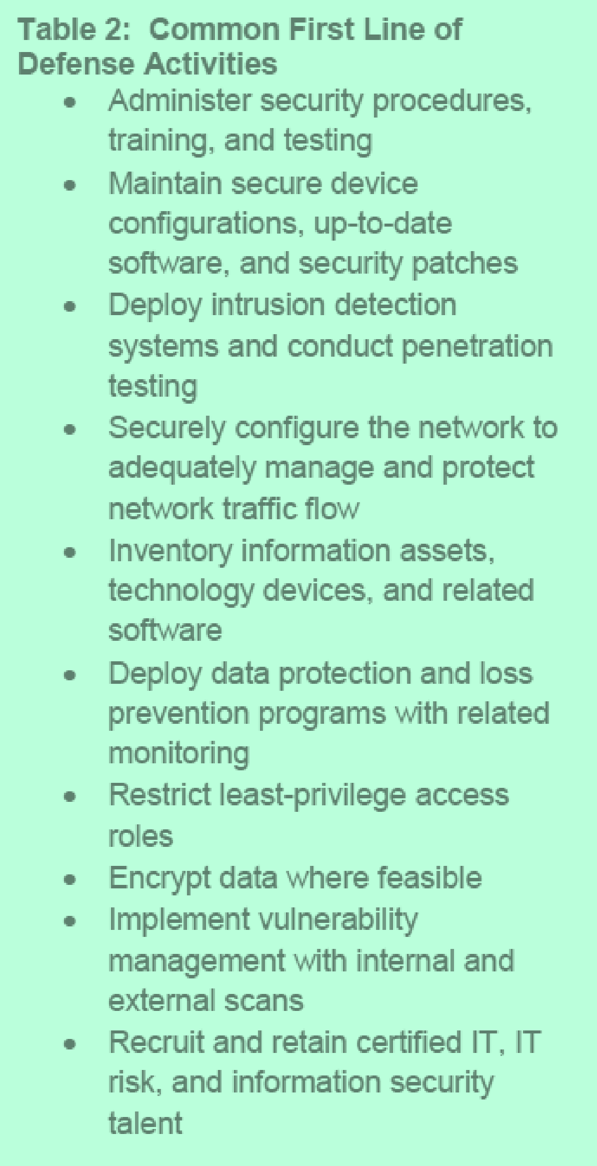


Table 2: Common First Line of Defense Activities

- Administer security procedures, training, and testing
- Maintain secure device configurations, up-to-date software, and security patches
- Deploy intrusion detection systems and conduct penetration testing
- Securely configure the network to adequately manage and protect network traffic flow
- Inventory information assets, technology devices, and related software
- Deploy data protection and loss prevention programs with related monitoring
- Restrict least-privilege access roles
- Encrypt data where feasible
- Implement vulnerability management with internal and external scans
- Recruit and retain certified IT, IT risk, and information security talent

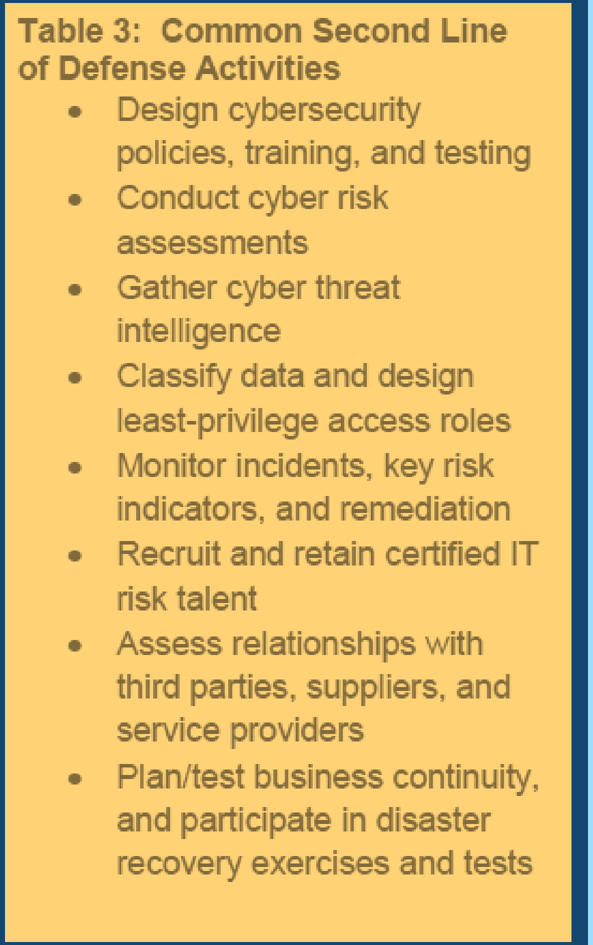


Table 3: Common Second Line of Defense Activities

- Design cybersecurity policies, training, and testing
- Conduct cyber risk assessments
- Gather cyber threat intelligence
- Classify data and design least-privilege access roles
- Monitor incidents, key risk indicators, and remediation
- Recruit and retain certified IT risk talent
- Assess relationships with third parties, suppliers, and service providers
- Plan/test business continuity, and participate in disaster recovery exercises and tests

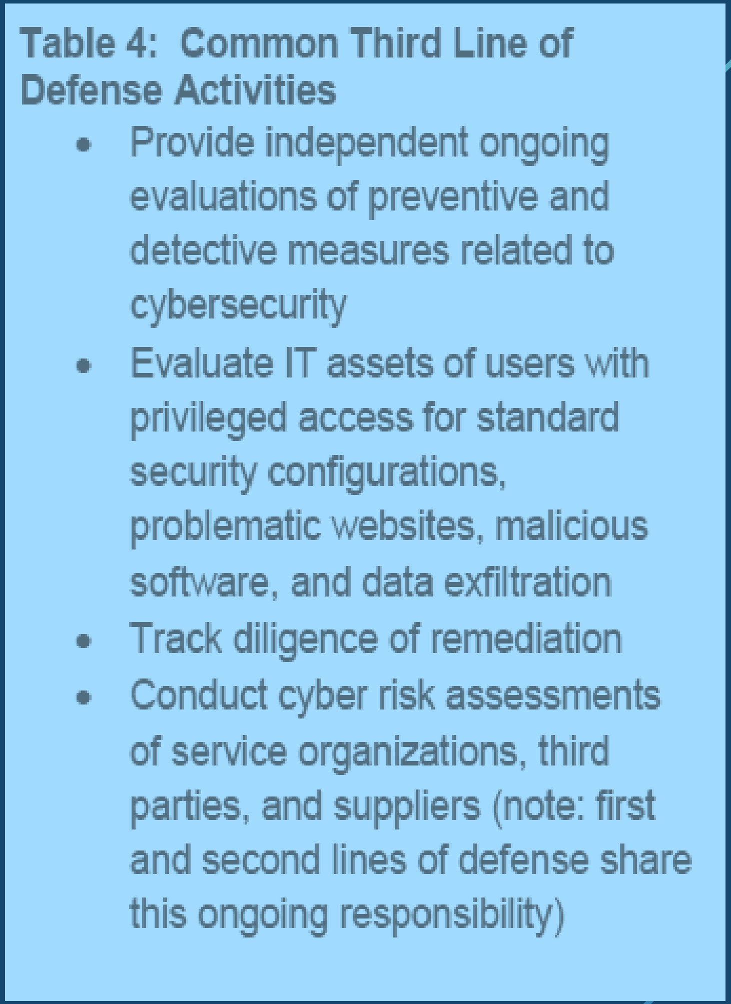


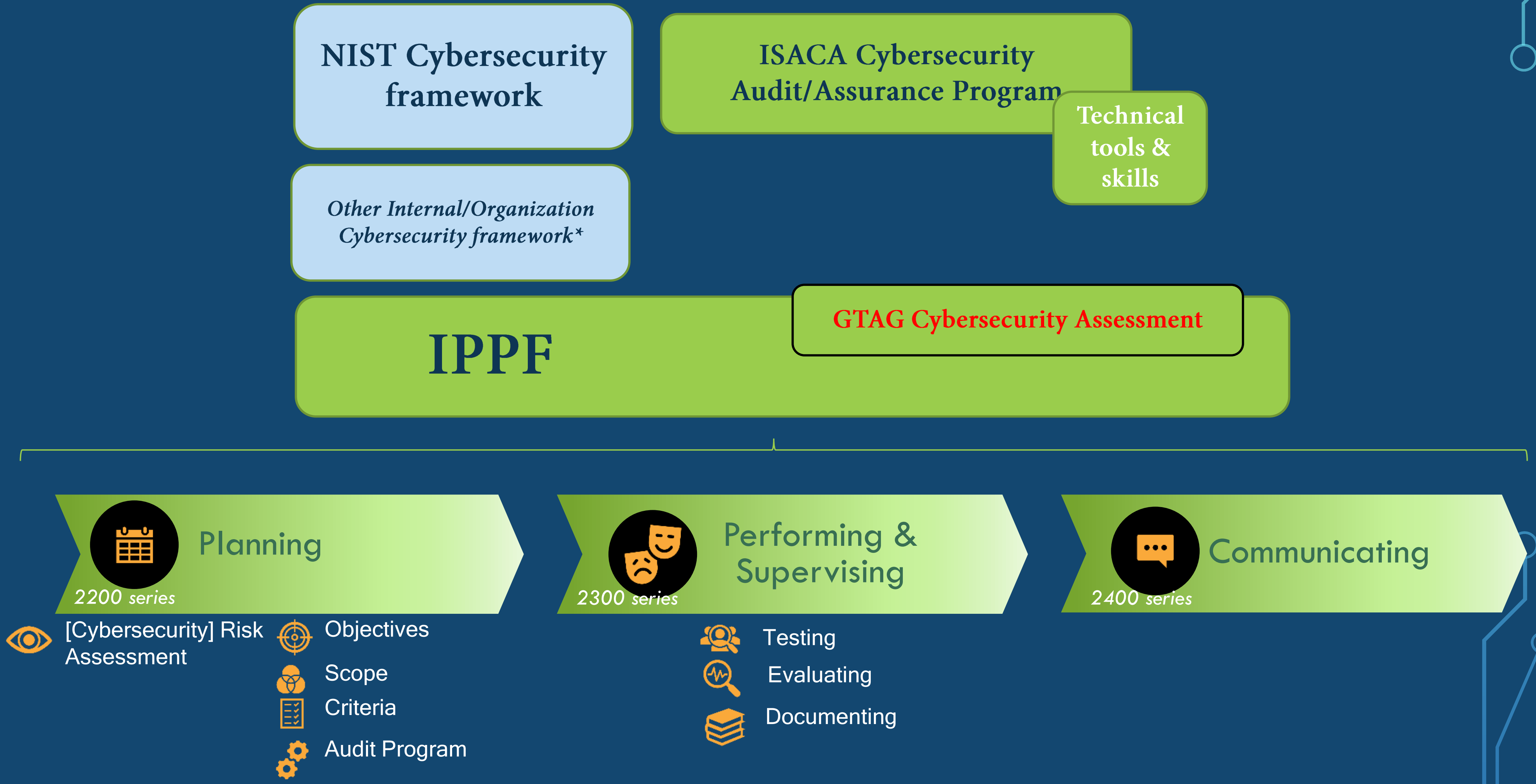
Table 4: Common Third Line of Defense Activities

- Provide independent ongoing evaluations of preventive and detective measures related to cybersecurity
- Evaluate IT assets of users with privileged access for standard security configurations, problematic websites, malicious software, and data exfiltration
- Track diligence of remediation
- Conduct cyber risk assessments of service organizations, third parties, and suppliers (note: first and second lines of defense share this ongoing responsibility)

Source : GTAG Assessing Cybersecurity risk, IIA 2016

PRACTICAL APPROACH

LEVERAGE AVAILABLE FRAMEWORKS



NIST Cybersecurity framework

*Other Internal/Organization Cybersecurity framework**

ISACA Cybersecurity Audit/Assurance Program

Technical tools & skills

IPPF

GTAG Cybersecurity Assessment

Planning

2200 series

Performing & Supervising

2300 series

Communicating

2400 series

[Cybersecurity] Risk Assessment

Objectives

Scope

Criteria

Audit Program

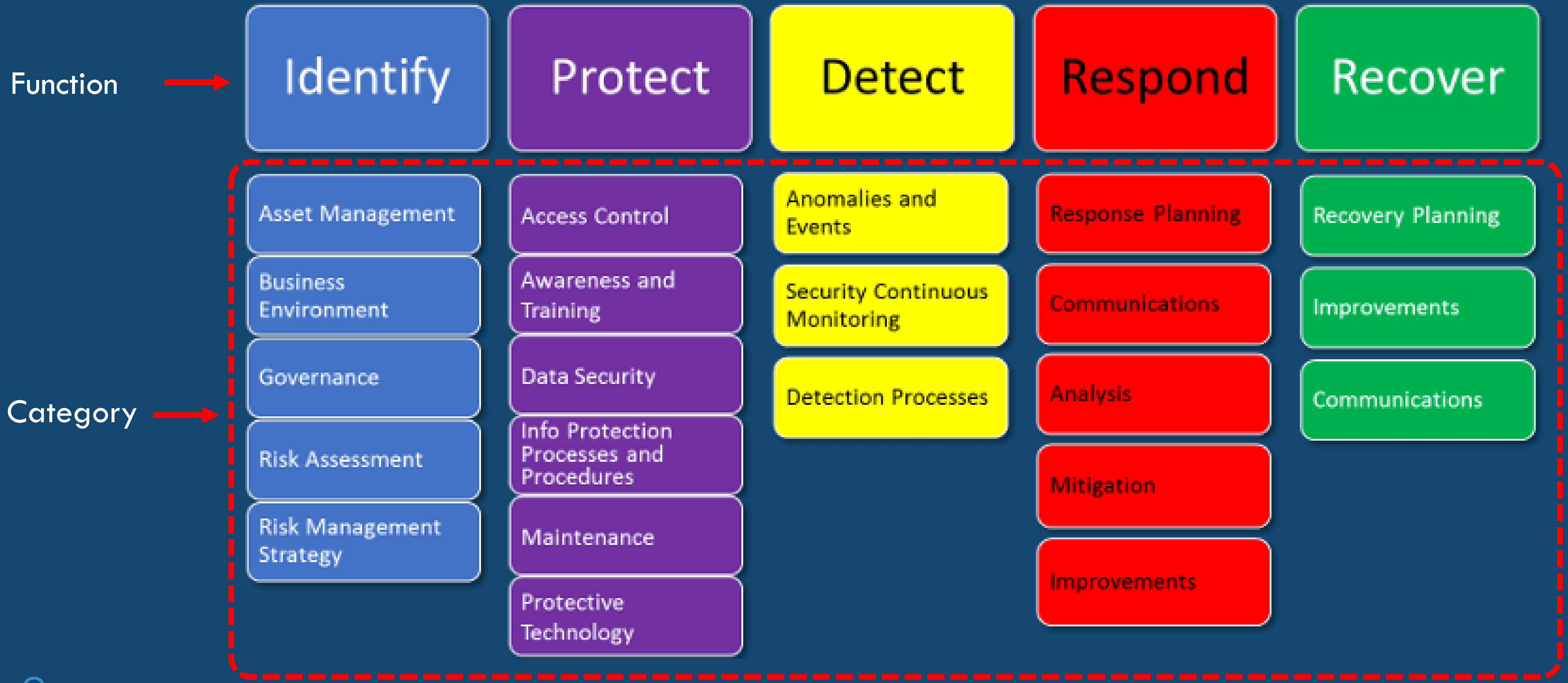
Testing

Evaluating

Documenting

CYBERSECURITY FRAMEWORK

NIST Cybersecurity Framework

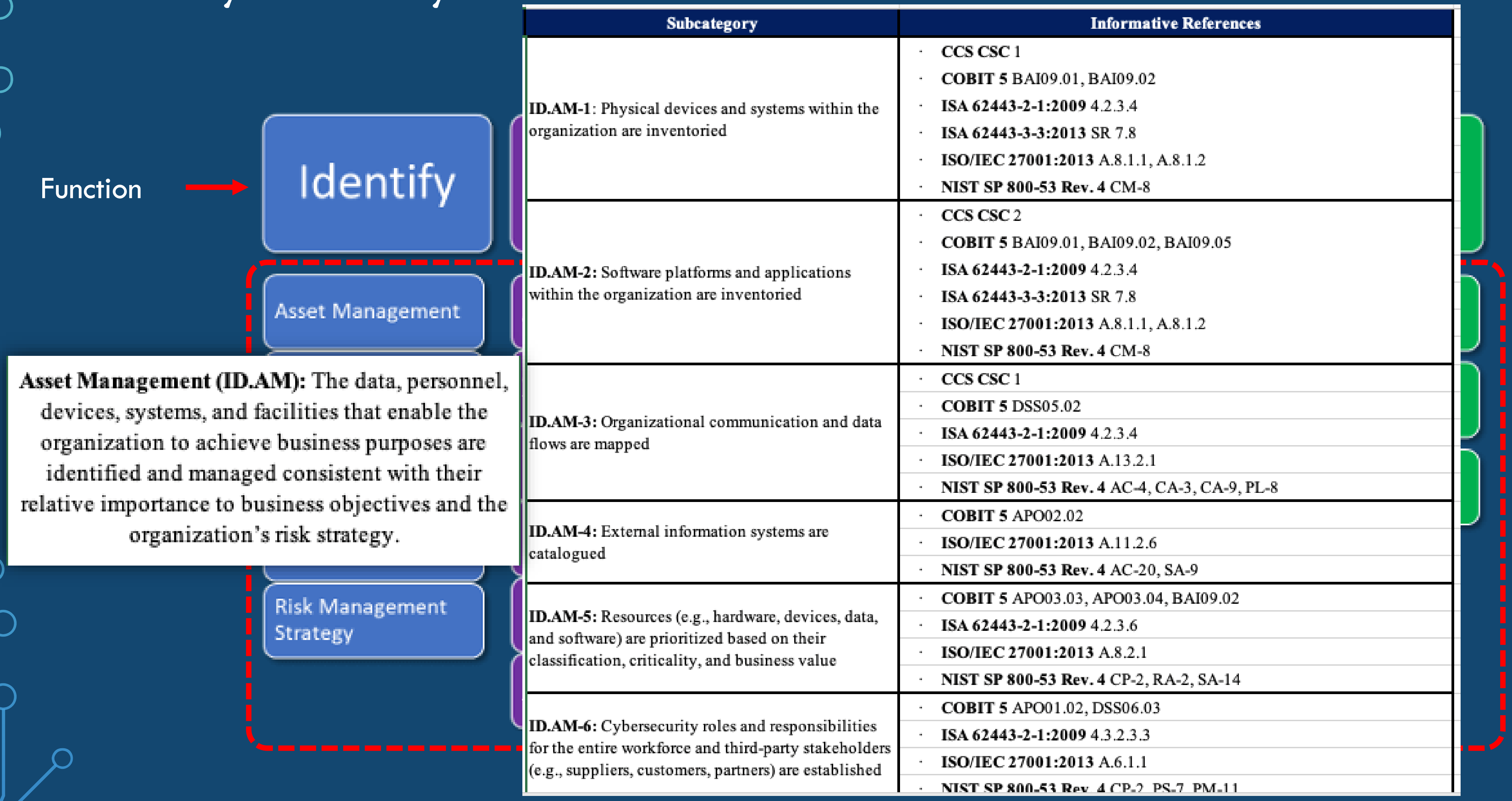


Function	Identify	Protect	Detect	Respond	Recover
Category	Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
	Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
	Governance	Data Security	Detection Processes	Analysis	Communications
	Risk Assessment	Info Protection Processes and Procedures		Mitigation	
	Risk Management Strategy	Maintenance		Improvements	
		Protective Technology			

Source : Framework for Improving Critical Infrastructure Cybersecurity , NIST 2018

CYBERSECURITY FRAMEWORK

NIST Cybersecurity Framework



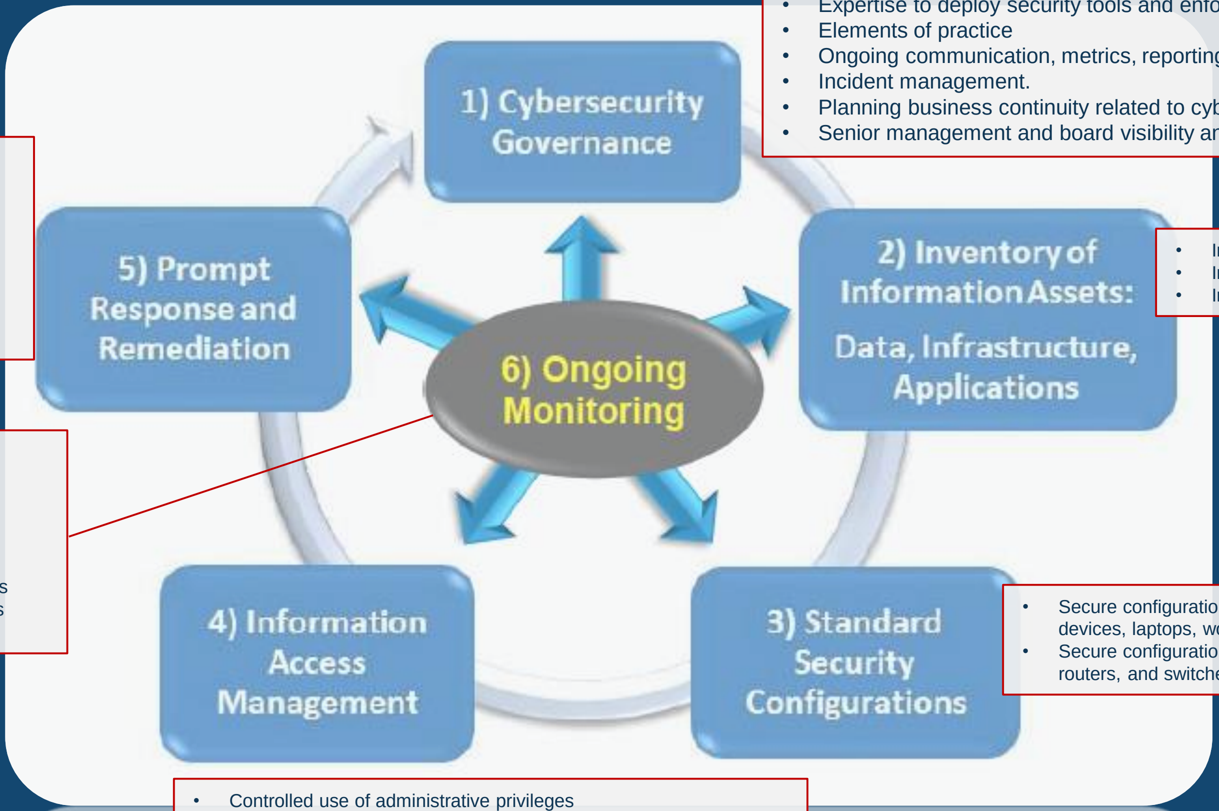
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Subcategory	Informative References
ID.AM-1: Physical devices and systems within the organization are inventoried	· **CCS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
ID.AM-2: Software platforms and applications within the organization are inventoried	· **CCS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
ID.AM-3: Organizational communication and data flows are mapped	· **CCS CSC** 1 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
ID.AM-4: External information systems are catalogued	· **COBIT 5** APO02.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· **COBIT 5** APO03.03, APO03.04, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **COBIT 5** APO01.02, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

Source : Framework for Improving Critical Infrastructure Cybersecurity , NIST 2018

CYBERSECURITY RISK & CONTROL ASSESSMENT

Internal Audit Considerations for Cybersecurity Risk*


1) Cybersecurity Governance
2) Inventory of Information Assets:
Data, Infrastructure, Applications
3) Standard Security Configurations
4) Information Access Management
5) Prompt Response and Remediation
6) Ongoing Monitoring

- Clear, strategic purpose with accountable stakeholders and defined roles and responsibilities.
- Reporting line to enable suitable authority and objectivity.
- Expertise to deploy security tools and enforce policy.
- Elements of practice
- Ongoing communication, metrics, reporting, and action tracking.
- Incident management.
- Planning business continuity related to cyberattack scenarios.
- Senior management and board visibility and involvement

- Inventory of data
- Inventory of authorized and unauthorized devices
- Inventory of authorized and unauthorized software

- Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers
- Secure configurations for network devices such as firewalls, routers, and switches

- Controlled use of administrative privileges
- Account monitoring and control
- Controlled access based on the need to know
- Population of users

- Malware defences
- Limitation and control of network ports, protocols, and services
- Application software security
- Wireless access control
- Boundary defence
- Penetration tests, phishing tests, and red team exercises
- Maintenance, monitoring, and analysis of change events
- Data protection/data loss prevention

- Continuous improvement of the cybersecurity program from raising recommendations and taking timely action to completion.
- Assess vulnerabilities, analyse threat intelligence, and identify gaps.
- Measure performance and compare to industry benchmarks and peer organizations.
- Identify specific knowledge, skills, and abilities needed to support program

) Source : GTAG Assessing Cybersecurity risk, IIA 2016*

CYBERSECURITY RISK

People Process

- Organization Policy-Function
- Culture
- Social Engineering
- Knowledge-skill
- Awareness
- 3rd parties/vendor

Technology

Assets - Threat - Vulnerabilities

Tangible or intangible value is worth protecting, including people, information, infrastructure, finances & reputation

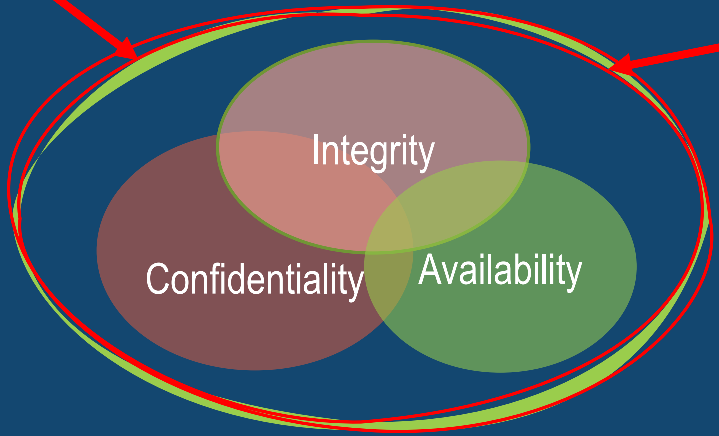
- People
- Data/Information
- Application
- Storage
- Computing
- Network

Any natural or man-made circumstance that could have an adverse impact on an organizational asset

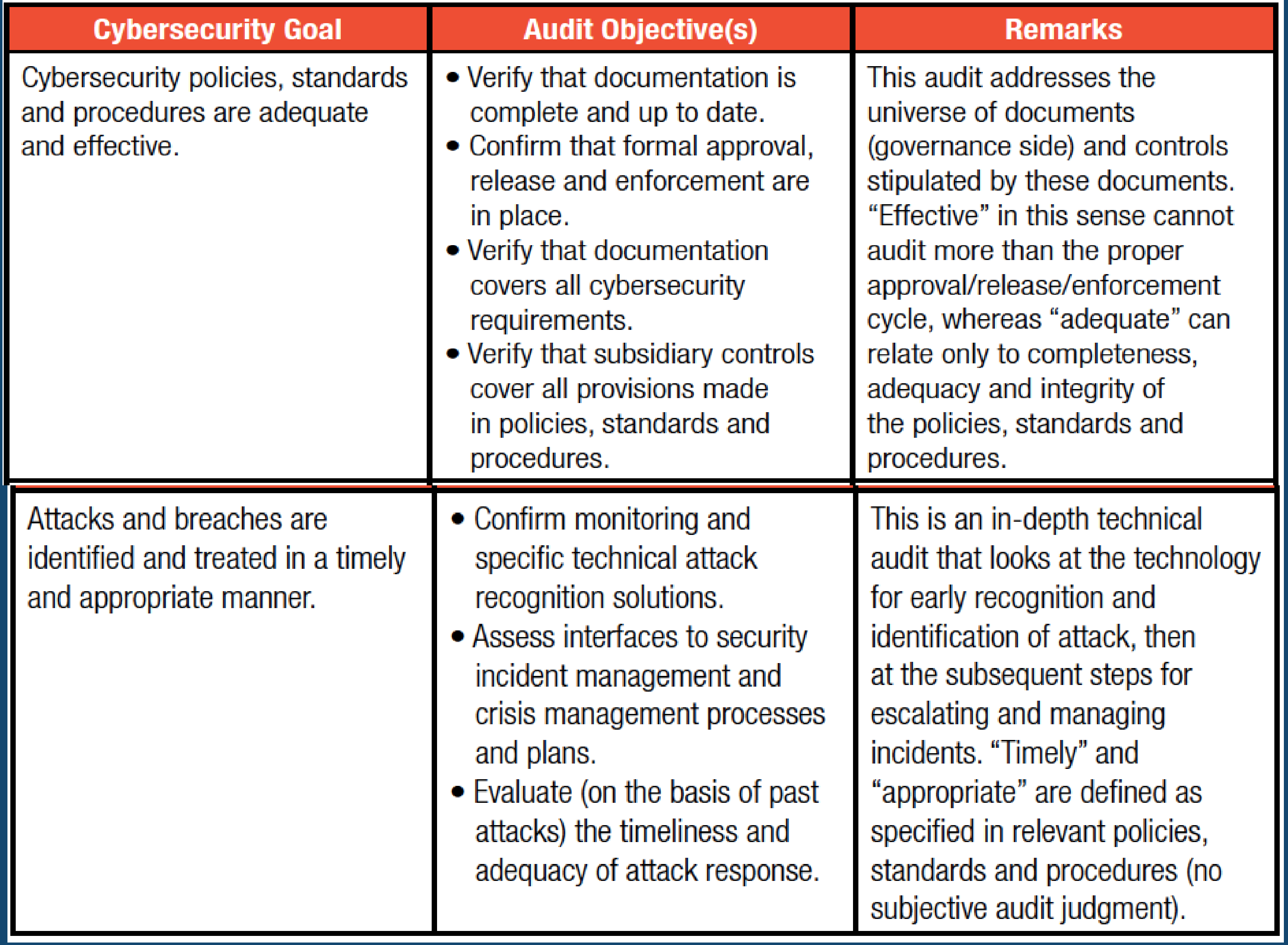
- Malware
- Phishing
- Denial of Services
- Spam
- Data breach
- Web based attacks
- Botnets
- Identity thefts-social engineering
- APT

The absence or weakness of a safeguard in an asset that makes a threat potentially more likely to occur, or likely to occur more frequently

- Lack of awareness
- Lack of policy
- Failure to monitor logs
- Inadequate passwords
- Open network ports
- Coding errors
- Interoperability errors



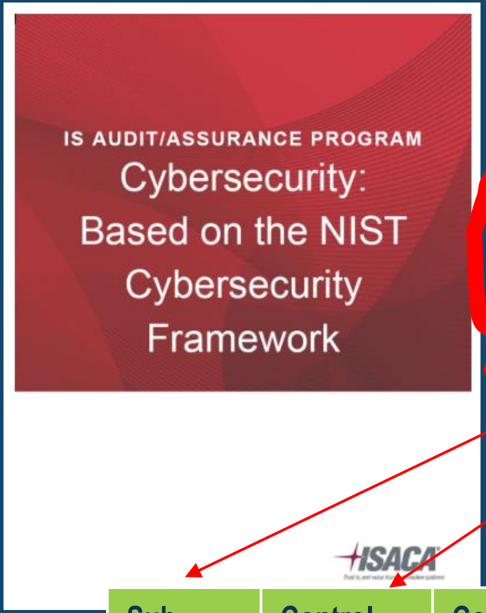
AUDIT OBJECTIVES



Cybersecurity Goal	Audit Objective(s)	Remarks
Cybersecurity policies, standards and procedures are adequate and effective.	• Verify that documentation is complete and up to date. • Confirm that formal approval, release and enforcement are in place. • Verify that documentation covers all cybersecurity requirements. • Verify that subsidiary controls cover all provisions made in policies, standards and procedures.	This audit addresses the universe of documents (governance side) and controls stipulated by these documents. “Effective” in this sense cannot audit more than the proper approval/release/enforcement cycle, whereas “adequate” can relate only to completeness, adequacy and integrity of the policies, standards and procedures.
Attacks and breaches are identified and treated in a timely and appropriate manner.	• Confirm monitoring and specific technical attack recognition solutions. • Assess interfaces to security incident management and crisis management processes and plans. • Evaluate (on the basis of past attacks) the timeliness and adequacy of attack response.	This is an in-depth technical audit that looks at the technology for early recognition and identification of attack, then at the subsequent steps for escalating and managing incidents. “Timely” and “appropriate” are defined as specified in relevant policies, standards and procedures (no subjective audit judgment).

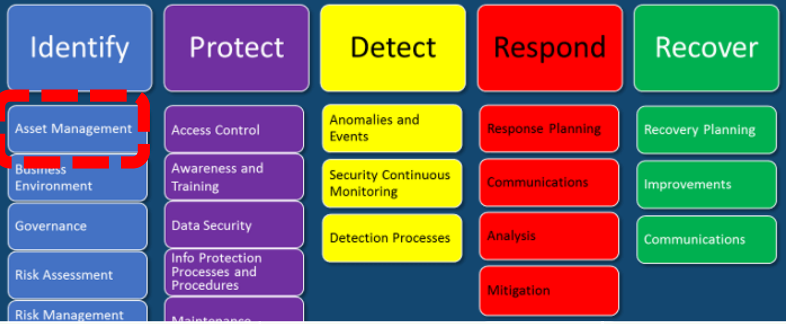
Source : Transforming Cybersecurity, ISACA 2014

CYBERSECURITY AUDIT/ASSURANCE PROGRAM



IS AUDIT/ASSURANCE PROGRAM

Cybersecurity: Based on the NIST Cybersecurity Framework



Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management	Maintenance			

Category	Subcategory	Informative Reference

Sub-Process	Control Objectives	Controls	Control Type	Control Classifcation	Control Frequency	Testing Step	NIST ref to COBIT5	Additional Ref. to COBIT5	Ref.Framework/Standard	Ref.Work paper	Pass/ Fail	Comments

Source : Framework for Improving Critical Infrastructure Cybersecurity , NIST 2018

: IS Audit/Assurance Program Cybersecurity: Based on the NIST Cybersecurity Framework, ISACA 2016

Column Name	Description
Process Sub-area	An activity within an overall process influenced by the enterprise's policies and procedures that takes inputs from a number of sources, manipulates the inputs and produces outputs
Ref. Risk	Specifies the risk this control is intended to address
Control Objectives	A statement of the desired result or purpose that must be in place to address the inherent risk in the review areas within scope
Controls	The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management or legal nature
Control Type	Controls can be automated (technical), manual (administrative) or physical. Automated/technical controls are things managed or performed by computer systems. Manual/administrative controls are usually things that employees can or cannot do. Physical controls include locks, fences, mantraps and even geographic specific controls.
Control Classification	Another way to classify controls is by the way they address a risk exposure. Preventive controls should stop an event from happening. Detective controls should identify an event when it is happening and generate an alert that prompts a corrective control to act. Corrective controls should limit the impact of an event and help resume normal operations within a reasonable time frame. Compensating controls are alternate controls designed to accomplish the intent of the original controls as closely as possible when the originally designed controls cannot be used due to limitations of the environment.
Control Frequency	Control activities can occur in real-time, daily, weekly, monthly, annually, etc.
Testing Step	Identifies the steps being tested to evaluate the effectiveness of the control under review
NIST Ref. to COBIT 5	Identifies the COBIT 5 processes related to the control objective or control activities as defined by the NIST Cybersecurity Framework
Additional Ref. COBIT 5	Identifies additional COBIT 5 processes related to the control objective or control activities
Ref. Framework/Standards	Specifies frameworks and/or standards that relate to the control under review (e.g., NIST, HIPAA, SOX, ISO)
Ref. Workpaper	The evidence column usually contains a reference to other documents that contain the evidence supporting the pass/fail mark for the audit step.
Pass/Fail	Document preliminary conclusions regarding the effectiveness of controls.
Comments	Free format field

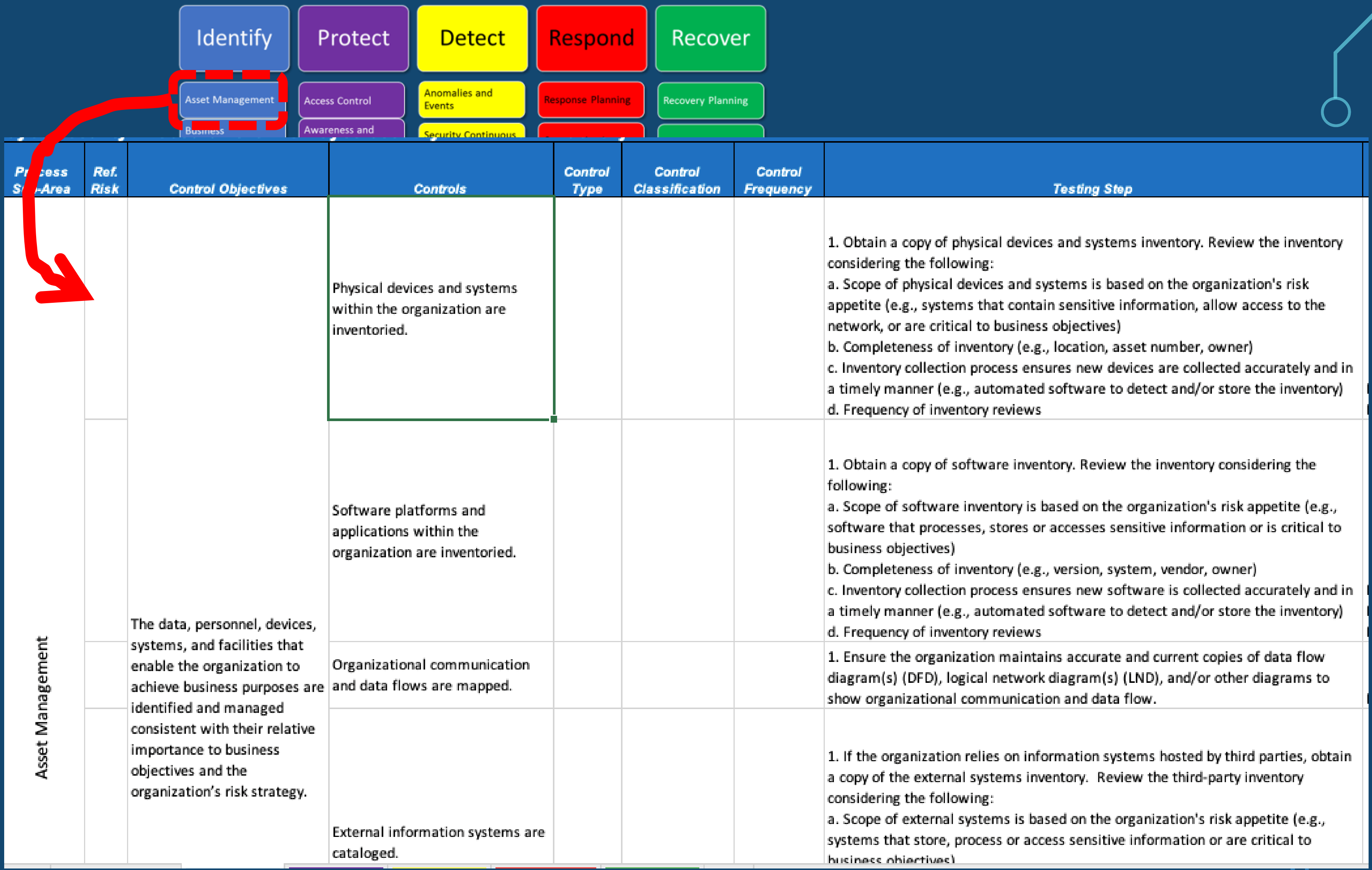
Source : IS Audit/Assurance Program Cybersecurity: Based on the NIST Cybersecurity Framework, ISACA 2016

CYBERSECURITY AUDIT/ASSURANCE PROGRAM

IS AUDIT/ASSURANCE PROGRAM

Cybersecurity: Based on the NIST Cybersecurity Framework

ISACA



Process Sub-Area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step
Asset Management		The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	Physical devices and systems within the organization are inventoried.				1. Obtain a copy of physical devices and systems inventory. Review the inventory considering the following: a. Scope of physical devices and systems is based on the organization's risk appetite (e.g., systems that contain sensitive information, allow access to the network, or are critical to business objectives) b. Completeness of inventory (e.g., location, asset number, owner) c. Inventory collection process ensures new devices are collected accurately and in a timely manner (e.g., automated software to detect and/or store the inventory) d. Frequency of inventory reviews
			Software platforms and applications within the organization are inventoried.				1. Obtain a copy of software inventory. Review the inventory considering the following: a. Scope of software inventory is based on the organization's risk appetite (e.g., software that processes, stores or accesses sensitive information or is critical to business objectives) b. Completeness of inventory (e.g., version, system, vendor, owner) c. Inventory collection process ensures new software is collected accurately and in a timely manner (e.g., automated software to detect and/or store the inventory) d. Frequency of inventory reviews
			Organizational communication and data flows are mapped.				1. Ensure the organization maintains accurate and current copies of data flow diagram(s) (DFD), logical network diagram(s) (LND), and/or other diagrams to show organizational communication and data flow.
			External information systems are cataloged.				1. If the organization relies on information systems hosted by third parties, obtain a copy of the external systems inventory. Review the third-party inventory considering the following: a. Scope of external systems is based on the organization's risk appetite (e.g., systems that store, process or access sensitive information or are critical to business objectives)

Source : IS Audit/Assurance Program Cybersecurity: Based on the NIST Cybersecurity Framework, ISACA 2016

KEY TAKEAWAYS

- *Auditor(s) need to equipped with relevant knowledge, skill & tool, recent trends/research (1200 - proficiency & due professional care)*

- *Leverage available best practices-guidelines, frameworks, standard including technology-vendor relevant with organization*

- *Audit/assurance programs should be considered a starting point and adjusted based upon risk and criteria that are relevant to the organization being audited*

- *Identify and categorize audit areas where reliance on the work of others makes sense (SSAE 16/SOC Report)*

- *"one cannot plan against everything and prevent it" and addresses exactly those (probable or improbable) attacks and breaches that require targeted response and investigative activities.*

10 THINGS AUDITOR SHOULD KNOW

ABOUT CYBERSECURITY

- LEVERAGE EXISTING FRAMEWORKS/GUIDELINES
- CONSIDER FORTHCOMING LEGISLATION
- ALL RISKS ARE SUBJECTIVE
- USERS ARE (AND WILL ALWAYS BE) THE BIGGEST SECURITY RISK
- BASIC INFORMATION SECURITY CONTROLS STILL HOLD TRUE
- NEED A CYBER INCIDENT RESPONSE POLICY AND PLAN THAT IS FULLY TESTED
- CYBER SECURITY STRATEGY NEEDS TO BE AGILE – LANDSCAPE IS “MUTATING”
- CYBER SECURITY AWARENESS DEPENDS ON THE RIGHT TRAINING
- EVERYTHING IS CONNECTED TO EVERYTHING
- BE AWARE OF CREDENTIAL THEFT TECHNIQUES

Source : ISACA 2016 https://m.isaca.org/Knowledge-Center/Research/Documents/Auditing-Cyber-Security-Infographic_ifg_eng_0217.pdf

REFERENCES

- International Professional Practices Framework (IPPF), 2017 IIA
- SG GTAG Assessing Cybersecurity Risk - Roles of the three lines of defense, 2016 IIA
- Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework 1.1), NIST 2018
- Transforming Cybersecurity, 2013 ISACA
- IS Audit/Assurance Program Cybersecurity: Based on the NIST Cybersecurity Framework, 2016 ISACA
- https://www.cisecurity.org/
- https://www.enisa.europa.eu/

thank you

taufik.purba@gmail.com

0811224093

www.linkedin.com/in/taufiksnpurba