CYBERSECURITY

MAMATHA SPARKS - CIA, CISA
CITY OF DALLAS, OFFICE OF THE CITY AUDITOR

FEBRUARY 15, 2019

AGENDA

- Defining Cybersecurity
- Auditing Cybersecurity
- Being in the know

DEFINING CYBERSECURITY

Making it Audit Worthy

COMMONLY DESCRIBED AS…

Ransomware

Phishing

Hacker

Worms

Social Engineering

Malware

DDoS

Trojans

Virus

Man in the Middle

Stolen Identities

FORMAL DEFINITIONS

ISACA: *The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems.*

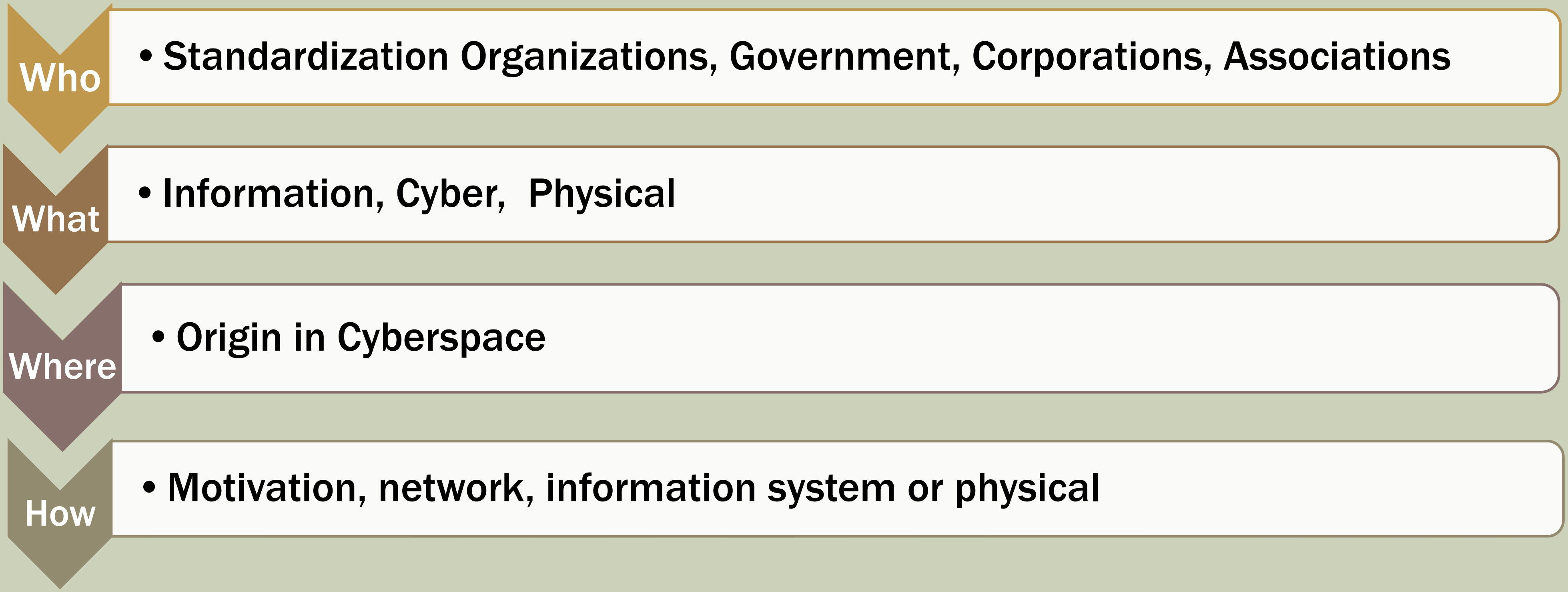
Gartner: *Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack* adversaries.

NIST: *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.*

Webster*: Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack*

ISO 27032: *Preservation of confidentiality, integrity and availability of information in the Cyberspace*

FORMAL DEFINITION VARIATIONS



Who

- Standardization Organizations, Government, Corporations, Associations

What

- Information, Cyber, Physical

Where

- Origin in Cyberspace

How

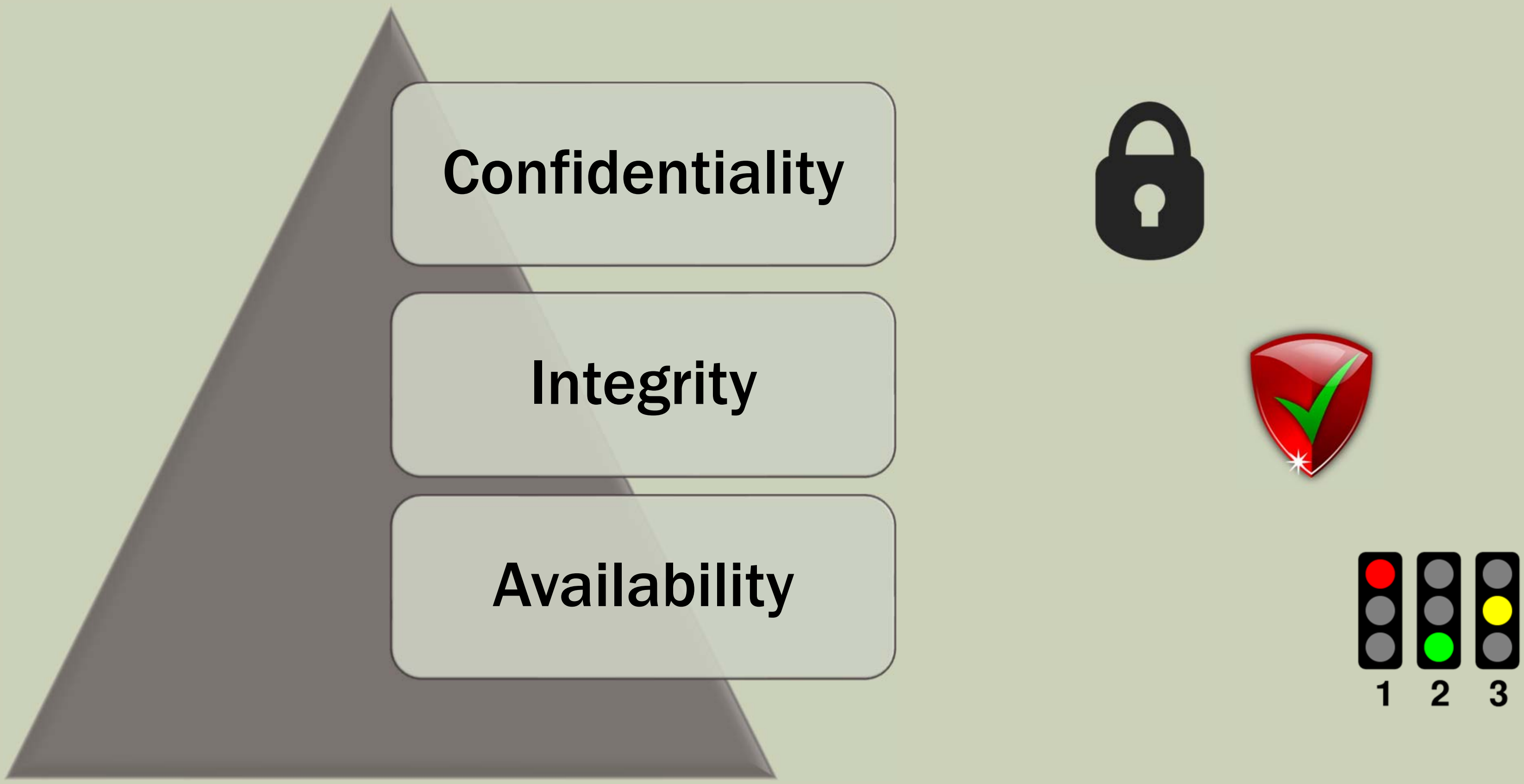
- Motivation, network, information system or physical

ensia

COMMON THEMES

- Protection/Prevention/Preservation…
- Digital /electronic information assets…
- Activity *might* originates in cyberspace…
- Information, Communications, Physical and Operational

PROTECTION/PREVENTION/PRESERVATION

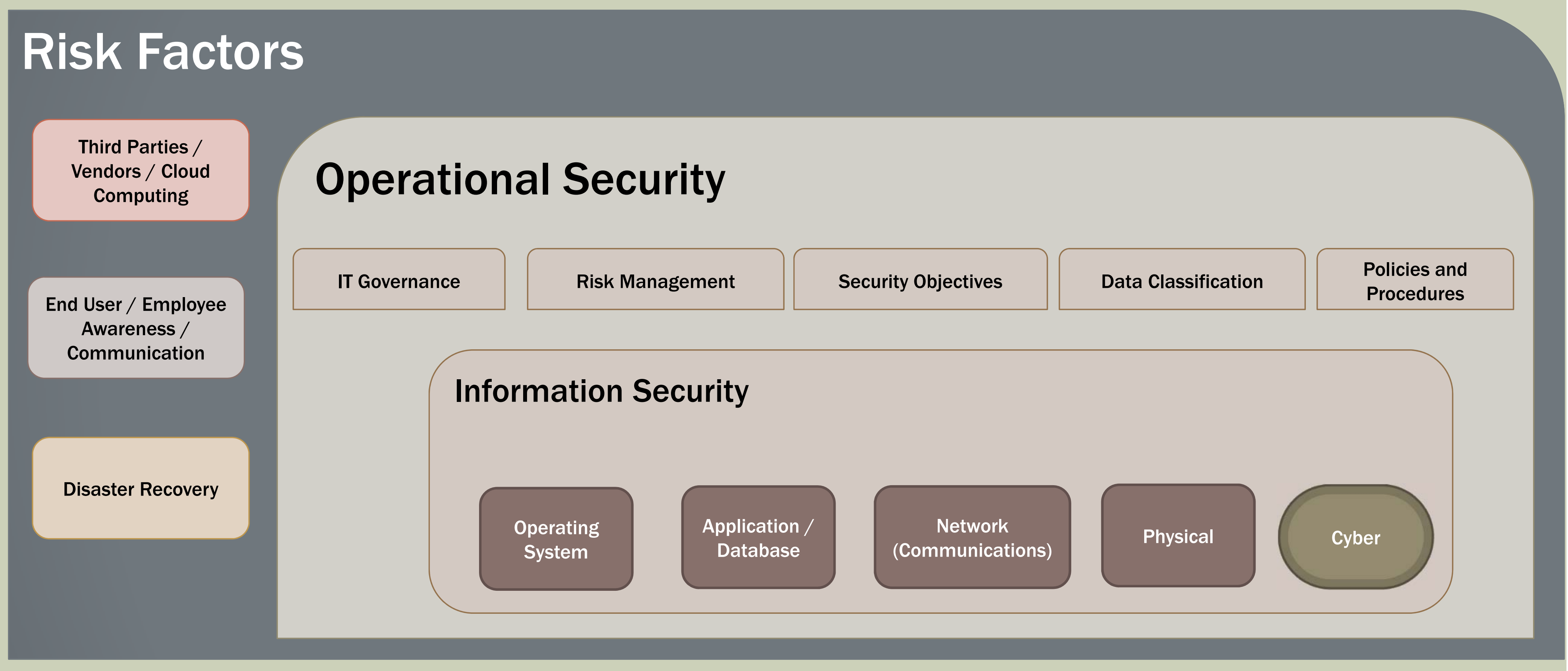


Confidentiality

Integrity

Availability

INFORMATION, COMMUNICATIONS, PHYSICAL, AND OPERATIONS SECURITY



Risk Factors

Third Parties / Vendors / Cloud Computing

End User / Employee Awareness / Communication

Disaster Recovery

Operational Security

IT Governance

Risk Management

Security Objectives

Data Classification

Policies and Procedures

Information Security

Operating System

Application / Database

Network (Communications)

Physical

Cyber

PUTTING INTO WORDS

Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** is the practice of securing a computer network from intruders
- **Application security** focuses on keeping software and devices free of threats
- **Information security** protects the integrity and privacy of data, both in storage and in transit
- **Operational security** includes the processes and decisions for handling and protecting data assets
- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data.
- **End-user education** addresses the most unpredictable cyber-security factor: people.

Modified from https://usa.kaspersky.com/resource-center/definitions/what-is-cyber-security

FORMAL DEFINITION

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

The general security objectives comprise the following: Availability, Integrity (which may include authenticity and non-repudiation) and, Confidentiality.

International Telecommunication Union

AUDITING CYBERSECURITY

Points of Focus

APPROACHES

Cybersecurity Audit

- *Scope, Objectives, Control Activities, Testing Steps*
- *Cybersecurity as a component of overall security program*
- *Requires involvement of various management and operational levels*
- *Message can be difficult to convey*

Cybersecurity Program Assessment

- *Limited in scope – focuses on providing a design/baseline assessment*
- *Cybersecurity as a individual element of overall security program*
- *Appeals to senior level management*
- *Message is simplified but incomplete*

Cybersecurity –At a Glance

- *Quick-hits*
- *Expertise and resources are minimal*
- *Focuses on individual topics associated with Cybersecurity*

CYBERSECURITY AUDIT

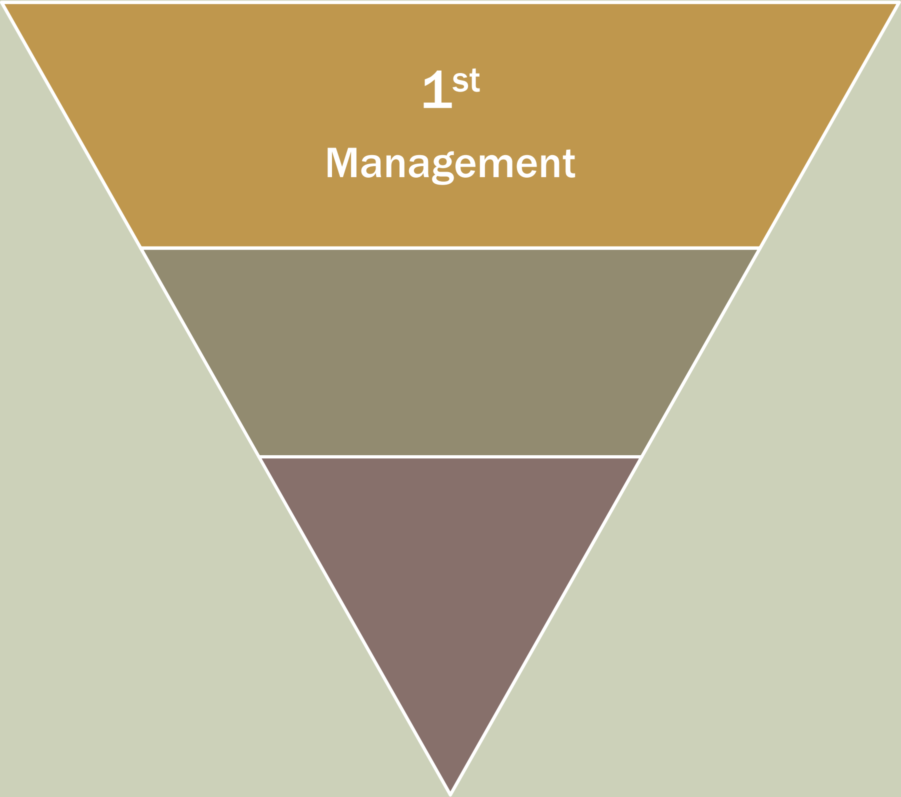
COBIT 5

COBIT 5

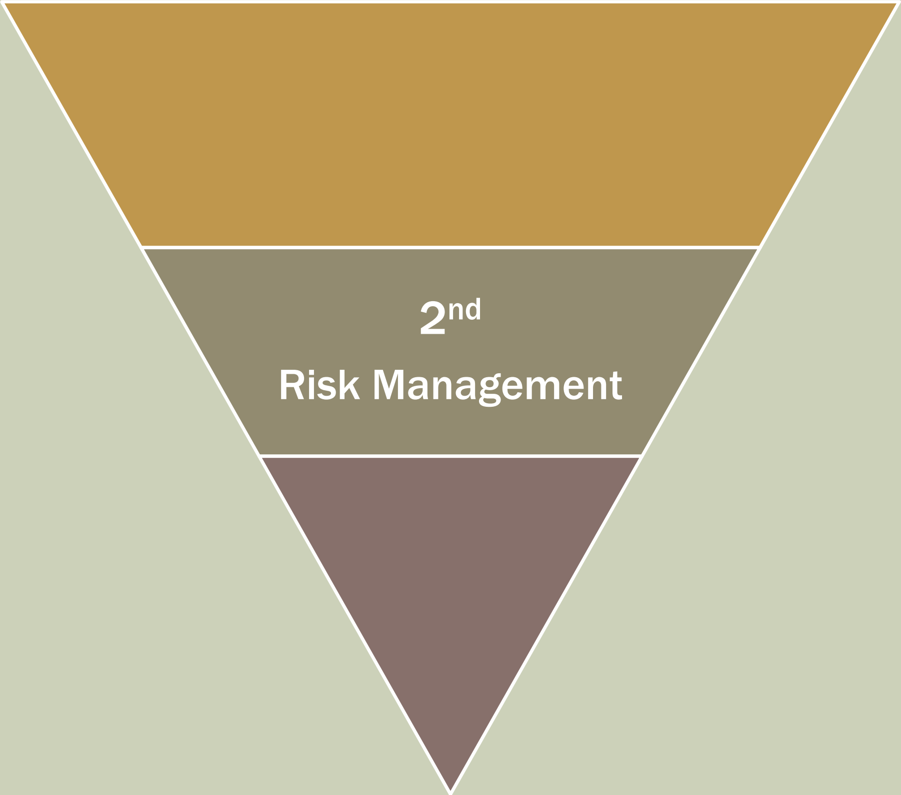
- Audit and review universe is across three lines of defense
- Basic information security controls still hold true
- Users are the biggest security risk
- Uses NIST to develop audit work program

COBIT5 - LAYERS OF DEFENSE

- Control Self-Assessments
- Authorize Attack/ Penetration Testing
- Functional/technical testing
- Focus on Social Behavior for Employees (End User Training)
- Regular management review
- Making investments



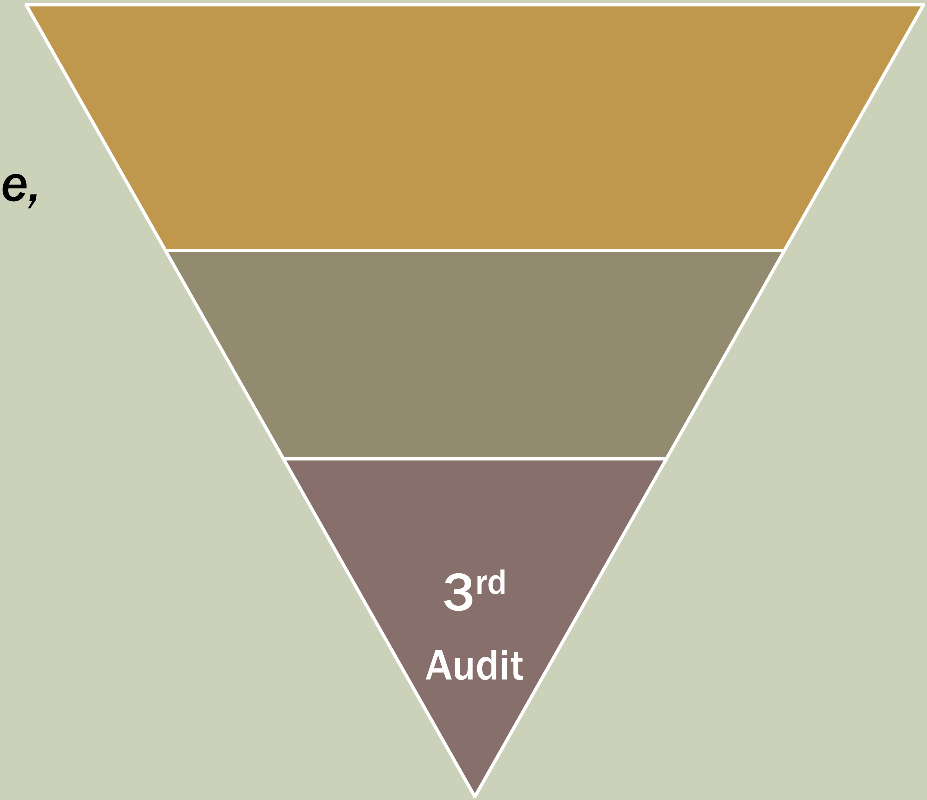
COBIT5 - LAYERS OF DEFENSE



- Risk assessments -baseline
- Identifying vulnerabilities and threats (review existing controls)
- Business impact analysis
- Emerging tools

COBIT 5- LAYERS OF DEFENSE

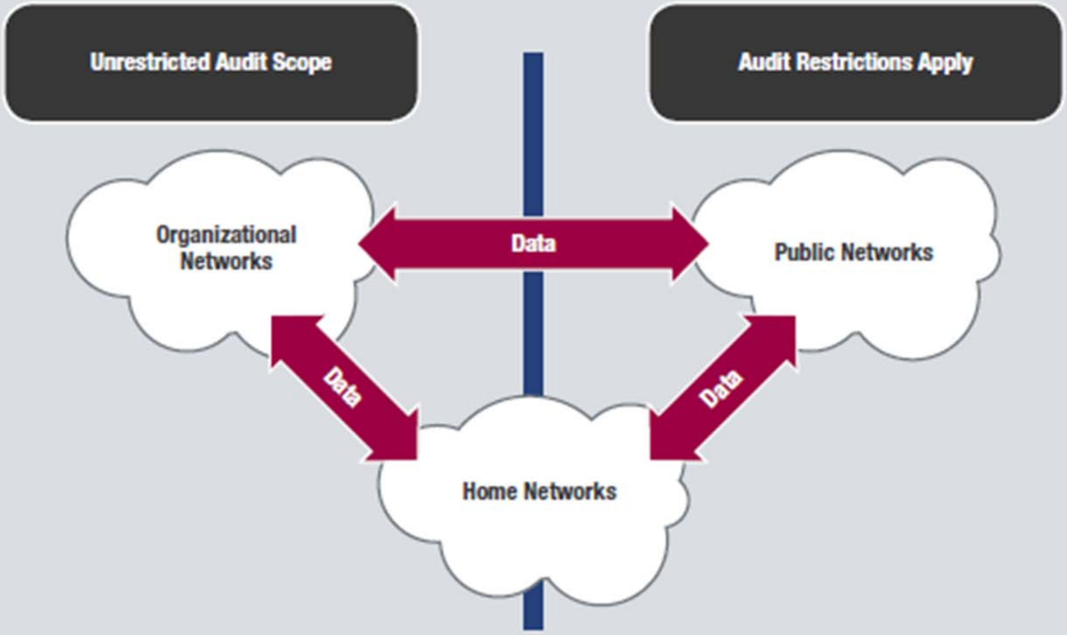
- Audit Scope (restrictions)
- Type of Cybersecurity Review *(Governance, Risk Management, Assurance)*
- Cyber Security Goals / Audit Objectives
- Cybersecurity Maturity Model
- Corrective Action Plans



THIRD LINE OF DEFENSE

AUDIT SOCPE

FIGURE 3—AUDIT BOUNDARIES



SOURCE: ISACA, *Transforming Cybersecurity*, USA, 2013, figure 46

THIRD LINE OF DEFENSE

TYPE OF REVIEW

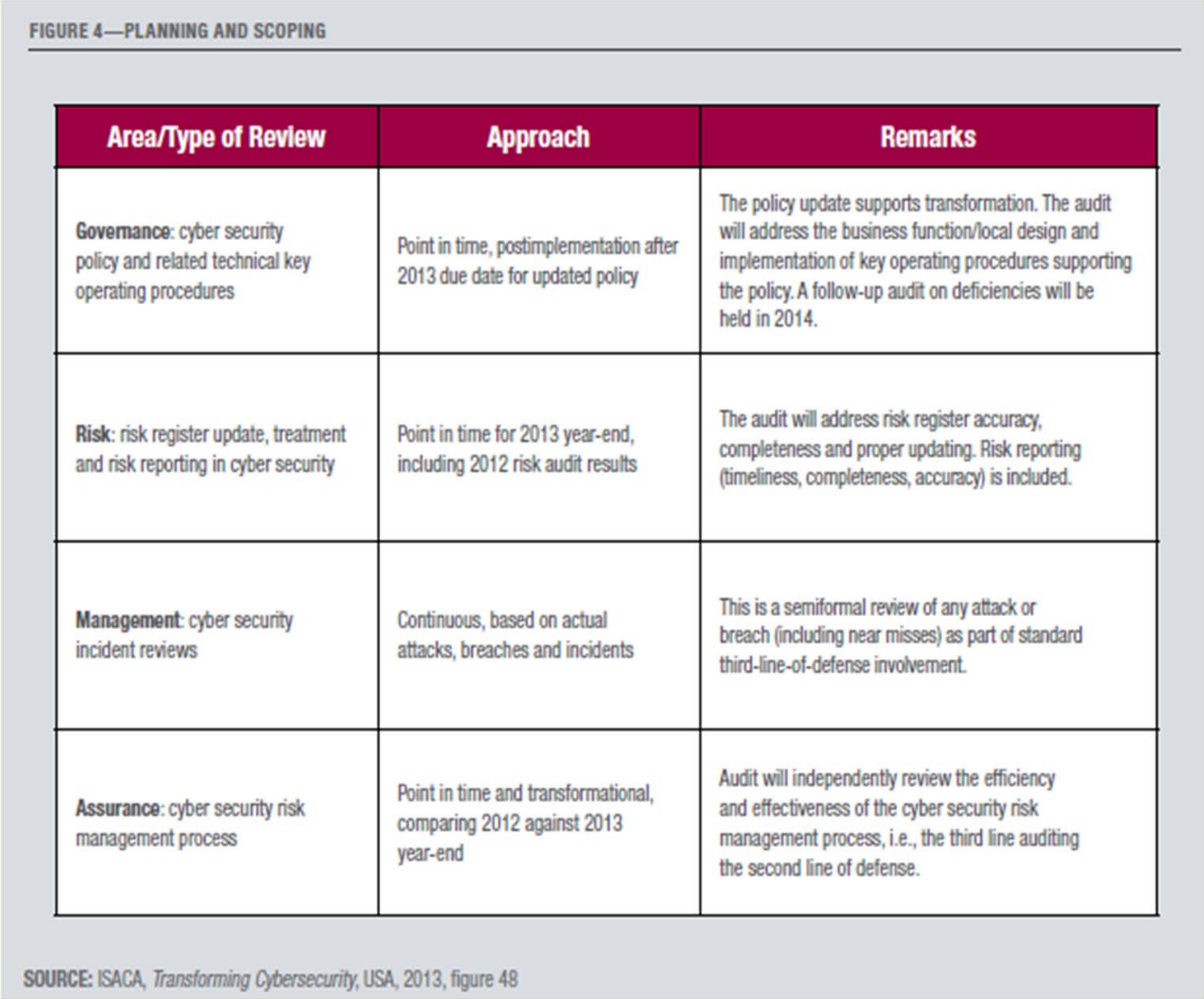


FIGURE 4—PLANNING AND SCOPING

Area/Type of Review	Approach	Remarks
Governance: cyber security policy and related technical key operating procedures	Point in time, postimplementation after 2013 due date for updated policy	The policy update supports transformation. The audit will address the business function/local design and implementation of key operating procedures supporting the policy. A follow-up audit on deficiencies will be held in 2014.
Risk: risk register update, treatment and risk reporting in cyber security	Point in time for 2013 year-end, including 2012 risk audit results	The audit will address risk register accuracy, completeness and proper updating. Risk reporting (timeliness, completeness, accuracy) is included.
Management: cyber security incident reviews	Continuous, based on actual attacks, breaches and incidents	This is a semiformal review of any attack or breach (including near misses) as part of standard third-line-of-defense involvement.
Assurance: cyber security risk management process	Point in time and transformational, comparing 2012 against 2013 year-end	Audit will independently review the efficiency and effectiveness of the cyber security risk management process, i.e., the third line auditing the second line of defense.

SOURCE: ISACA, *Transforming Cybersecurity*, USA, 2013, figure 48

THIRD LINE OF DEFENSE

GOAL

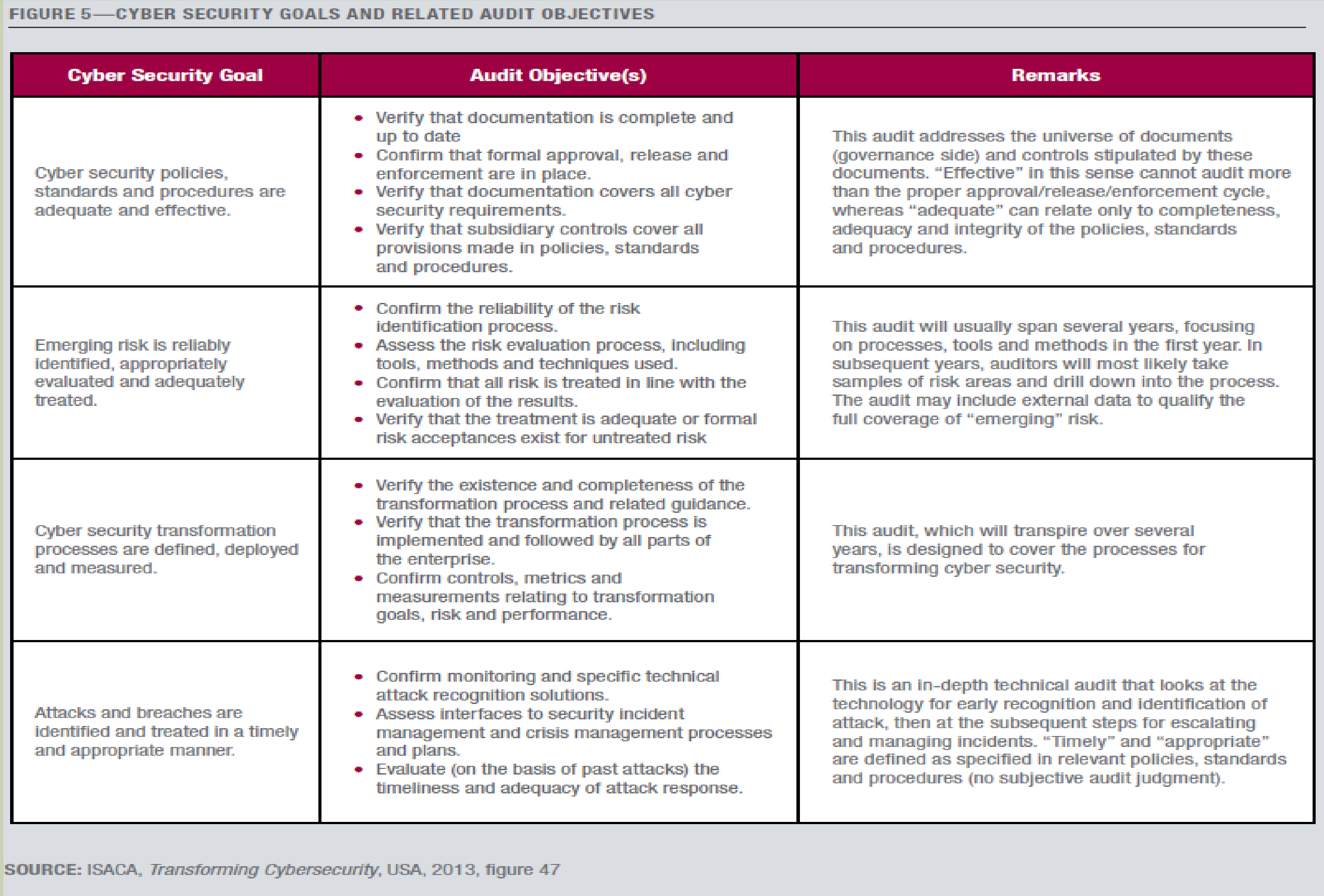


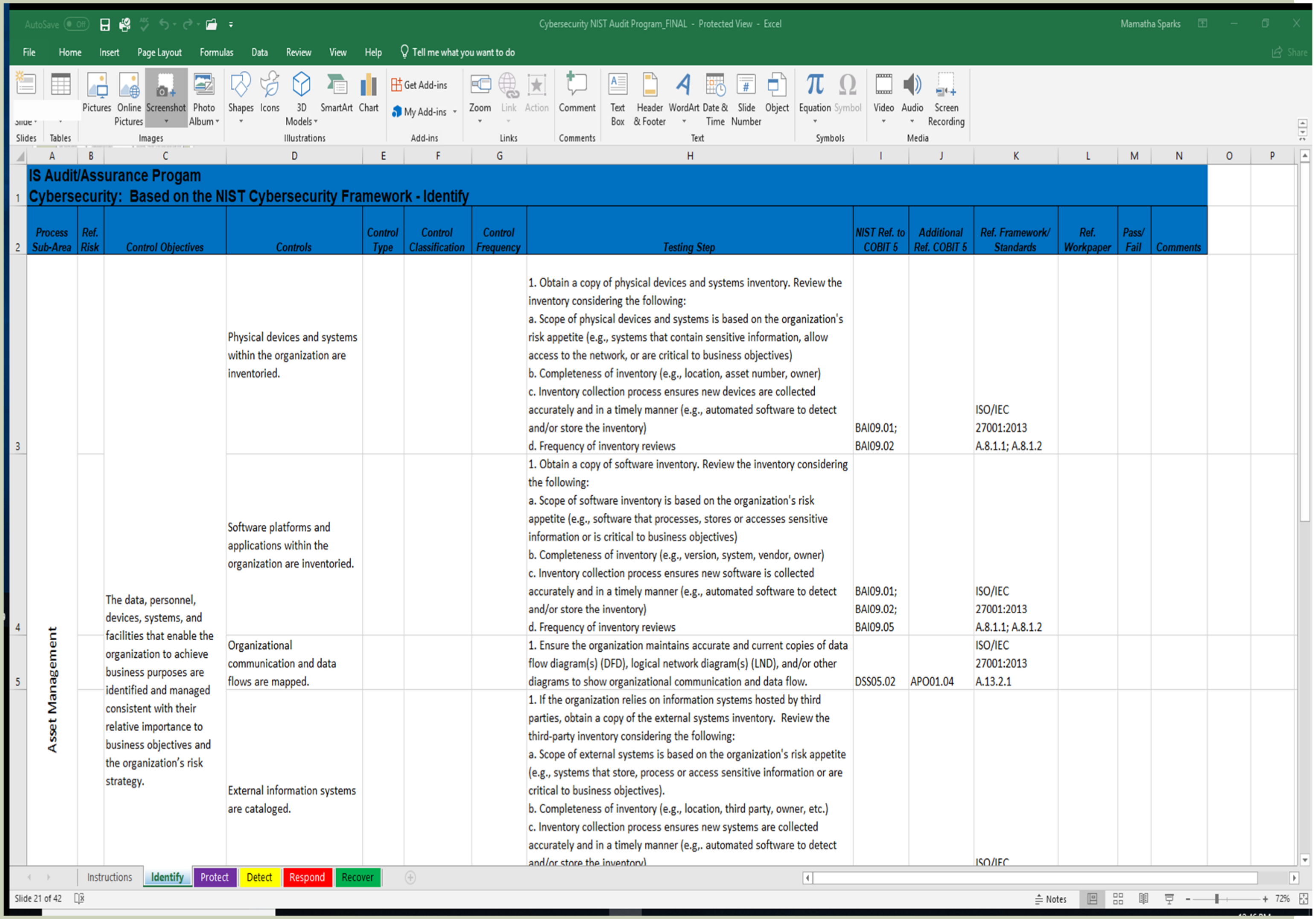
FIGURE 5—CYBER SECURITY GOALS AND RELATED AUDIT OBJECTIVES

Cyber Security Goal	Audit Objective(s)	Remarks
Cyber security 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 cyber security 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.
Emerging risk is reliably identified, appropriately evaluated and adequately treated.	• Confirm the reliability of the risk identification process. • Assess the risk evaluation process, including tools, methods and techniques used. • Confirm that all risk is treated in line with the evaluation of the results. • Verify that the treatment is adequate or formal risk acceptances exist for untreated risk	This audit will usually span several years, focusing on processes, tools and methods in the first year. In subsequent years, auditors will most likely take samples of risk areas and drill down into the process. The audit may include external data to qualify the full coverage of "emerging" risk.
Cyber security transformation processes are defined, deployed and measured.	• Verify the existence and completeness of the transformation process and related guidance. • Verify that the transformation process is implemented and followed by all parts of the enterprise. • Confirm controls, metrics and measurements relating to transformation goals, risk and performance.	This audit, which will transpire over several years, is designed to cover the processes for transforming cyber security.
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: ISACA, *Transforming Cybersecurity*, USA, 2013, figure 47

THIRD LINE OF DEFENSE

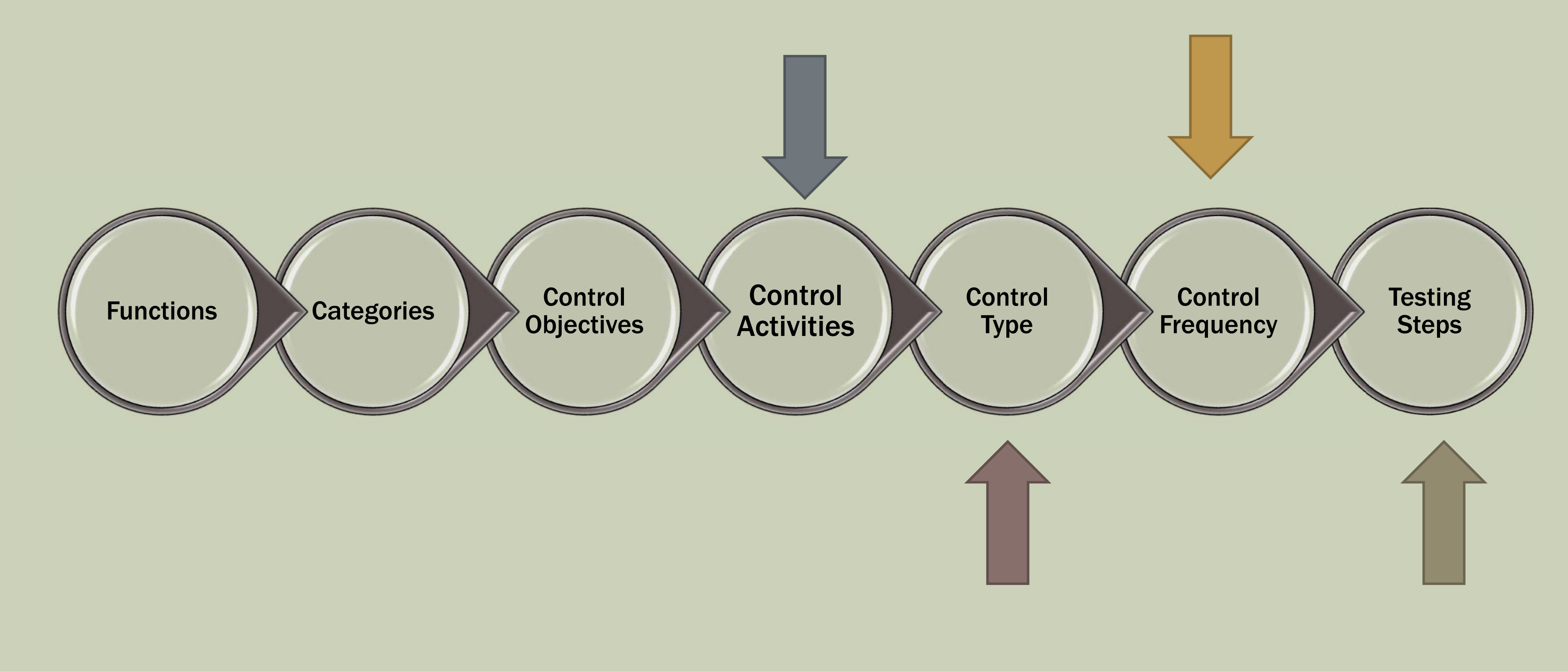
COBIT AUDIT WORK PROGRAM



IS Audit/Assurance Progam
Cybersecurity: Based on the NIST Cybersecurity Framework - Identify

Process Sub-Area	Ref. Risk	Control Objectives	Controls	Control Type	Control Classification	Control Frequency	Testing Step	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/ Standards	Ref. Workpaper	Pass/ Fail	Comments
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	BAI09.01; BAI09.02		ISO/IEC 27001:2013 A.8.1.1; A.8.1.2			
			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	BAI09.01; BAI09.02; BAI09.05		ISO/IEC 27001:2013 A.8.1.1; A.8.1.2			
			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.	DSS05.02	APO01.04	ISO/IEC 27001:2013 A.13.2.1			
			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). b. Completeness of inventory (e.g., location, third party, owner, etc.) c. Inventory collection process ensures new systems are collected accurately and in a timely manner (e.g,. automated software to detect and/or store the inventory)			ISO/IEC			

COBIT 5 – AUDIT WORK PROGRAM



Functions

Categories

Control Objectives

Control Activities

Control Type

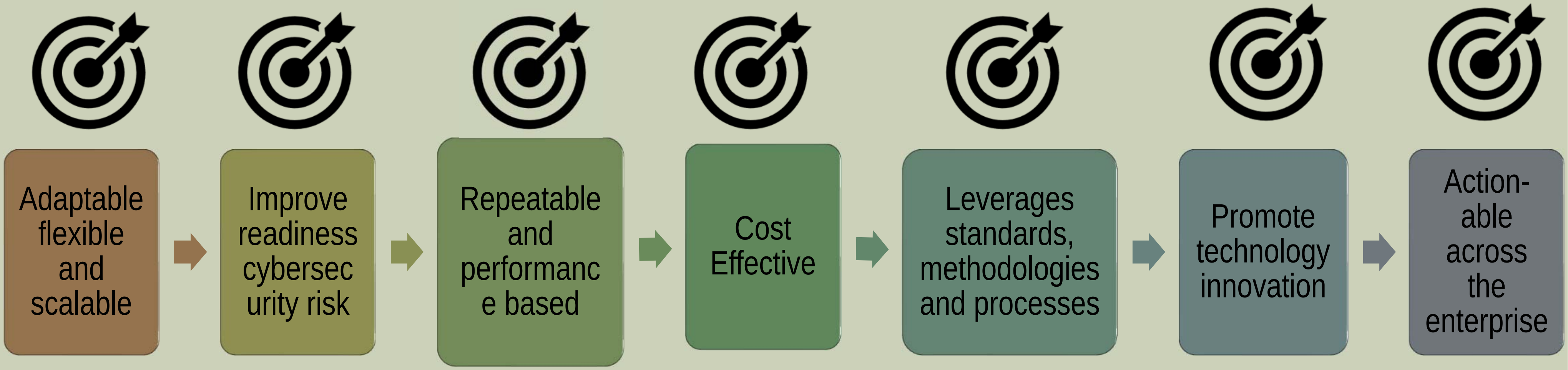
Control Frequency

Testing Steps

CYBERSECURITY ASSESSMENT

NIST

NIST CYBERSECURITY FRAMEWORK



Adaptable flexible and scalable

Improve readiness cybersecurity risk

Repeatable and performance based

Cost Effective

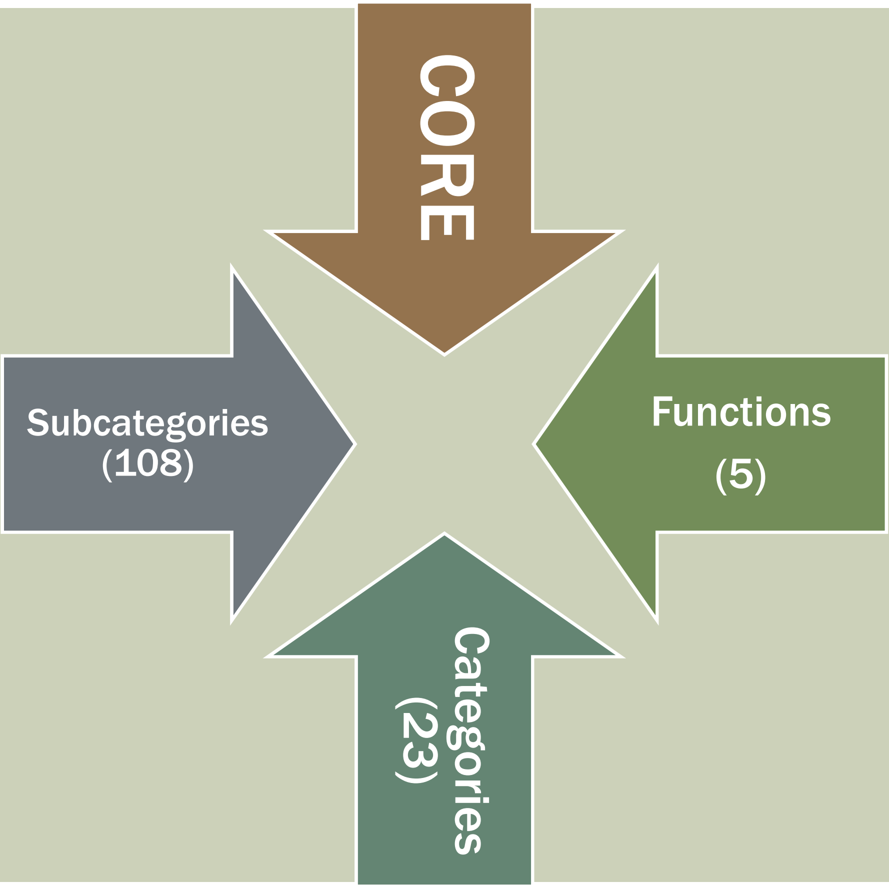
Leverages standards, methodologies and processes

Promote technology innovation

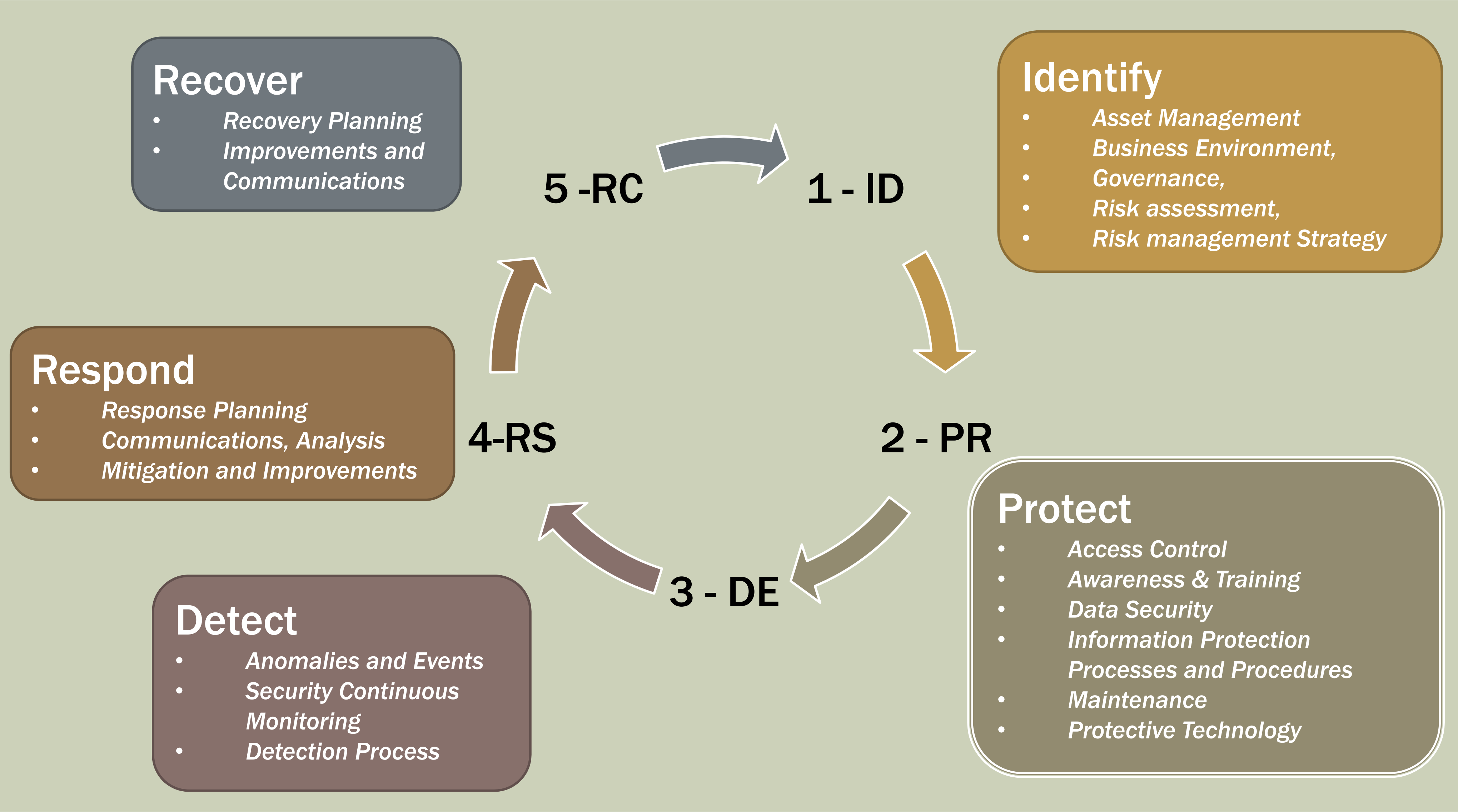
Actionable across the enterprise

CORE PROFILE TIERS

NIST FRAMEWORK - *CORE*



- Strategic view of the life cycle of risk
- Based on incident management review
- Organization Profile / Security Posture
- Not designed to be a checklist



1 - ID

Identify

- Asset Management
- Business Environment,
- Governance,
- Risk assessment,
- Risk management Strategy

2 - PR

Protect

- Access Control
- Awareness & Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

3 - DE

Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

4-RS

Respond

- Response Planning
- Communications, Analysis
- Mitigation and Improvements

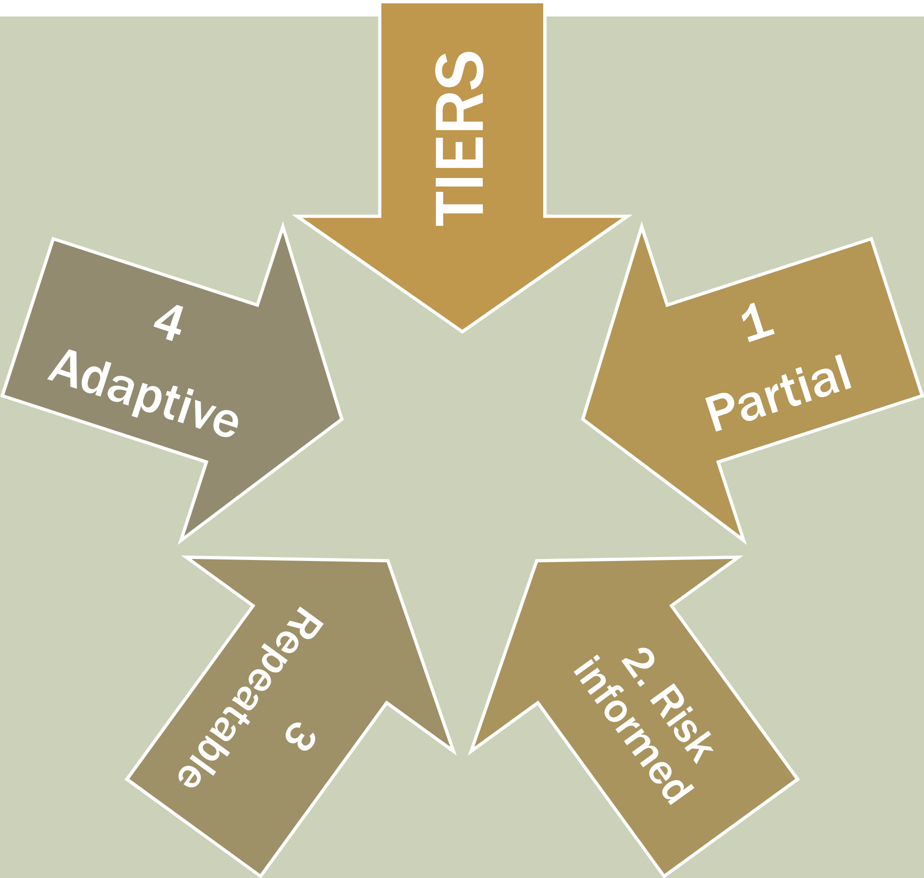
5 -RC

Recover

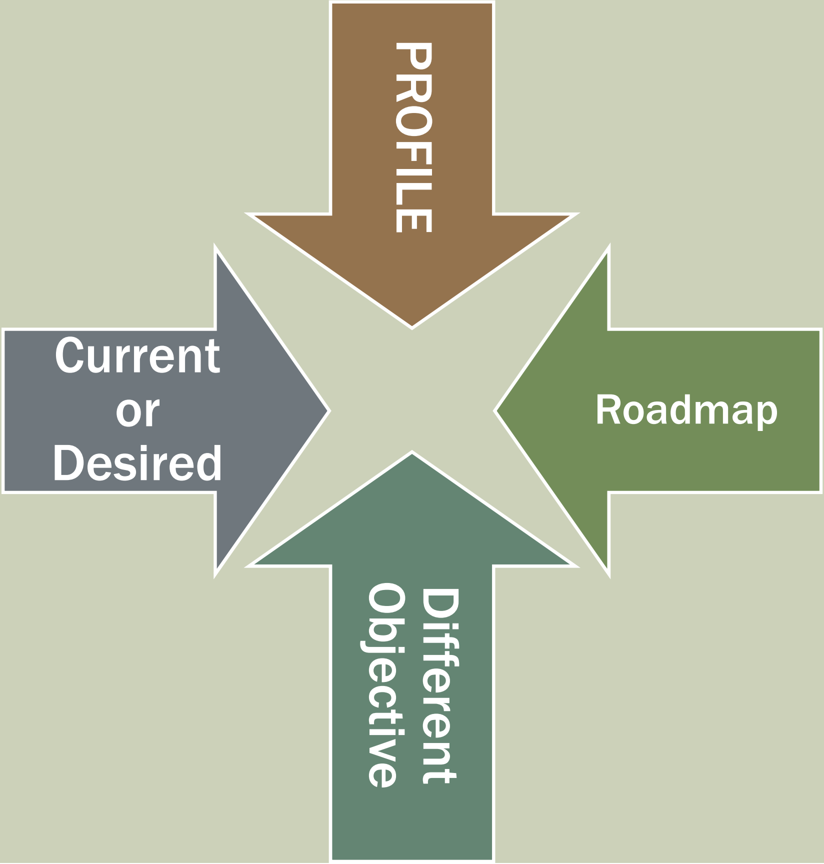
- Recovery Planning
- Improvements and Communications

NIST FRAMEWORK - *TIERS*

- Describes how risk is managed
- Reflect progression
- Not maturity model
- Considers supply chain
- Process, Program and Participation

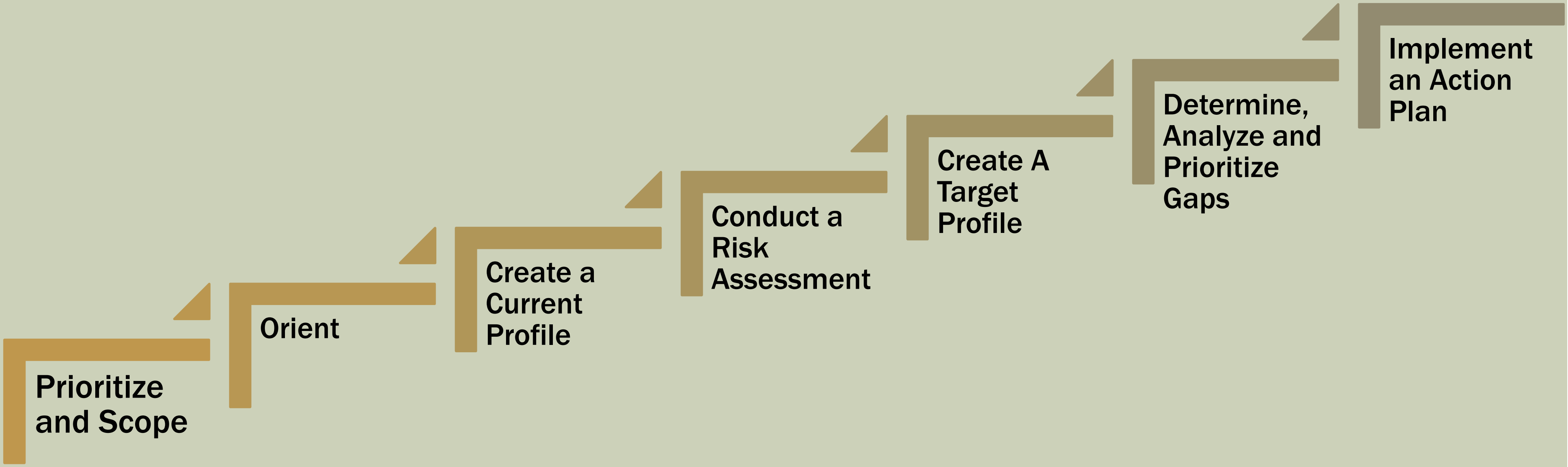


NIST FRAMEWORK - *PROFILE*



- Alignment of core elements with the tiers
- Current vs. target
- Gap analysis
- Corrective action plan

NIST FRAMEWORK – IN PLAY



Prioritize and Scope

Orient

Create a Current Profile

Conduct a Risk Assessment

Create A Target Profile

Determine, Analyze and Prioritize Gaps

Implement an Action Plan

CYBERSECURITY – AT A GLANCE

Individual Focused Areas

CLOUD COMPUTING

- Review internal process for vendor selection, management and monitoring
- Identify vendor risk profiles
- Evaluate contracting process / right to audit
- Use of frameworks/best practices
- Obtain Security Standard Certification / periodic audit
- Survey vendors

DISASTER RECOVERY END USER AWARENESS

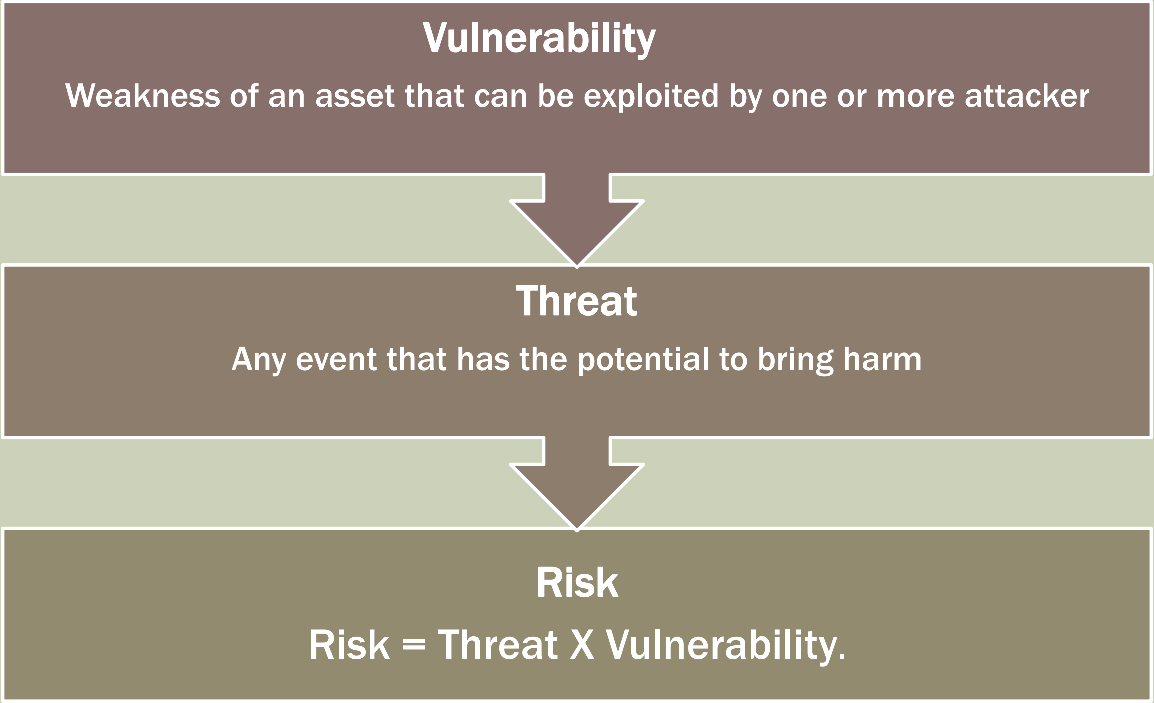
Disaster Recovery

- Backup of data
- Quality of backed up data
- Time to recover
- Testing of data

End User Awareness

- Training
- Evaluate improvement in social behavior
- Reinforce
- Habit

MINI RISK ASSESSMENT



Vulnerability

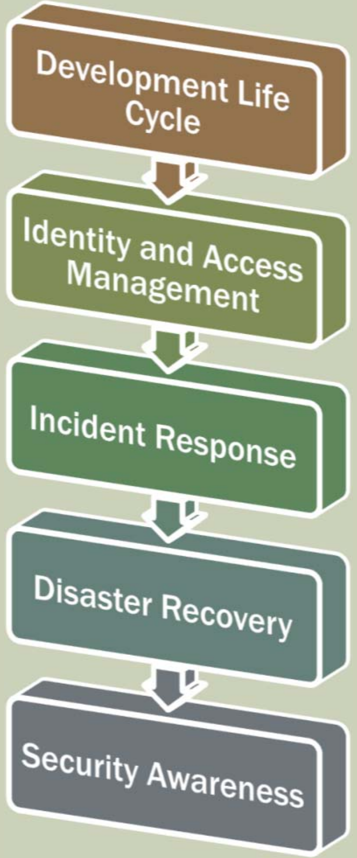
Weakness of an asset that can be exploited by one or more attacker

Threat

Any event that has the potential to bring harm

Risk

Risk = Threat X Vulnerability.



SECURITY OBJECTIVES / CYBERATTACKS

	Confidentiality	Integrity	Availability
Types of Attacks	• Password attacks • MiTM / Session Hi-Jacking • Phishing/Spear/Clone • Cracking encrypted data • Data leakage • Spyware/Malware	• Unauthorized dB scans • Maliciously accessing servers and forging records • Malware/Spyware/Ransomware	• DDoS Attacks (APT) • Ransomware • Disrupting or flooding a server
Audit Topics	• Access control • Encryption • Password policies • End user training	• Intrusion Detection • Data Analytics • Data Classification • Patch management • Password • Access Controls	• Backup and recovery • Data Replication • Bandwidth • Network Segmenting • System Hardening

INTEGRITY - APPLICATION SECURITY

Risk	What Happens
Injection Flaw	Sends untrusted data to an interpreter that is executed as a command without proper authorization
Broken Authentication & Session Management	Compromise passwords, keys, or session tokens to take control of users’ account to assume identities
Sensitive Data Exposure	Access information such as financial data, usernames and passwords to commit fraud
XML External Entity	Use references in XML documents to attack using remote code execution and to disclose internal files
Broken Access Control	Authenticated users access unauthorized functionality or data and modifying data and access rights
Security Misconfiguration	Improper implementation of controls and not patching or upgrading systems
Cross-Site Scripting	Attackers inject client-side scripts into the application and redirect users to malicious websites
Insecure deserialization	Execute code in the application remotely, tamper or delete serialized objects, and elevate privileges
Using Components With Known Vulnerabilities	Exploit an insecure component to take over the server or steal sensitive data
Insufficient Logging and Monitoring	Attackers pivot to other systems and maintain persistent threats

APPLICATION SECURITY LAYER

AUDIT TECHNIQUES

- Adequate segregation of duties between different application environments
- Logical access controls at different layers
- Source code controls (change management)
  - Secure source code
  - Monitor for changes in source code
  - Treat code like intellectual property
  - Inquire / Suggest/ Inspect code reviews
- Education and training developers and application security managers
- Emergency change process controls

BEING IN THE KNOW

Good to know

INFORMATION SECURITY

VS.

CYBERSECURITY

Information Security

Protects data from any illegal access

Applies to physical and digital information

Protects information from unauthorized access, disclosure, use, modification, disruption or destruction

Uses the security triangle

Professionals develop strategies, policies, solutions and risk management

Cybersecurity

Protects data from unauthorized digital access

Applies to digital information only

Protect information from cybercrime, cyber frauds, and law enforcement

Protecting social media accounts and personal details

Professionals perform data recovery, reporting security metrics, and install antimalware software

THINGS TO CONSIDER

- Shadow IT (USB Keys, Smart phones)
- Mobile Working /Telecommuting data is in transit – look for telecommuting policies and confidentiality and integrity of data
- Bring your own device
- Data Analytics
- Cyber attack process

SUMMARY

- Defined cybersecurity and its elements

- How to leverage existing guidelines/frameworks and provide assurance, assessment or snapshot of cybersecurity at your organization

- Lesser known risks that are on the horizon for consideration

COPYRIGHT PAGE

Information for this presentation was sourced from the following:

- *Auditing Cyber Security: Evaluating Risk and Auditing Controls* Information Systems Audit Control Association
- *Cybersecurity Fundamentals Glossary* Information Systems Audit Control Association
- *CoBIT 5 Vendor Management* Information Systems Audit Control Association
- *Frame for Improving Critical Infrastructure Cybersecurity Version 1.1* National Institute of Standards and Technology
- *Cybersecurity and the role of internal audit* Deloitte
- *Definition of Cybersecurity: Gaps and overlaps in standardizatio*n European Union Agency for Network and Information Security
- *What you can do to combat cyber attacks* National Cyber Security Centre
- *10 Steps to Cyber Security* National Cyber Security Centre
- Differencebetween.net – Infographic for information security vs. cybersecurity
- *Fundamentals of Cybersecurity* edureka.com
- *Cybersecurity 101* npr.com
- Cybersecurity project.com
- Vericode.com
- Wikipedia.com
- Open Web Application Security Project (OWASP)

QUESTIONS / THANK YOU!

You Just Don't Get IT
MASERGY
I NEED COMPLETE ASSURANCE THAT THERE'S NO WAY WE CAN GET HACKED.
OUR SECURITY POSTURE IS PRETTY GOOD, BUT I CAN'T GUARANTEE THAT WE WILL NEVER BE HACKED! THERE ARE SO MANY WAYS ...
IF YOU CAN'T GUARANTEE THE CYBER SAFETY OF THIS COMPANY I'LL FIND SOMEONE WHO CAN...
WELL, THERE IS ONE WAY...
GOOD. MAKE IT HAPPEN!
YOINK!
INTERNET
POWER
youjustdontget.it