PUTTING THE “PRO” IN PROACTIVE: BUILDING A NEXT-GEN CYBERSECURITY PROGRAM

DAN DIDIER
@GREYCASTLESEC

Introduction

Problem Statement

Cybersecurity is a strategic business issue that does not have the visibility necessary for the business to make relevant, practical and effective decisions, and has the following impacts:

- Budgeting for cybersecurity isn't performed at the strategic level.
- Inability to quantify the strategic importance of cybersecurity.
- False sense of security whereby technical solutions are seen as both the only option and the right option.
- Do not have a defensible position.
- Risk owners are not able to be accountable for their decisions (or lack thereof)

Why We’re Here

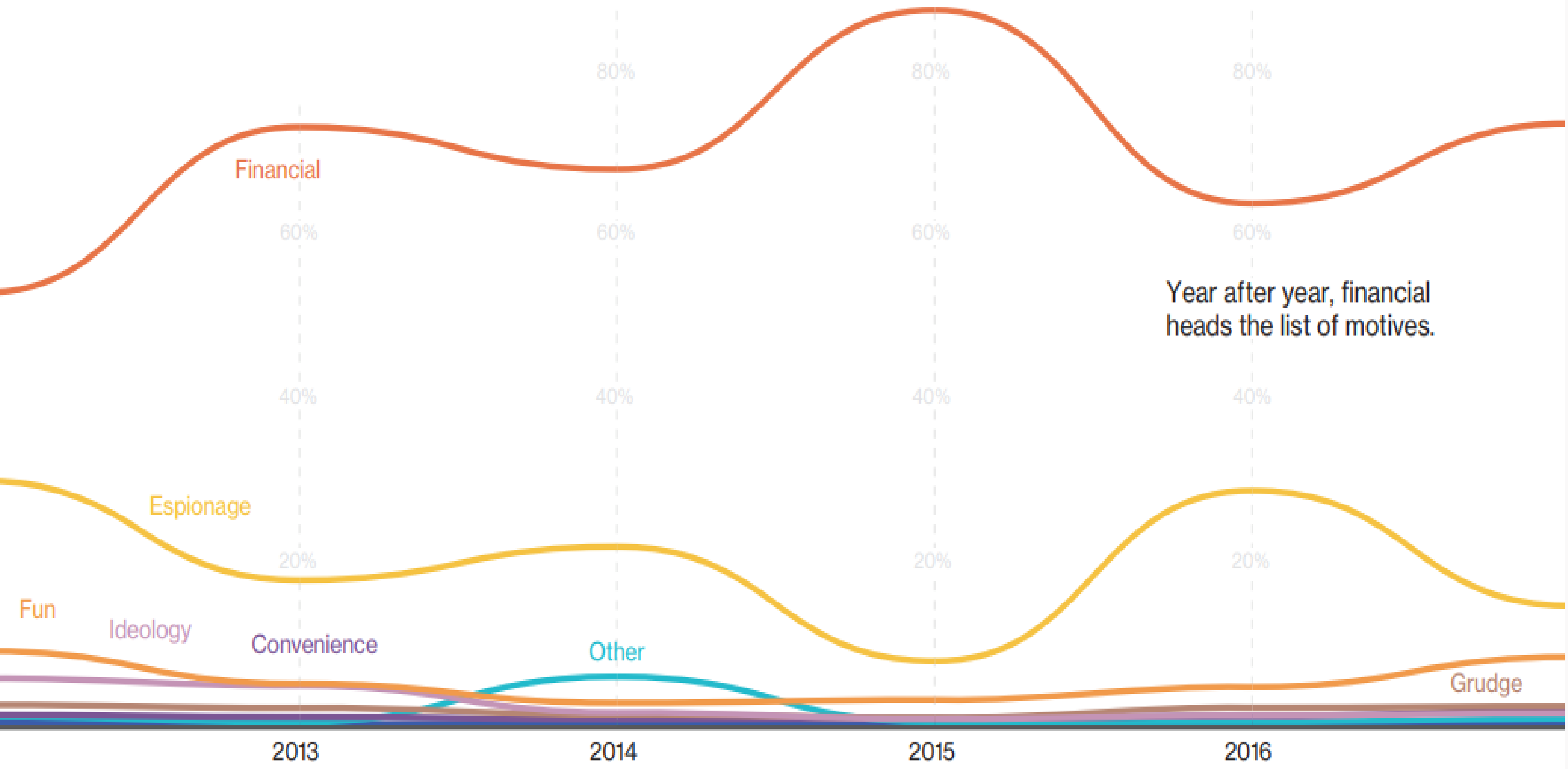
The New Face of Organized Crime

Hackers are no longer lone wolves. They're now banding together to run fewer—yet much larger—attacks, similar to the traditional crime rings of the 20th century.

80%

of cyber-attacks are driven by **organized crime rings,** in which data, tools, and expertise are widely shared.[1]

The Motives Behind Attacks



Year after year, financial heads the list of motives.

Elvis Rodriguez & Emir Yasser

Getting security right is hard for the best teams in the world.

It's impossible for average teams.

Bruce Shneier

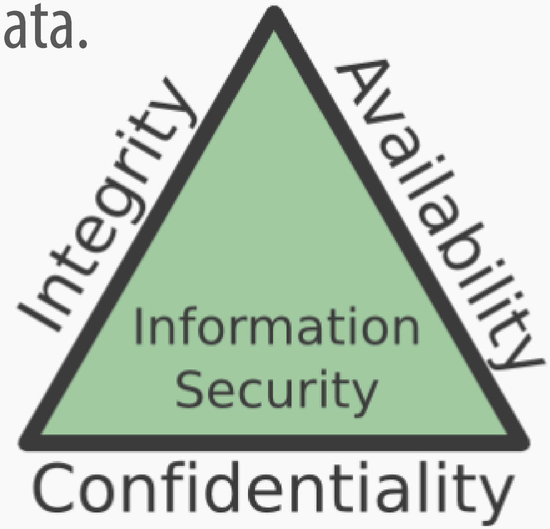
Perception,
Emotion & Reality

Business Change

- Every day there are changes to the business that impact risk.
- Not only is the business composition very different, but changes are constant:
  - Business Process
  - People
  - Technology

~~Keep on Keeping on~~

- Cybersecurity wouldn't exist if we didn't have data.
- The way data is processed, stored, created and transmitted is ever-changing.
- The nature and impact of attacks can and will change quickly and without warning:
  - Breach vs. Ransomware



Right Decision
Wrong Decision

Case-in-Point

- Someone runs in and informs you that there was a huge mess of water on the floor from the thunderstorm last night and found there is a **huge hole in the roof**.
- What do you do?
- You and everyone else is very likely to suggest that we **immediately fix the hole** in the roof. After all, there is a hole in the roof and everything is getting wet.

Summary

- Cybercrime is organized and largely financially motivated.
- Different Industries have to pay attention to unique vulnerabilities and exploits.
- Business constantly changes: people, process, technology.
- Cannot secure your business using the same tactics as your competitors or partners.
- Must avoid emotion and use actionable data
- Must use risk as common language

Build a Next-Gen Cybersecurity Program

Objectives

- Spend only what is necessary to reasonably secure the business
- Create a defensible position
- Set clear direction
- Enable buy-in and ownership
- Keep your job

VISION STATEMENT

TO BE THE WORLD'S LEADING PROVIDER OF RELEVANT, PRACTICAL AND EFFECTIVE CYBERSECURITY SOLUTIONS.

Six Steps to Building a Cybersecurity Program

Step 1 - Identify and Inventory Data Assets

Step 2 - Conduct a Risk Assessment

Step 3 - Implement Governance

Step 4 - Implement Policies, Standards and Controls

Step 5 - Implement and Align Supporting Plans & Procedures

Step 6 - Ensure Program Integrity & Course Correct

Step 1

Data Asset Inventory

Data Asset Inventory

- Build a comprehensive list of data assets
  - Data assets are not information assets
  - Information Assets (Servers, workstations, switches, routers, firewalls, laptops, mobile phones, etc.) exist for the sole purpose of processing, storing or transmitting data.
- Data Assets
  - Structured and unstructured
  - Stored anywhere (locally, cloud, database, business partner, thumb drive)
  - Needed (in most cases) to run the business and has inherent risk

Identify (risk) Owners and Classification

- Organized data sets by owner and classification
  - All data is owned (HR, Finance, Development, R&D, IT)
  - All data has a classification
  - Define categories in a policy and create a functional procedure to ensure consistent classification
- Watch out: IT owns almost zero data
  - Know the difference between a data owner and a custodian
  - Know the difference between a data owner and an information asset owner

Build an Actual Inventory

1. Interview each department and document what data sets they have (or believe they have)

2. Identify the volume of data

3. Identify the data owner (Department and individual)

Fill in the Blanks

1. Identify where the information resides (information system, partner, cloud, etc.)
2. Identify the information system owner
3. Identify legal or contractual requirements
4. Identify availability requirements
5. Classify the data
6. Identify minimum security controls for each data classification
7. Enable collaboration between the data owner and information asset owner to ensure minimum controls are implemented

Step 2

Risk Assessment

Risk Assessment

- The process of risk assessment enables a repeatable and measurable way for all parties to understand business impacts and select reasonable controls to facilitate remediation, without having to understand the underlying complexities.
- Select appropriate standards for baseline/compliance and ensure the scope is clear and understood by all.

Select Standards

- FISMA
- NERC CIP
- HIPAA
- PCI-DSS
- SOX
- GLBA
- MASS 201 CMR 17
- NYS DFS
- DFARS
- GDPR
- IRS Publication 1075
- FERPA
- ISO 27001
- NIST 800-53
- NIST 800-171
- NIST CSF
- FFIEC
- DSRIP
- fedRAMP
- Privacy Shield
- Business Legal Contracts

GreyCastle security

Select Controls

1. Access Control
2. Media Protection
3. Awareness and Training
4. Personnel Security
5. Audit and Accountability
6. Physical Protection
7. Configuration Management
8. Risk Assessment
9. Identification and Authentication
10. Security Assessment
11. Incident Response
12. System and Communications Protection
13. Maintenance
14. System and Information Integrity

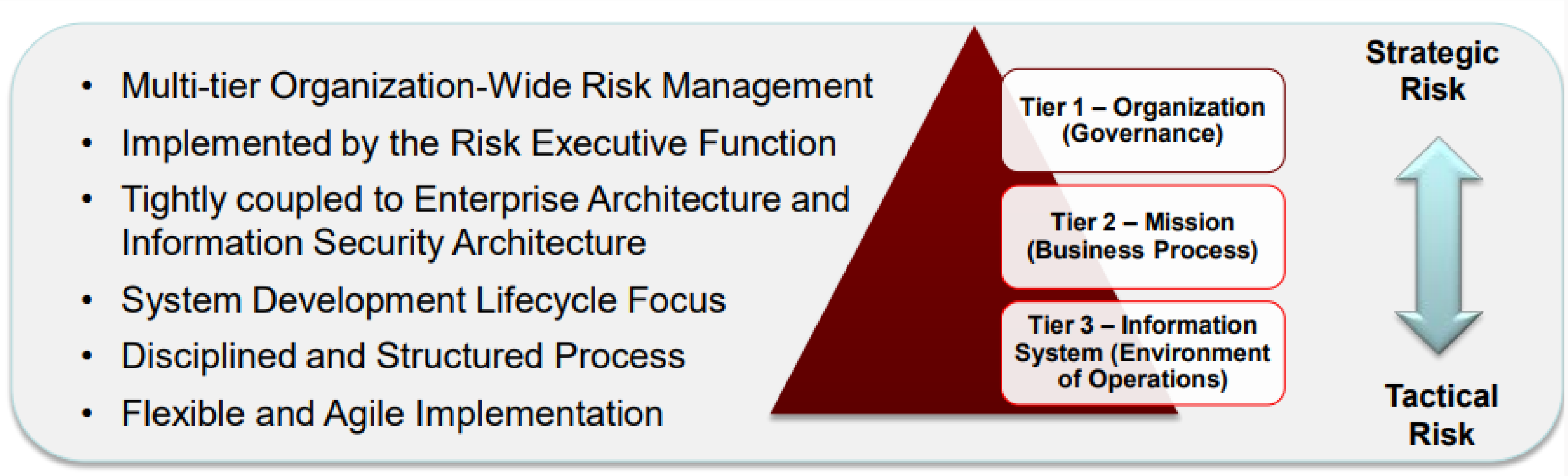
Key Steps to Risk Assessment

1. Characterize system boundaries, criticality and sensitivity
2. Identify **vulnerabilities**
3. Identify **threats**
4. Review existing **controls**
5. Determine **probability** of a threat exploit
6. Assess the **impact** of threat exploitation
7. Calculate **risk**
8. Identify reasonable **controls** to mitigate risk
9. Document the **findings**

Must. Resist. Temptation.

The Three Tiers of Risk Management (NIST 800-39)

- Organizational Tier
- Business Process Tier
- Information Systems Tier



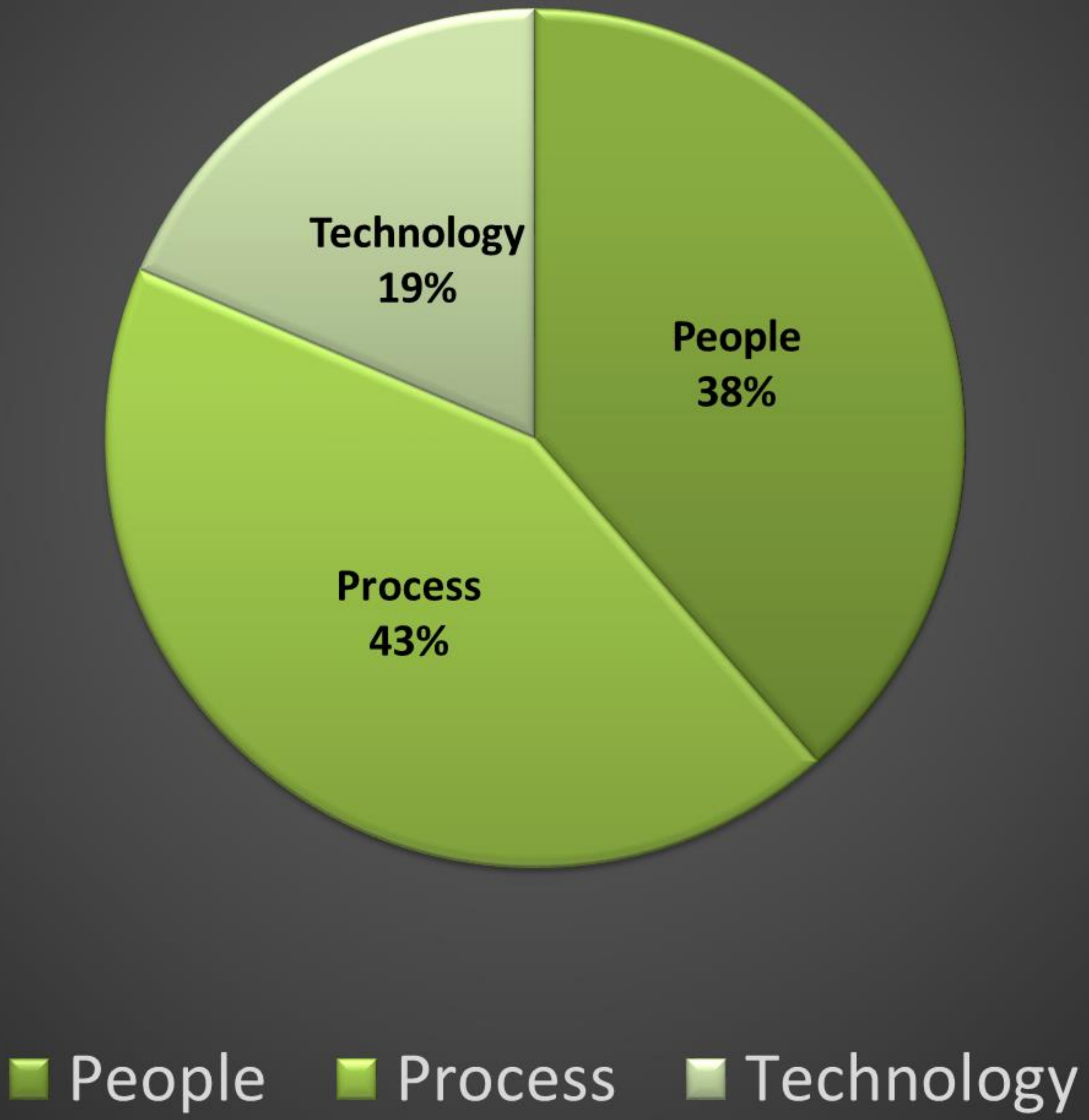
- Multi-tier Organization-Wide Risk Management
- Implemented by the Risk Executive Function
- Tightly coupled to Enterprise Architecture and Information Security Architecture
- System Development Lifecycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation

Tier 1 – Organization (Governance)
Tier 2 – Mission (Business Process)
Tier 3 – Information System (Environment of Operations)
Strategic Risk
Tactical Risk

COGNITIVE BIAS

BEWARE THE CURSE OF KNOWLEDGE

Findings by Category



Step 3

Governance

Objectives

- Make strategic business decisions for cybersecurity
  - Subset of corporate governance
- Establish the appropriate level of security for the environment
- Inform the cybersecurity budget planning process
- Satisfy regulatory and legal requirements
- Establish ownership and visibility around risk management
- Communicate cybersecurity risks clearly and comprehensively to senior leadership, including the Board

Information Security Officer

- An information security officer will be appointed with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. Responsibilities will include:
  - Oversight of development, maintenance, and distribution of policies, procedures and plans
  - Ensure controls are defined and implemented
  - Ensure responsibilities and assignment for monitoring alerts and incident response processes are understood and performed
  - Development, maintenance, and implementation of a security incident response plan
  - Ensure all access control processes are monitored
  - Report to the board on the risk management process, including top risks, remediation plans and status.

Steering Committee

The Information Security Steering Committee provides a number of “soft” benefits, including those gained by the active participation of business leaders in information security decision-making. The Information Security Steering Committee shall:

- Establishing goals for the Information Security program.
- Review and approve Information Security policies and standards.
- Recommend, review and prioritize information security initiatives.
- Communicate information security needs.
- Review the effectiveness of the Information Security program and resources.
- Ensure corrective action plans have been developed and implemented to address risks.

Ownership

- Participation and accountability is required from departments and individuals across the business:
  - Legal
  - Human Resources
  - Risk Management
  - Compliance
  - Safety
  - Research & Development
  - Physical Security
  - Information Technology
  - Information Security

Ownership - Control Areas

Controls	**Impacted Areas**						
	Security	IT	Audit / Compliance	HR	Physical Security	Finance / Procurement / Legal	Business Office / Administration
Access Control	X	X	X	X	X	X	
Awareness & Training	X	X	X	X			
Audit & Accountability	X	X	X	X	X	X	
Security Assessment & Authorizations	X	X	X				
Configuration Management	X	X	X				
Contingency Planning	X	X					X
Identification & Authentication	X	X	X				
Incident Response	X	X		X	X	X	
Maintenance	X	X			X		

Step 4

Policies, Standards and Controls

Policies

- Three/Four major policy documents:
  - Information Security Policy
  - Data Classification Policy
  - Acceptable Use Policy
  - Privacy Policy
- Have a single Information Security Policy for all security efforts. Do not create standalone policy documents
  - One policy for common functions reduces confusion and overhead, and enables compliance.

publication is structured into 18 control groupings, herein referred to as Information Security Standards. These Standards must meet all statutory and contractual requirements.

7.1 ACCESS CONTROL (AC)

ABC Company must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

7.2 AWARENESS AND TRAINING (AT)

ABC Company must: (i) ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security of organization information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

7.3 AUDIT AND ACCOUNTABILITY (AU)

ABC Company must: (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum; and (ii) ensure that the actions of individual information system users can be uniquely traced for all restricted systems.

7.4 ASSESSMENT AND AUTHORIZATION (CA)

ABC Company must: (i) periodically assess the security controls in organization information

Standards

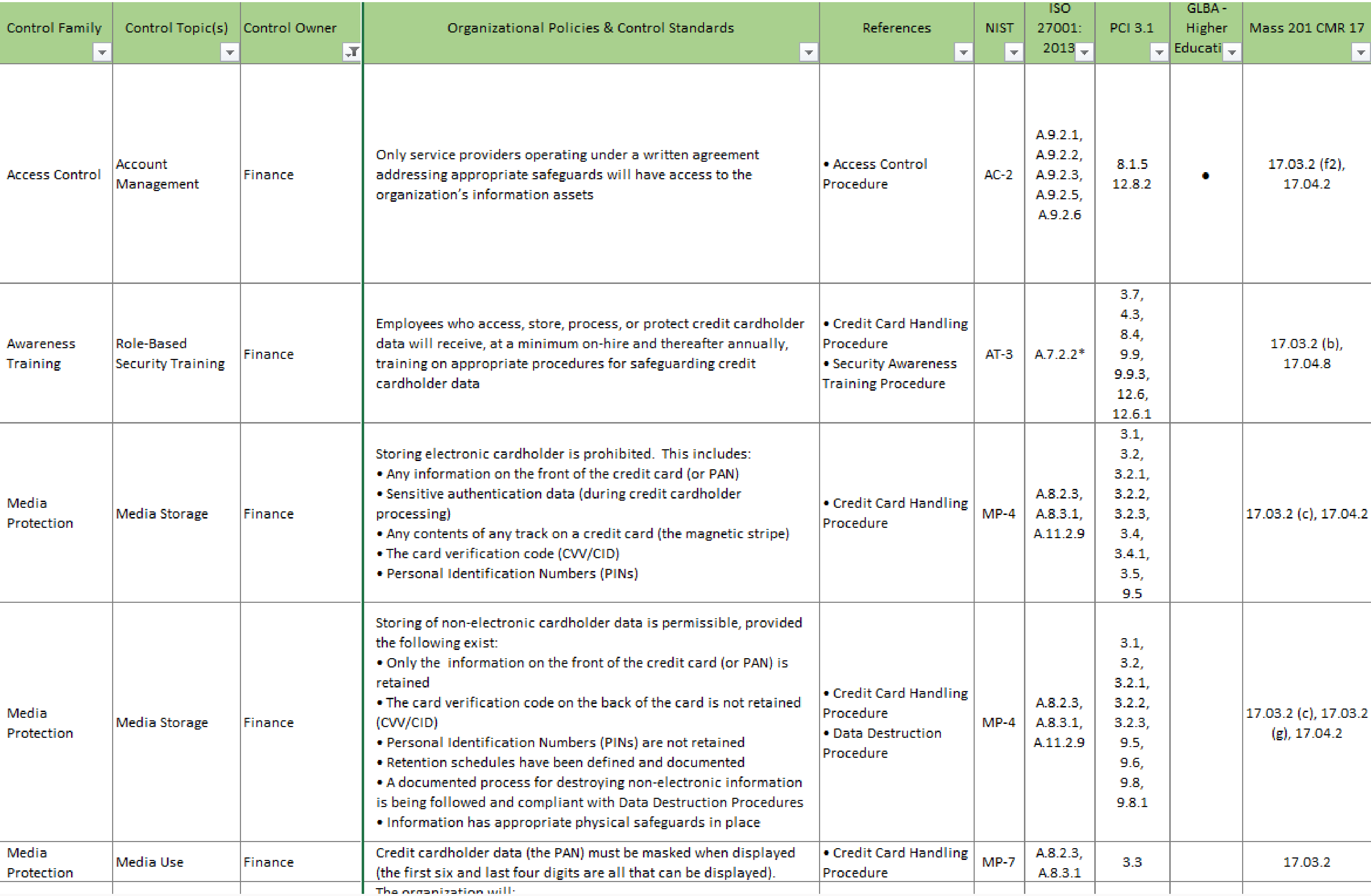
- Address Multiple Regulations:
  - NIST, PCI , GLBA, FERPA,, ISO 27001/2 , GDPR, etc.
- Establishes Security Position and Ownership in support of Policy
- Common Control Families
  - Access Control
  - Awareness & Training
  - Audit & Accountability
  - Security Assessments & Authorizations
  - Configuration Management
  - Contingency Planning
  - Identification & Authentication
  - Incident Response
  - Maintenance
  - Media Protection
  - Personnel Security
  - Physical and Environmental Protection
  - Planning
  - Risk Assessment
  - System and Services
  - System & Communication Protection
  - System & Information Integrity
  - Program Management

GreyCastle security

Policies vs. Standards

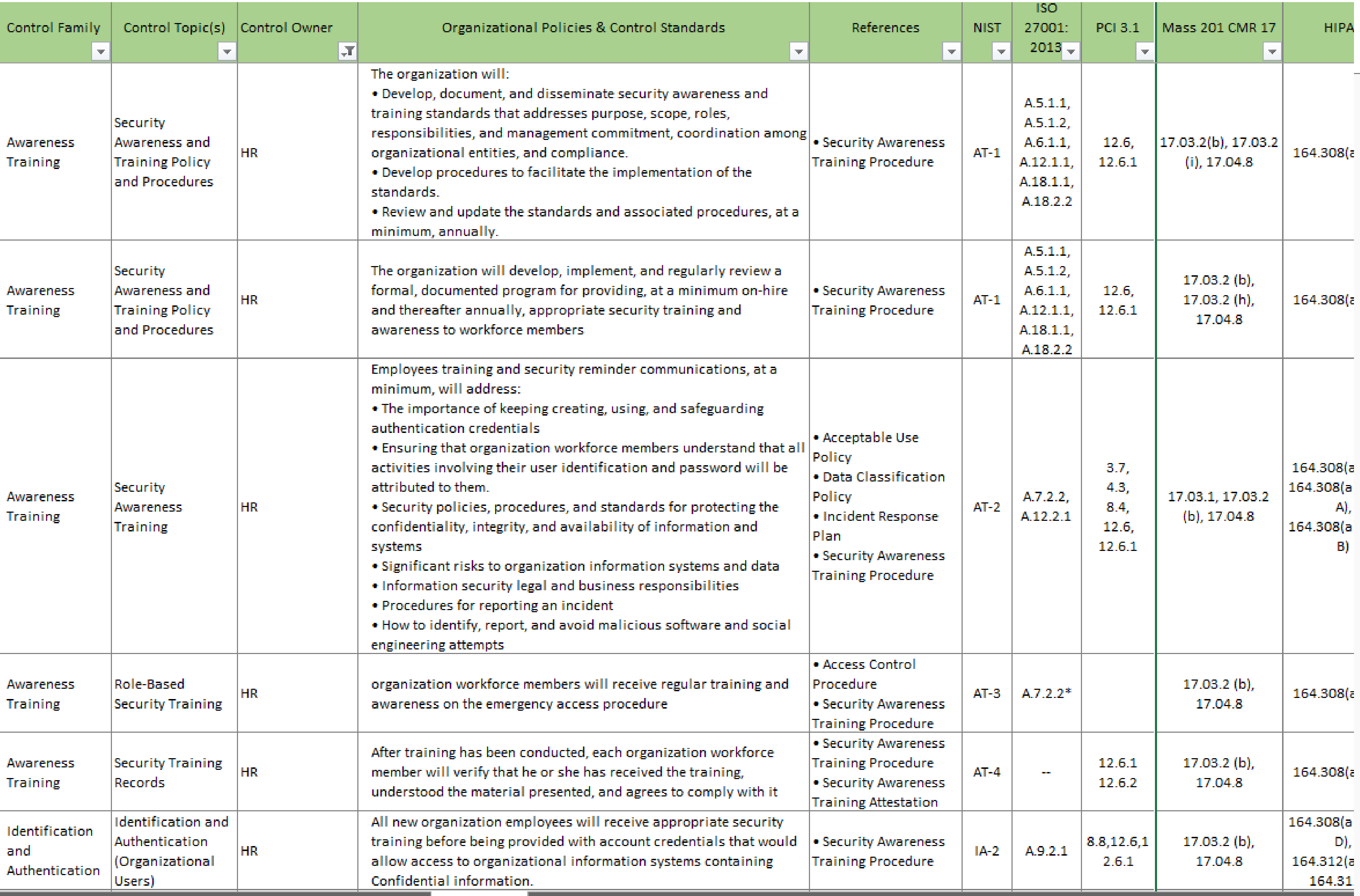
- Policies (Information Security, Acceptable Use, Data Classification)
  - Describe the direction
  - High level Objectives that are clear and distinct to all that read them
  - Ex: You must build a house.
- Standards
  - Describe rules for what you will do
  - Ex: You must build a house with 4 bedrooms and two baths that complies with local building codes.

Control Standards (Finance)



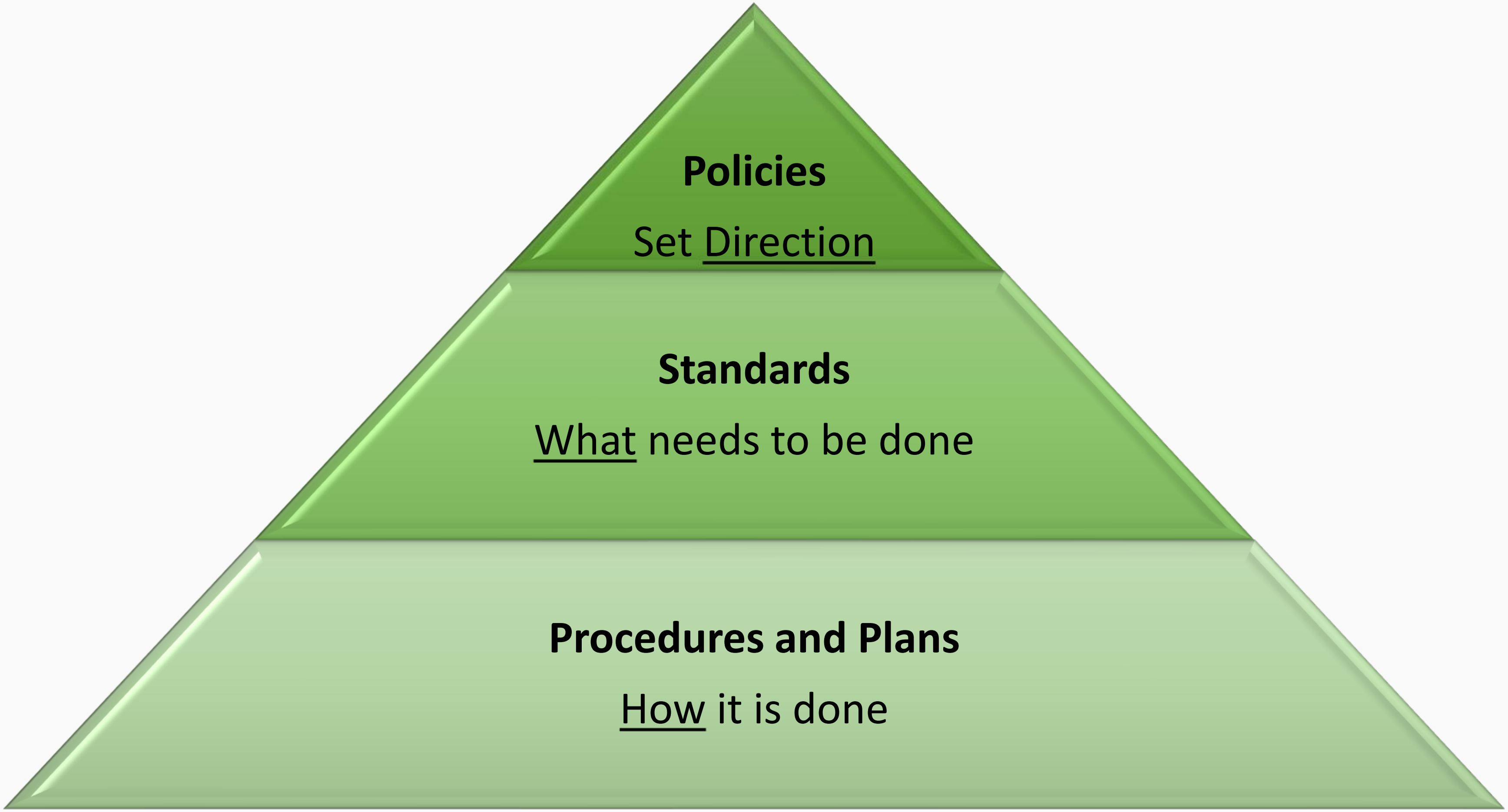
Control Family	Control Topic(s)	Control Owner	Organizational Policies & Control Standards	References	NIST	ISO 27001: 2013	PCI 3.1	GLBA - Higher Educati	Mass 201 CMR 17
Access Control	Account Management	Finance	Only service providers operating under a written agreement addressing appropriate safeguards will have access to the organization's information assets	• Access Control Procedure	AC-2	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	8.1.5 12.8.2	•	17.03.2 (f2), 17.04.2
Awareness Training	Role-Based Security Training	Finance	Employees who access, store, process, or protect credit cardholder data will receive, at a minimum on-hire and thereafter annually, training on appropriate procedures for safeguarding credit cardholder data	• Credit Card Handling Procedure • Security Awareness Training Procedure	AT-3	A.7.2.2*	3.7, 4.3, 8.4, 9.9, 9.9.3, 12.6, 12.6.1		17.03.2 (b), 17.04.8
Media Protection	Media Storage	Finance	Storing electronic cardholder is prohibited. This includes: • Any information on the front of the credit card (or PAN) • Sensitive authentication data (during credit cardholder processing) • Any contents of any track on a credit card (the magnetic stripe) • The card verification code (CVV/CID) • Personal Identification Numbers (PINs)	• Credit Card Handling Procedure	MP-4	A.8.2.3, A.8.3.1, A.11.2.9	3.1, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.4, 3.4.1, 3.5, 9.5		17.03.2 (c), 17.04.2
Media Protection	Media Storage	Finance	Storing of non-electronic cardholder data is permissible, provided the following exist: • Only the information on the front of the credit card (or PAN) is retained • The card verification code on the back of the card is not retained (CVV/CID) • Personal Identification Numbers (PINs) are not retained • Retention schedules have been defined and documented • A documented process for destroying non-electronic information is being followed and compliant with Data Destruction Procedures • Information has appropriate physical safeguards in place	• Credit Card Handling Procedure • Data Destruction Procedure	MP-4	A.8.2.3, A.8.3.1, A.11.2.9	3.1, 3.2, 3.2.1, 3.2.2, 3.2.3, 9.5, 9.6, 9.8, 9.8.1		17.03.2 (c), 17.03.2 (g), 17.04.2
Media Protection	Media Use	Finance	Credit cardholder data (the PAN) must be masked when displayed (the first six and last four digits are all that can be displayed).	• Credit Card Handling Procedure	MP-7	A.8.2.3, A.8.3.1	3.3		17.03.2
			The organization will:						

Control Standards (Human Resources)



Control Family	Control Topic(s)	Control Owner	Organizational Policies & Control Standards	References	NIST	ISO 27001: 2013	PCI 3.1	Mass 201 CMR 17	HIPA
Awareness Training	Security Awareness and Training Policy and Procedures	HR	The organization will: • Develop, document, and disseminate security awareness and training standards that addresses purpose, scope, roles, responsibilities, and management commitment, coordination among organizational entities, and compliance. • Develop procedures to facilitate the implementation of the standards. • Review and update the standards and associated procedures, at a minimum, annually.	• Security Awareness Training Procedure	AT-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	12.6, 12.6.1	17.03.2(b), 17.03.2 (i), 17.04.8	164.308(a
Awareness Training	Security Awareness and Training Policy and Procedures	HR	The organization will develop, implement, and regularly review a formal, documented program for providing, at a minimum on-hire and thereafter annually, appropriate security training and awareness to workforce members	• Security Awareness Training Procedure	AT-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	12.6, 12.6.1	17.03.2 (b), 17.03.2 (h), 17.04.8	164.308(a
Awareness Training	Security Awareness Training	HR	Employees training and security reminder communications, at a minimum, will address: • The importance of keeping creating, using, and safeguarding authentication credentials • Ensuring that organization workforce members understand that all activities involving their user identification and password will be attributed to them. • Security policies, procedures, and standards for protecting the confidentiality, integrity, and availability of information and systems • Significant risks to organization information systems and data • Information security legal and business responsibilities • Procedures for reporting an incident • How to identify, report, and avoid malicious software and social engineering attempts	• Acceptable Use Policy • Data Classification Policy • Incident Response Plan • Security Awareness Training Procedure	AT-2	A.7.2.2, A.12.2.1	3.7, 4.3, 8.4, 12.6, 12.6.1	17.03.1, 17.03.2 (b), 17.04.8	164.308(a 164.308(a A), 164.308(a B)
Awareness Training	Role-Based Security Training	HR	organization workforce members will receive regular training and awareness on the emergency access procedure	• Access Control Procedure • Security Awareness Training Procedure	AT-3	A.7.2.2*		17.03.2 (b), 17.04.8	164.308(a
Awareness Training	Security Training Records	HR	After training has been conducted, each organization workforce member will verify that he or she has received the training, understood the material presented, and agrees to comply with it	• Security Awareness Training Procedure • Security Awareness Training Attestation	AT-4	--	12.6.1 12.6.2	17.03.2 (b), 17.04.8	164.308(a
Identification and Authentication	Identification and Authentication (Organizational Users)	HR	All new organization employees will receive appropriate security training before being provided with account credentials that would allow access to organizational information systems containing Confidential information.	• Security Awareness Training Procedure	IA-2	A.9.2.1	8.8,12.6,1 2.6.1	17.03.2 (b), 17.04.8	164.308(a D), 164.312(a 164.31

Visualizing the Structure



Policies

Set Direction

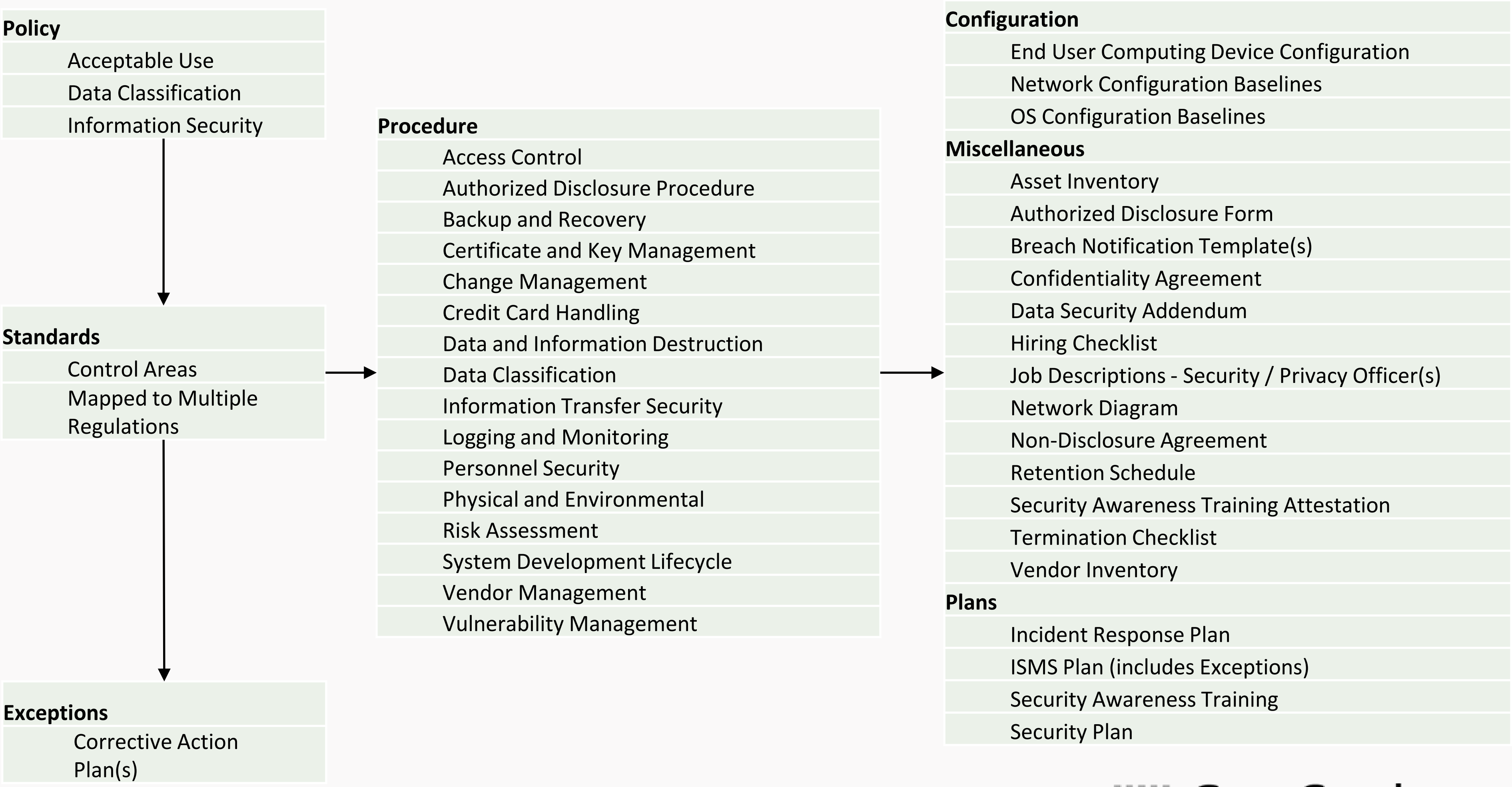
Standards

What needs to be done

Procedures and Plans

How it is done

Documentation Inventory



Policy
- Acceptable Use
- Data Classification
- Information Security

Standards
- Control Areas
- Mapped to Multiple Regulations

Exceptions
- Corrective Action Plan(s)

Procedure
- Access Control
- Authorized Disclosure Procedure
- Backup and Recovery
- Certificate and Key Management
- Change Management
- Credit Card Handling
- Data and Information Destruction
- Data Classification
- Information Transfer Security
- Logging and Monitoring
- Personnel Security
- Physical and Environmental
- Risk Assessment
- System Development Lifecycle
- Vendor Management
- Vulnerability Management

Configuration
- End User Computing Device Configuration
- Network Configuration Baselines
- OS Configuration Baselines

Miscellaneous
- Asset Inventory
- Authorized Disclosure Form
- Breach Notification Template(s)
- Confidentiality Agreement
- Data Security Addendum
- Hiring Checklist
- Job Descriptions - Security / Privacy Officer(s)
- Network Diagram
- Non-Disclosure Agreement
- Retention Schedule
- Security Awareness Training Attestation
- Termination Checklist
- Vendor Inventory

Plans
- Incident Response Plan
- ISMS Plan (includes Exceptions)
- Security Awareness Training
- Security Plan

Step 5

Plans and Procedures

Plans

- Plans are developed using the Policies and Standards as key inputs.
- Plans should address specific processes that require a comprehensive approach to be successful. Typically, plans are needed when multiple business units are required to build and execute:
  - Incident Response Plan, Business Continuity Plan, Secure Architecture Plan, Security Awareness & Training Plan
- Process experts may still be required to ensure the complex nature of these processes are appropriately implemented in-line with the polices, standard and risk appetite of the organization.

Procedures

- Procedures must be developed to ensure appropriate and repeatable processes exist to support the operational execution of security controls and standards:
  - Access Control Procedure , Encryption key Management Procedure, Data Handling Procedure, Risk Assessment Procedure, etc.
- Procedures must use the clear guidance provided by the standards to be effective and in-line with business risk appetite.
- Example: (Finance – Account Management Procedure)
  - Only service providers operating under a written agreement addressing appropriate safeguard will have access to the organization's information assets

Policies vs. Standards vs. Procedures

- Policies (Information Security, Acceptable Use, Data Classification)
  - Describe “What.” High level Objectives.
  - Ex: You must build a house.
- Standards
  - Describe rules for “How” .
  - Ex: You must build a house with 4 bedrooms and two baths that complies with local building codes.
- Procedures
  - Describe “Who” and “How” we implement ***Standards.***
  - Ex: Who frames the house, lays brick, does plumbing, in what timeline and with what technology & tools.

Feedback Process

- As plans and procedures are developed, gaps should be formally identified and sent to the governance team for resolution.

- It is not reasonable to expect control standards to remain static and the process must support the identification of standards that are implement or in draft. It must also support feedback from operations if and when there is a potential conflict.

Step 6

Program ~~Maintenance~~ Integrity & Course Correction

Program Integrity Key Activities

- Program integrity *and* course correction.
- Roles & responsibilities must be updated as resources change.
- Data inventory should be updated annually or upon change.
- Risk Assessment should be performed annually or upon change.
- Risk remediation plans should be actively managed and reported to the board quarterly.
- Policies, standards, controls, plans and procedures should be reviewed annually or upon change.
- Plans should be tested annually or upon change.

Sanity Check

Sanity Checklist

- Did we build a defensible position?
- Are we using Risk to effectively communicate both vertically and horizontally through the business (and avoid jargon)?
- Do we have a clear direction that the board understands and supports?
- Do we have a governance function that establishes clear ownership of all data, controls and risk?
- Does our program support budgeting for cybersecurity-specific needs?
- Did we address all compliance and security requirements?
- Is everyone aware of the top risk items, who owns them and what the remediation plan is?

Thank You!