Thomas Bronack, CBCP

Presentation Topics

- What is Risk Management
- Why Risk Management is Important
- The Rise in Cybercrime costs
- Safeguarding the Organization
- "Whole of World", "Whole of Nation" and "Secure by Design"
- From Risk Management to Automated Compliance

Tom Specializes in:

- Enterprise Resilience,
- Corporate Certification,
- Vulnerability Management,
- Strategic and Tactical Planning,
- Project and Team Management
- Awareness and Training

Risk Management – Introduction and Overview

Contact Information:

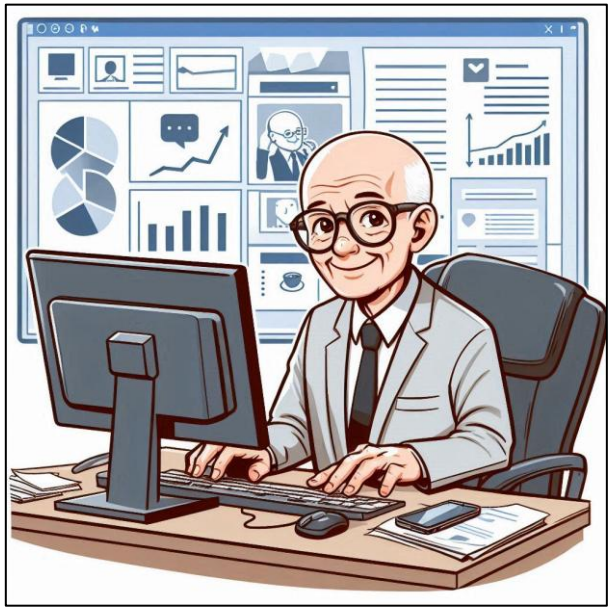
- bronackt@gmail.com
- bronackt@dcag.com
- http://www.dcag.com
- (917) 673-6992

A word from Thomas Bronack

I am a senior level manager with in-depth experience in **Enterprise Resilience, Vulnerability Management, Risk Management, and Corporate Certification** for large enterprises in disciplines like: Banking, Brokerage, Finance, Insurance, Pharmaceuticals, and Manufacturing which provided me with a solid understanding of the risks faced by companies and how best to safeguard a firm through workflow, compliance, and recovery.

I have provided enterprise analysis, evaluation, recommendations, identification of Key Performance Indicators (KPIs), Enterprise Risk Management, and planning materials to eliminate weaknesses and optimize operations. I have optimized the Planning, development, recovery, testing, and production process to provide vulnerability-free and recoverable products / services, while training teams to achieve a safeguarded, efficient, compliant, and vulnerability-free environment.

I follow the "**Whole of Nation**" and "**Secure by Design**" guidelines developed by DHS/CISA to produce vulnerability-free components through a Software Bill of Materials (SBOM) to identify and correct vulnerabilities prior to production and CTEM error identification while in production. This supports the software supply chain and production environment.



A strong generalist with extensive IT industry experience, ready to help you.

Thomas Bronack, CBCP
bronackt@gmail.com
(917) 673-6992

Protecting Organization is more difficult than ever

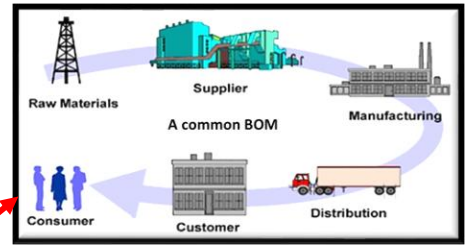
Suppliers

Vendors

Transport

Manufacturing

A World in Turmoil can choke supplies



Supply Issues cause delays in building and delivering goods, and increased costs

Builder Concerns

World Concerns

Delivery Concerns

Customers

Organization

Supply Chain

Technical Problems

Secure by Design

Cyber Crimes

Sales

Marketing

Services

Products

Applications

Engineering

Development

Operations

Inventory

Supply Chain

Delivery

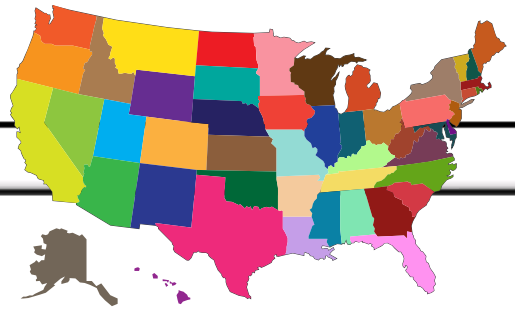
Idea | Engineer Solution | Develop Solution | Verify & Validate | Deploy & Continuity | Audit & Compliance | Deliver | Support & Maintain

Product Engineering and Development Life Cycle

A Whole of World approach to Cybersecurity

Whole of World Approach

Whole of Nation Approach



Department of Homeland Security

Cybersecurity Infrastructure Security Agency

CISA
CYBER+INFRASTRUCTURE

2030 Most Significant Cyber Concerns:

1. Supply Chain Compromises
2. Advanced disinformation campaigns
3. Rise of Digital Surveillance
4. Human error and legacy systems
5. Targeted Attacks
6. Lack of analysis and controls
7. Rise of advanced hybrid attacks
8. Skill shortage
9. Cross-border ICT suppliers as a single-point-of-failure
10. Artificial Intelligence abuse

Vulnerability Management Process:

1. Detect Vulnerability (SBOM)
2. Assess the Risk (CVE)
3. Prioritize Remediation (CVSS, KVE, EPSS)
4. Confirm Remediation
5. Optimize through automation
6. Advance the use of BOMs for Software, Release Control, and Artificial Intelligence

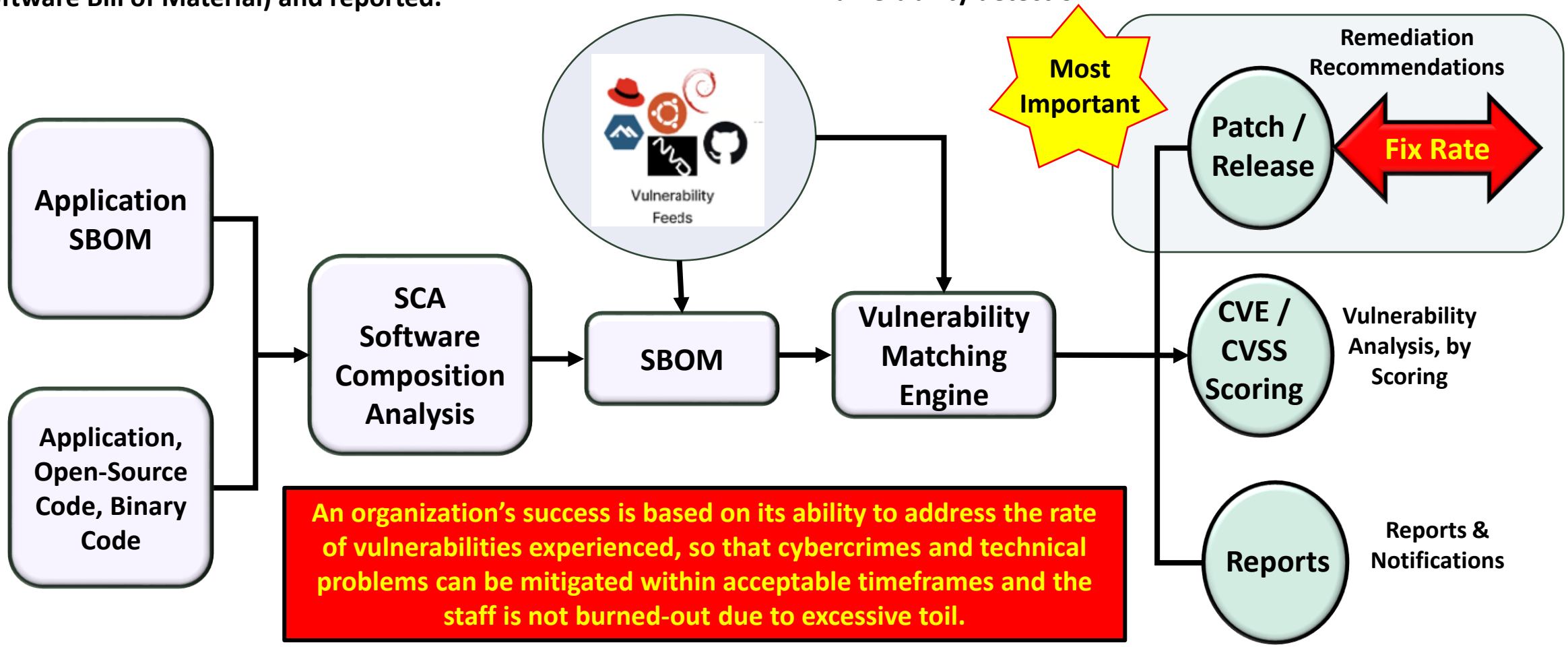
DHS/CISA - Secure by Design principles:

1. Build security considerations into the software requirements specification
2. Address possible abuse cases (e.g., how users may misuse the software).
3. Create and enforce secure code guidelines.
4. Use appropriate security tools.
5. Conduct security audits at multiple stages of the SDLC.
6. Conduct vulnerability testing that includes negative testing and penetration testing.
7. Incorporate security within deployment and maintenance processes.
8. Ensure reused software is from trusted sources and properly evaluated.
9. Provide feedback throughout the process on security effectiveness.
10. Educate developers and QA teams on secure coding techniques.

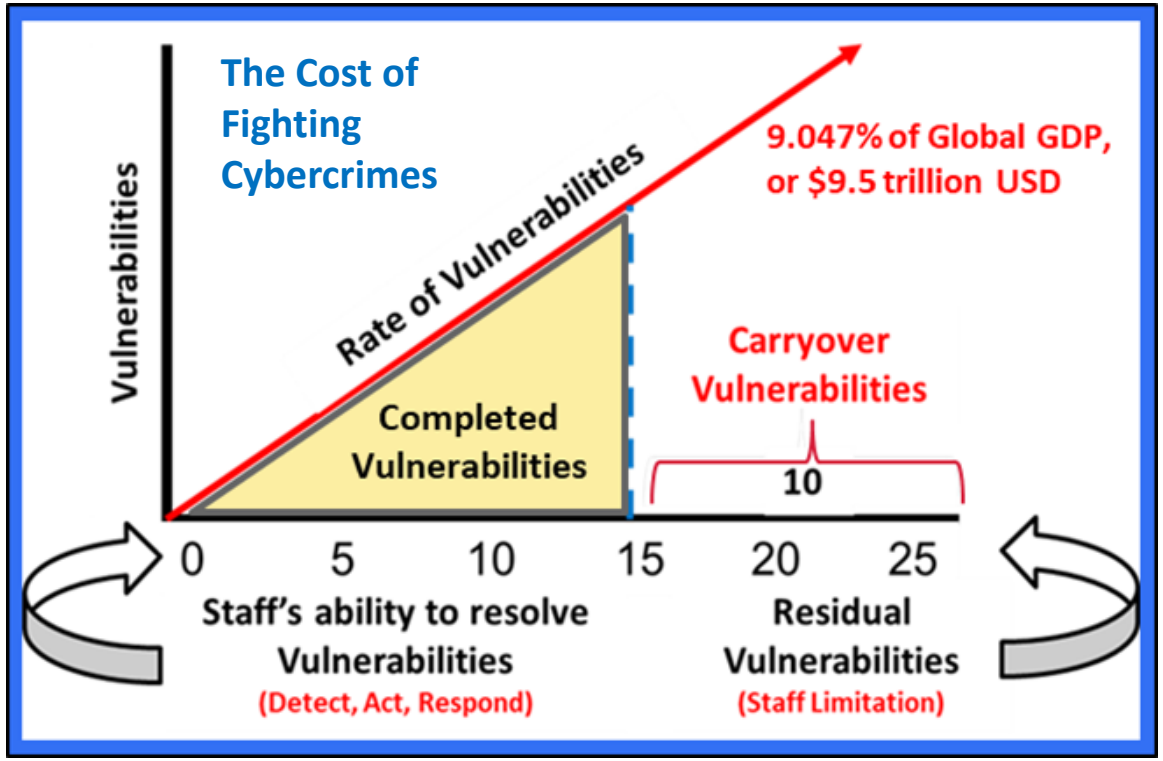
Identifying and Reporting Vulnerabilities

Vulnerabilities are identified within Applications, or existing Application SBOMs (Software Bill of Material) and reported.

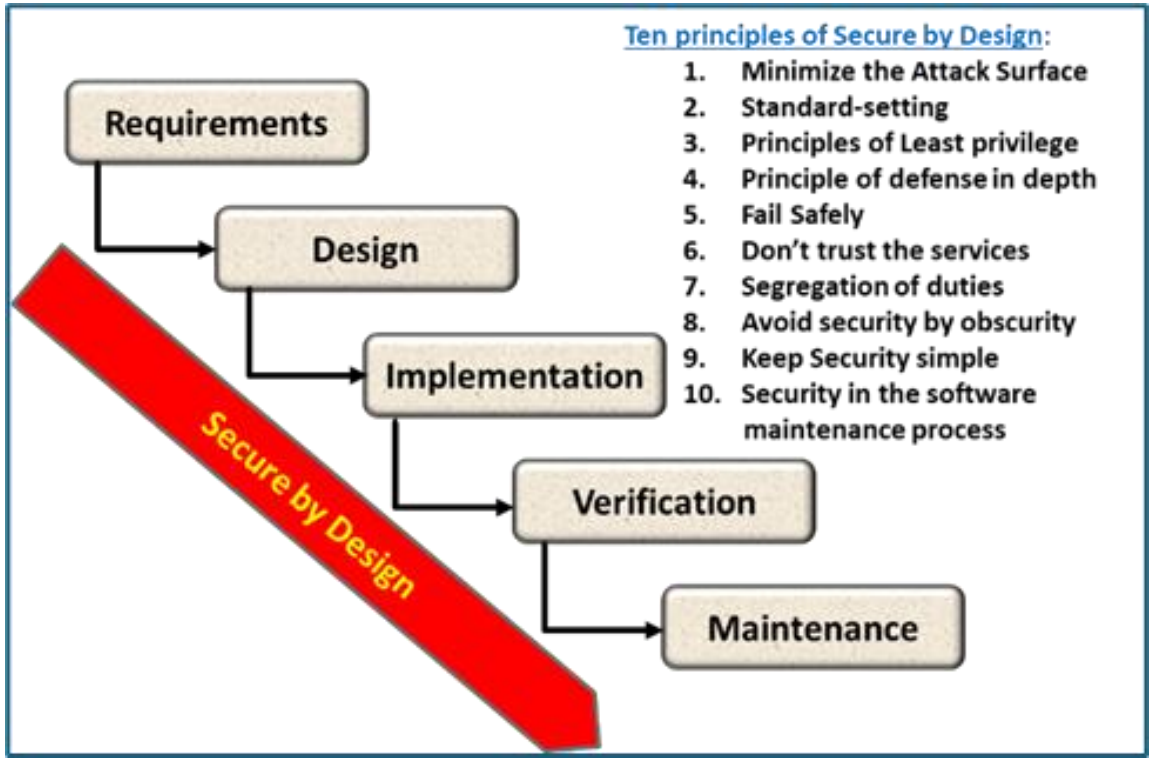
The Fix Rate associated with vulnerability repairs (Patch or New Release) should be equal to or higher than the rate of Vulnerability detection.



Fighting Cybercrime Costs with Secure by Design



The **cost of fighting cybercrimes** and technology threats is estimated at $9.5 Trillion and 9.04 % of Global GDP. Improving the vulnerability fix rate will greatly reduce costs and improve business service continuity and resilience.

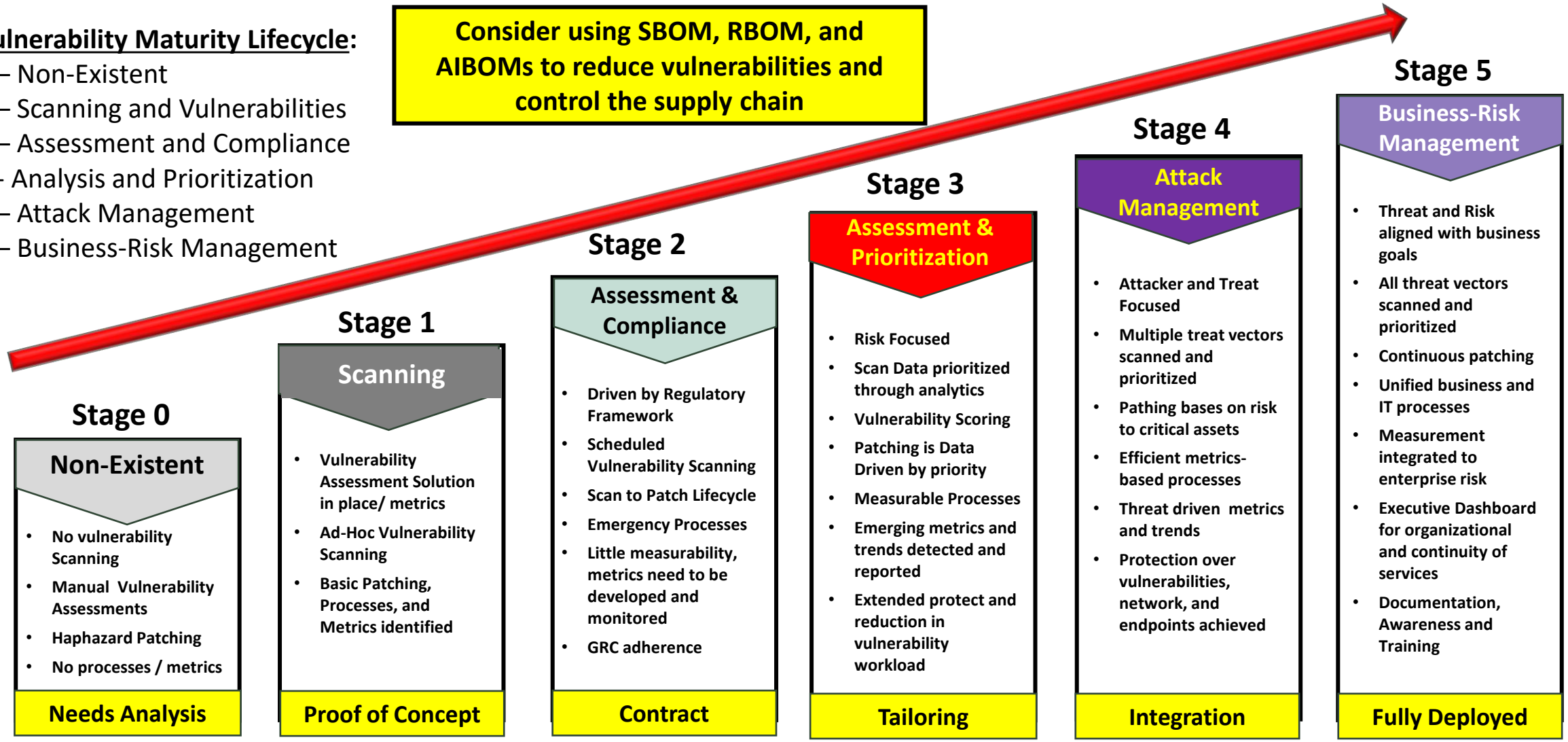


The government has developed a "**Whole of Nation**" approach to combat these costs through the "**Secure by Design**" methodology developed by DHS/CISA to safeguard Government, Business, Infrastructure, and Utilities from cybercrimes and technology threats.

Vulnerability Management Maturity Lifecycle

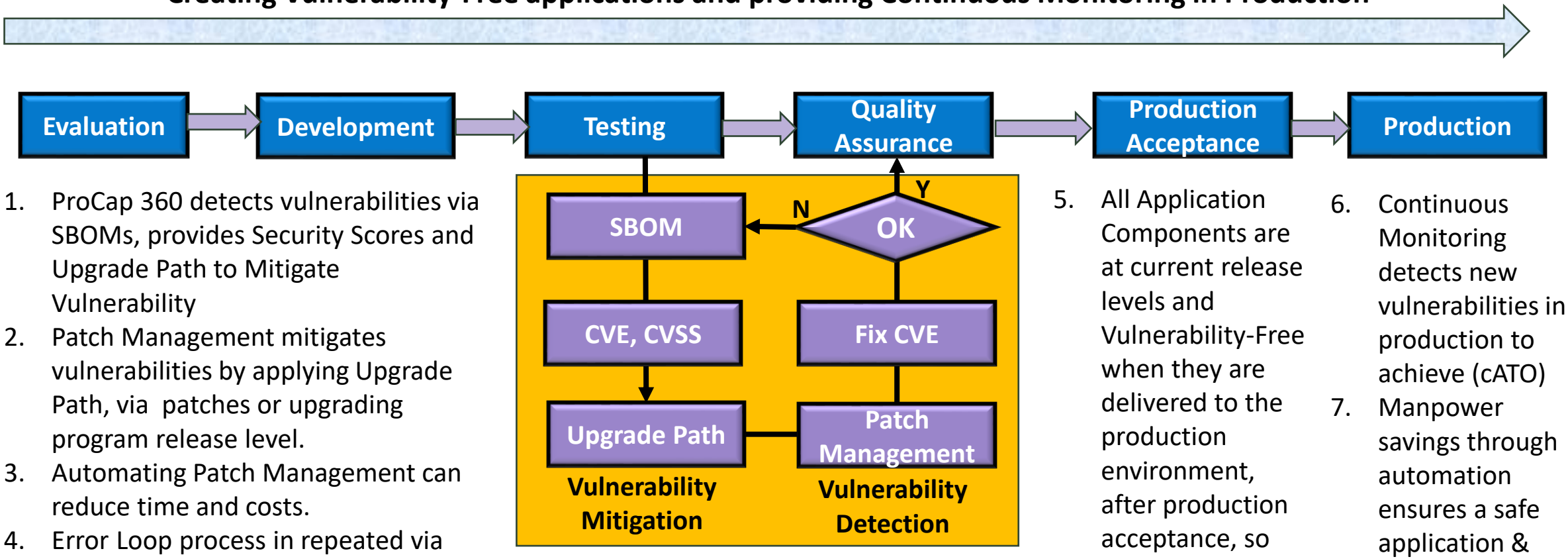
Vulnerability Maturity Lifecycle:
0 – Non-Existent
1 – Scanning and Vulnerabilities
2 – Assessment and Compliance
3 - Analysis and Prioritization
4 – Attack Management
5 – Business-Risk Management

Consider using SBOM, RBOM, and AIBOMs to reduce vulnerabilities and control the supply chain



Vulnerability Management using ProCap360™

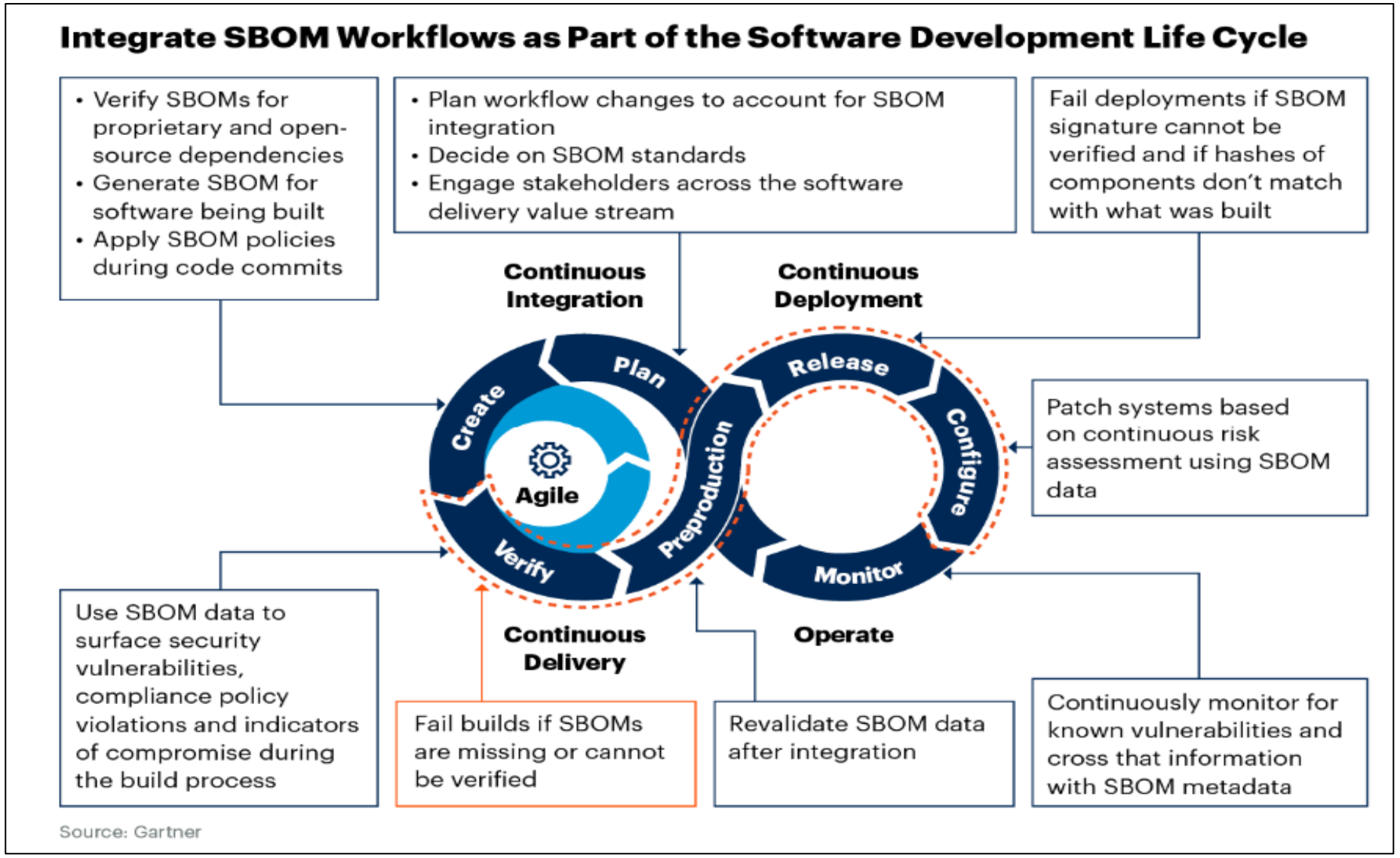
Creating Vulnerability-Free applications and providing Continuous Monitoring in Production



Vulnerability Management Detection and Mitigation

1. ProCap 360 detects vulnerabilities via SBOMs, provides Security Scores and Upgrade Path to Mitigate Vulnerability
2. Patch Management mitigates vulnerabilities by applying Upgrade Path, via patches or upgrading program release level.
3. Automating Patch Management can reduce time and costs.
4. Error Loop process in repeated via Quality Gates for every stage of product/service production.
5. All Application Components are at current release levels and Vulnerability-Free when they are delivered to the production environment, after production acceptance, so Assurance to Operate (ATO) is achieved.
6. Continuous Monitoring detects new vulnerabilities in production to achieve (cATO)
7. Manpower savings through automation ensures a safe application & service environment
8. Cost Savings and quick ROI

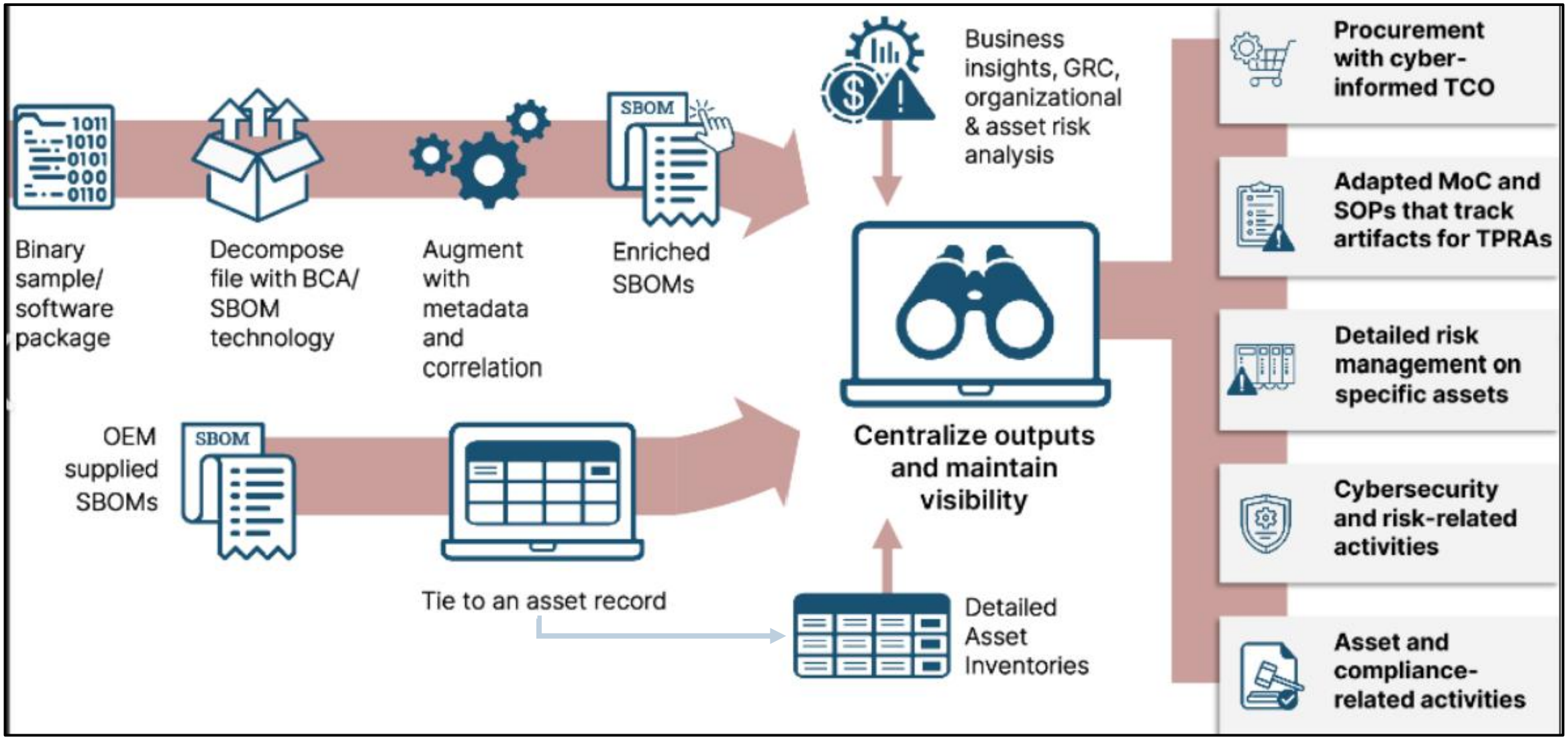
Gartner description of SBOMs in SDLC



Applications are comprised of many open-source modules so, if a Component in the application should change, then the SBOM should be run again to ensure the product is still vulnerability-free.

To repair vulnerabilities, apply a Patch or load the recommended new release of the product.

How SBOMs are created and their benefits



CWE – Common Weakness Enumeration

Shift Left Testing, or "Left of Boom" proactive problem management

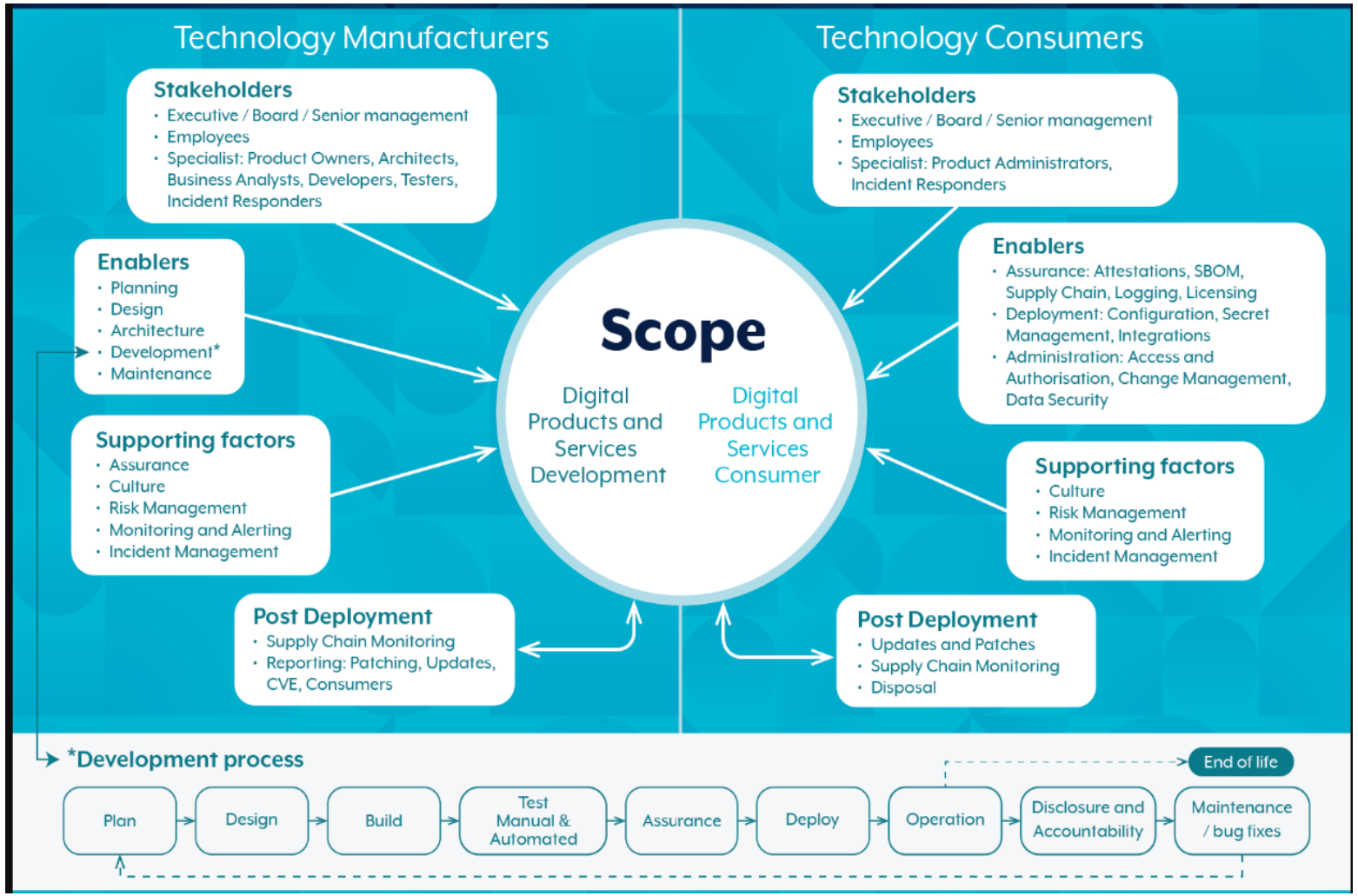
Common Weakness Enumeration (CWE™) is a community-developed list of common software and hardware weaknesses. A "weakness" is a condition in a software, firmware, hardware, or service component that, under certain circumstances, could contribute to the introduction of vulnerabilities. The CWE List and associated classification taxonomy identify and describe weaknesses in terms of CWEs.

Knowing the weaknesses that result in vulnerabilities means software developers, hardware designers, and security architects can eliminate them before deployment, which is considered a Left of Boom condition to proactively protect against business interruptions.

CWE List

The CWE List is updated three to four times per year to add new and update existing weakness information. Before being published on the CWE website, weaknesses are developed in the CWE Content Development Repository (CDR) on GitHub.com. The CDR provides visibility into the CWE working queue and a platform for CWE community partners to collaborate on content development.

Secure by Design – Process Overview



What is Secure by Design:

The Cyber Infrastructure Security Agency, CISA is charged with defending our nation against ever-evolving cyber threats and to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day. But, as we introduce more unsafe technology to our lives, this has become increasingly difficult.

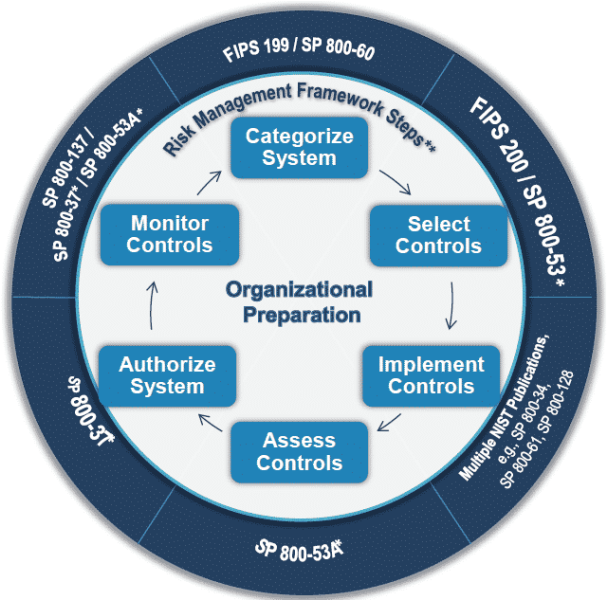
As a nation, we have allowed a system where the cybersecurity burden is placed disproportionately on the shoulders of consumers and small organizations and away from the producers of the technology and those developing the products that increasingly run our digital lives. Americans need a new model to address the gaps in cybersecurity—a model where consumers can trust the safety and integrity of the technology that they use every day.

Every technology provider must take ownership at the executive level to ensure their products are secure by design.

What it Means to Be Secure by Design

Products designed with Secure by Design principles prioritize the security of customers as a core business requirement, rather than merely treating it as a technical feature. During the design phase of a product's development lifecycle, companies should implement Secure by Design principles to significantly decrease the number of exploitable flaws before introducing them to the market for widespread use or consumption. Out-of-the-box, products should be secure with additional security features such as multi-factor authentication (MFA), logging, and single sign-on (SSO) available at no extra cost.

What is Risk Management and why is it important



Risk management is the systematic process of identifying, assessing, and mitigating threats or uncertainties that can affect your organization. It involves analyzing risks' likelihood and impact, developing strategies to minimize harm, and monitoring measures' effectiveness.

Related searches

1. foundations **of** risk management **pdf**
2. foundations **of quality** risk management
3. management **of** risk foundation **course**
4. **basics of** risk management **pdf**
5. management **of** risk foundation **exam**
6. **introduction to** risk management **pdf**
7. **sigma chi** risk management foundation
8. **harvard** risk management foundation

Risk Management includes:

1. Operational Risk
2. Asset Impairment Risk
3. Competitive Risk
4. Franchise Risk

Why is Risk Management Important:

1. Protects Organizational Reputation
2. Minimizes Losses
3. Encourages Innovation and Growth
4. Enhances Decision Making

Needs associated with Risk Management

- **Risk Assessment** must be completed to achieve compliance and reduce gaps and exposures.
- **Flaws and Risks** uncovered and repaired during assessment can lower potential damage to company and its reputation, lowering costs and improving company functionality.
- **Trained personnel** must be involved with a Risk Assessment, especially the leadership.
- **Scoring** should be decided upon before the assessment is commenced, both the scale and what its meaning is – just like a recovery group would relate to RTO and RPOs, the impact should be an indicator of the potential damage by an asset to the company reputation, revenue, and costs.
- **Reducing** a large list of risks to a manageable amount is a good practice. Summarize (aggregate) the results with drill downs to specifics. Reduce risks to assets, by category and/or user (i.e., Administrator's PC is more important that normal employee) and reduce threats analyzed.
- **Scoping** the Risk Assessment will include an Organizational Review, Asset Review, Competitive Risk, and Franchise Risk to maintain the Enterprise Reputation, Reduce Risk Exposures, and Save Costs.

Business Resilience Plan must contain

- Business Analysis and Needs
- Customer Services & Support (SLA)
- Organization and Functions
- Define Risk Appetite
- Review Assets and Environments
- Risk Assessment for Recovery Groups
- Business Continuity Management
- Technology Disaster Recovery
- Emergency Management
- Crisis Management
- Facility Recovery Management
- Supply Chain and Vendor Management
- Personnel Safety and Violence Prevention
- Business Impact Analysis (RTO, RPO)
- Recovery Strategy and Tool(s)
- Training and Awareness
- Recovery Planning, Testing and Exercising
- Emergency Communications
- Integration, Support & Maintenance

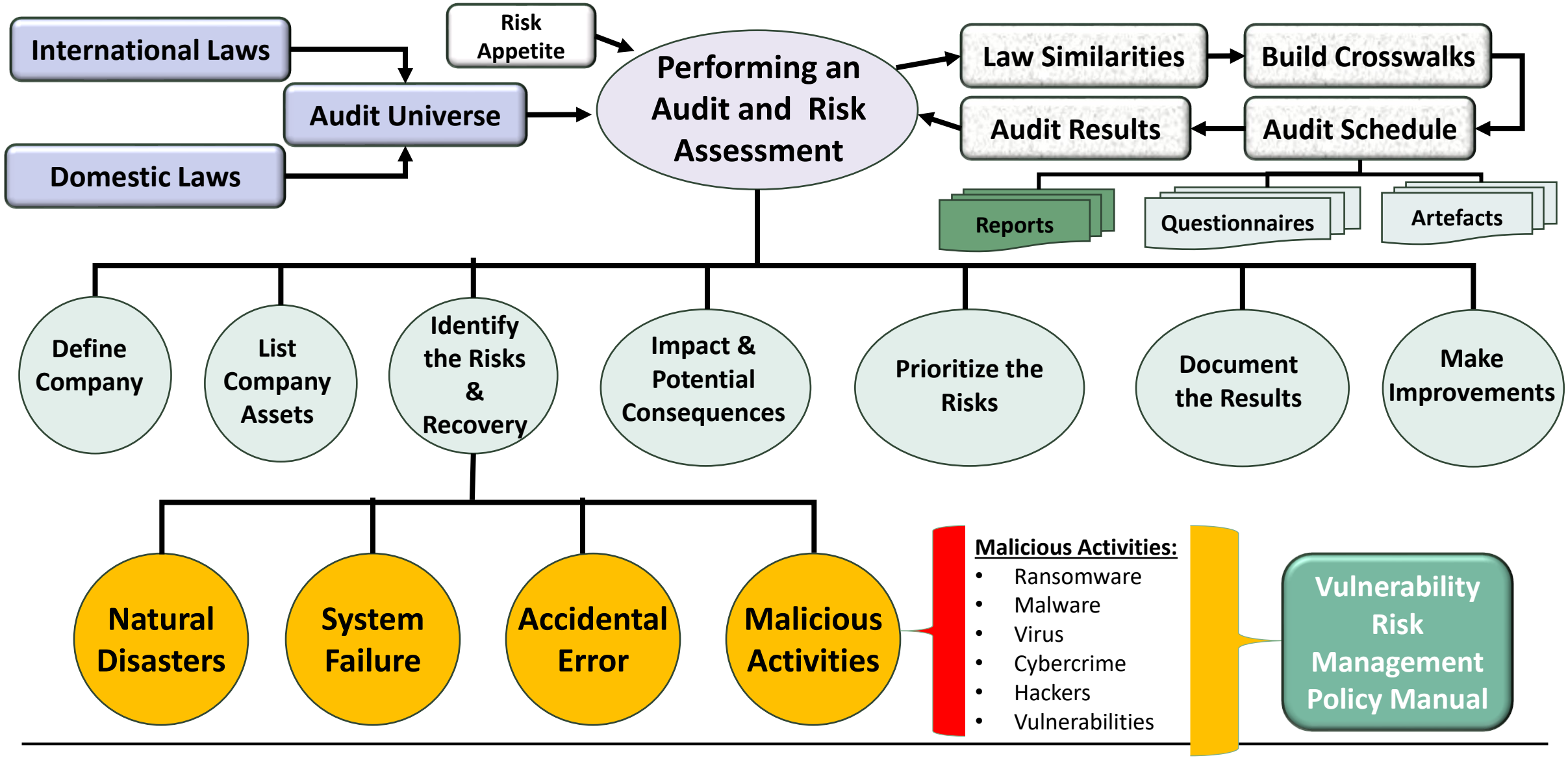
Risk Management phases and approach

Risk Management Phases:

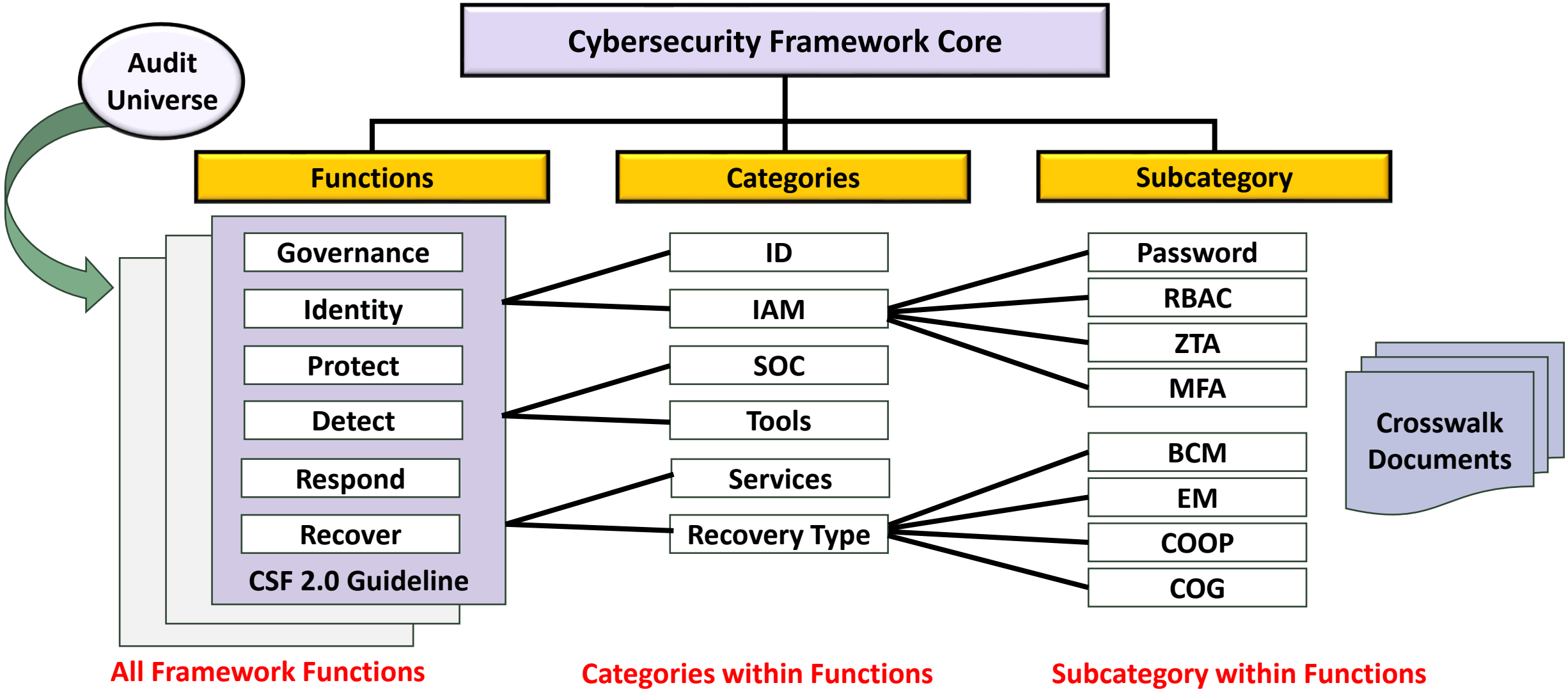
1. **Risk Identification**
2. **Risk Assessment**
3. **Risk Prioritization**
4. **Risk Reporting**
5. **Risk Monitoring**
6. **Risk Response & Mitigation**

Understanding Vulnerabilities, Malware, Insider Treats, IOT, Network, Phishing, and the Dark Web.

Performing an Audit and Risk Assessment

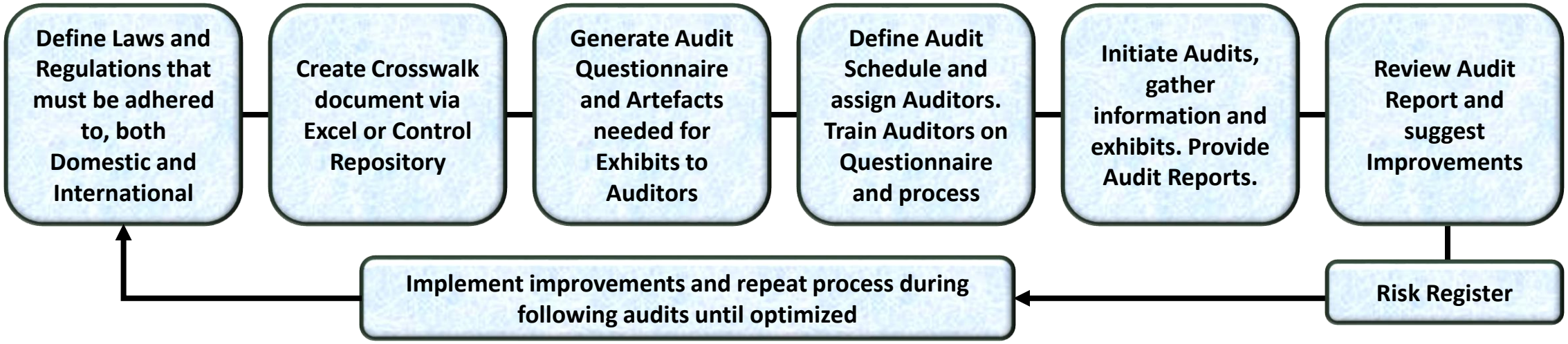


Creating a Crosswalk Audit Document

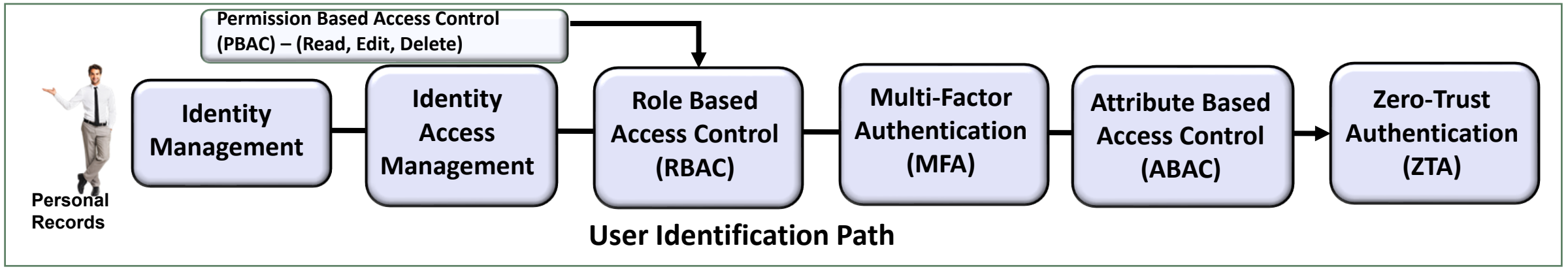


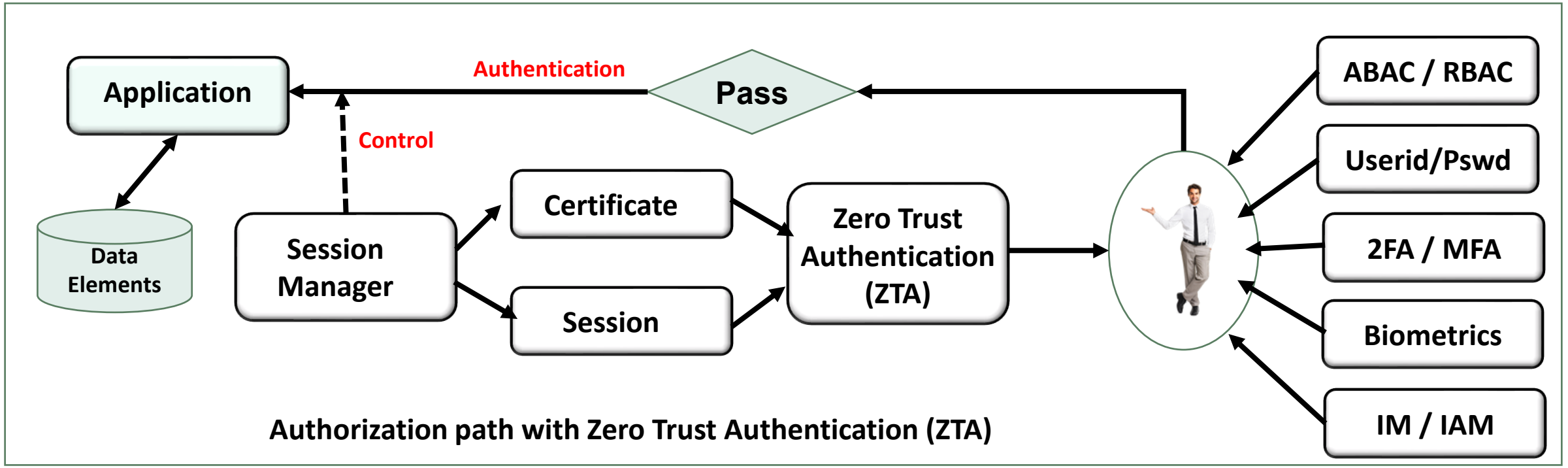
Defining your Audit Universe and Audit Process

Audit Universe						
Laws and Regulations:	**Function:**	**Category:**	**Subcategory:**	**Location:**	**Industry:**	**Size:**
List the Laws and Regulations your company must adhere to, like CSF 2.0, or ISO 27000, EO 14028, SEC Rule 2023 – 139, FFIEC, DORA, etc.	Define the Functions you must adhere to, like: Govern (GV), Identity (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC).	Define Categories like Organizational Context, Risk Management Strategy, etc.	Define the Subcategories associated with the category, like GV,OC and GV,RM.	Define if this law is Global (ISO) or Local (NIST).	Define any Industry Specific laws and regulations like FFIEC, DORA, EO 14028, etc.	Define the size of the organization that must comply with Law or Regulation

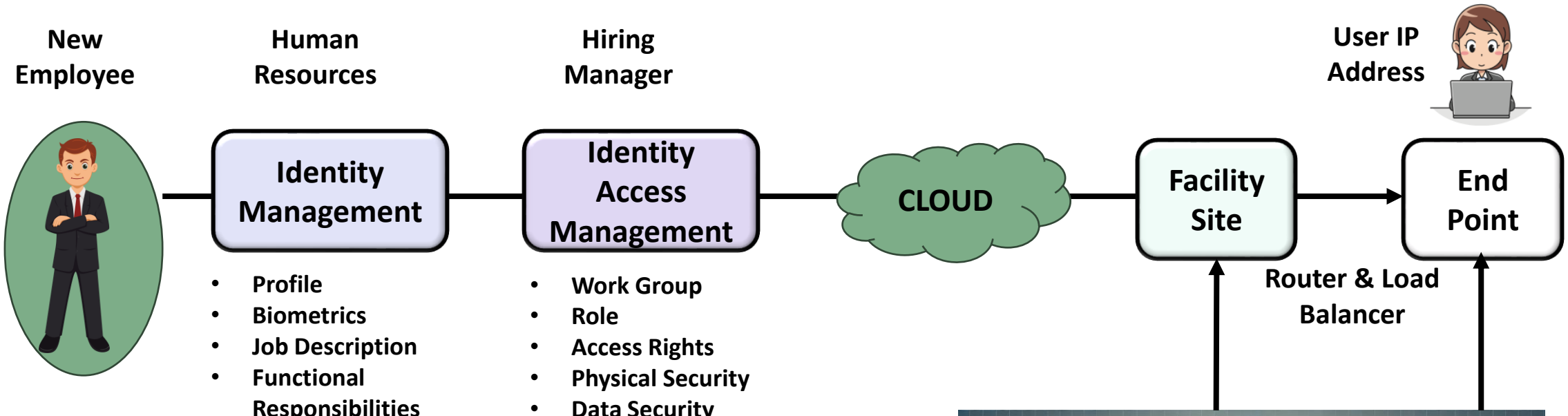


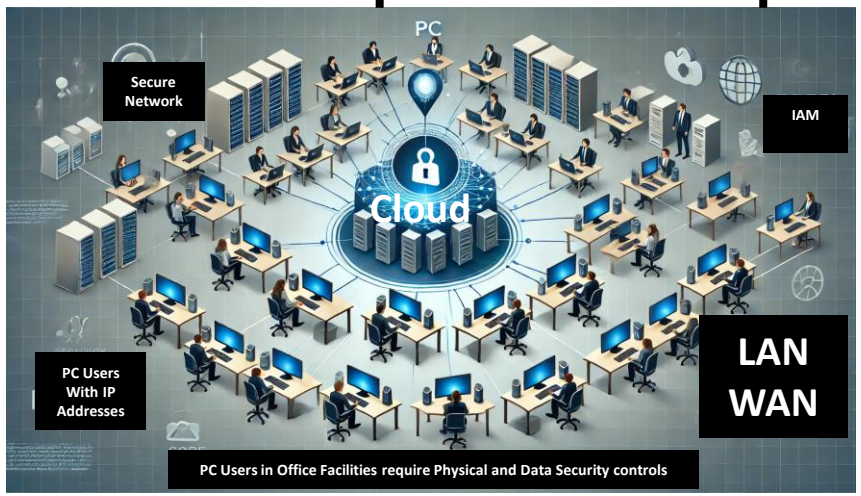
Identity and Access Management technologies





IAM Implementation

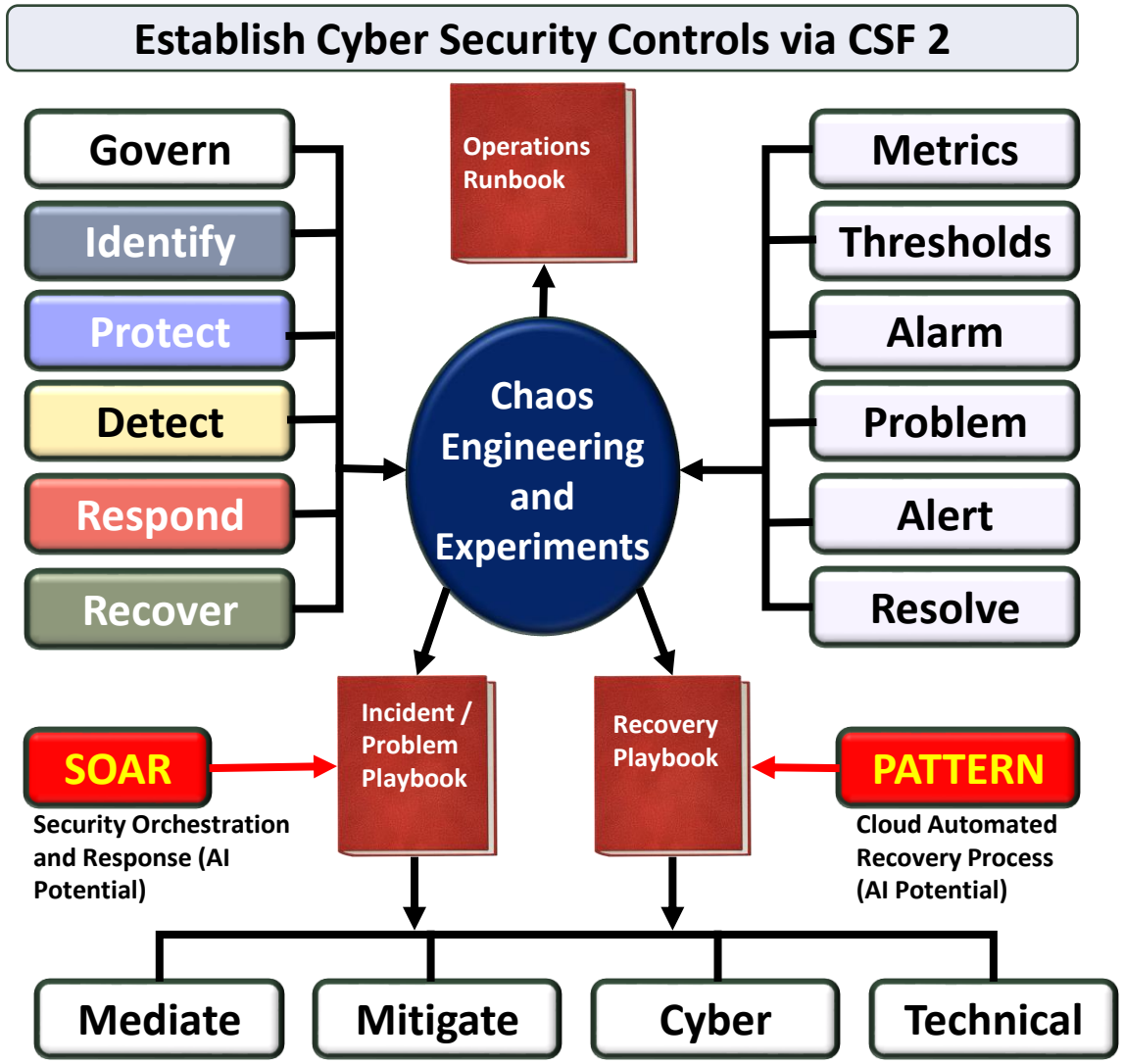




1. Personnel are Hired for open positions through the Human Resource Management (HR) Department, who performs Identity Management (IM).
2. Hiring Manager's onboard employee through Identity Access Management (IAM).
3. Personnel security is based on the Role they must perform under Role Based Access Control (RBAC) comprised of Work Group (i.e., Department) and Role (i.e., Functional Responsibilities).
4. Higher level of security can be provided through Two Factor Authentication (2FA), Multi-Factor Authentication (MFA), Attribute Based Access Control (ABAC for physical devices), and Zero Trust Authentication (ZTA).

NIST CSF 2.0 Categories and Application

NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	**CSF 2.0 Category**	**CSF 2.0 Category Identifier**
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identity (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



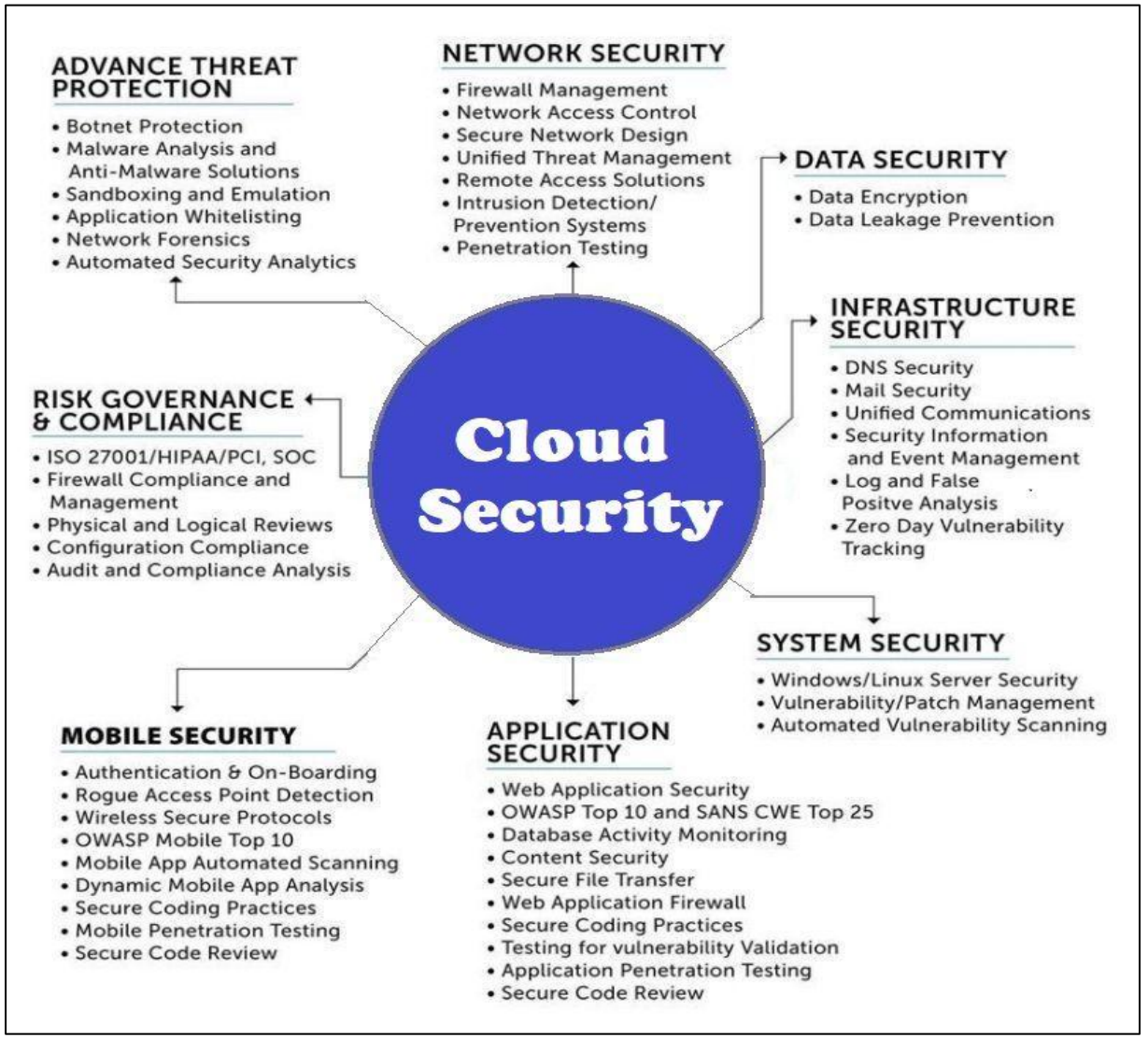
Cloud Security Disciplines

Advanced Threat Protection:
- Botnet Protection
- Malware Analysis and Anti-Malware Solutions
- Sandboxing and Emulation
- Application Whitelisting
- Network Forensics
- Automated Security Analytics

Risk Governance & Compliance:
- ISO 27001/HIPAA/PCI. SOC
- Firewall Compliance & Management
- Physical & Logical Reviews
- Configuration Compliance
- Audit and Compliance Analysis

Mobile Security:
- Authenticating & On-Boarding
- Rogue Access Point Detection
- Wireless Security Protocols
- OWASP Mobile Top Ten
- Mobile App Automated Scanning
- Dynamic Mobile App Analysis
- Secure Coding Practices
- Mobile Penetration Testing
- Secure Code Review

Data Security:
- Data Encryption
- Data Leakage Prevention



Network Security:
- Firewall Management
- Network Access Control
- Secure Network Design
- Unified Threat Management
- Remote Access Solutions
- Intrusion Detection
- Prevention Systems
- Penetration Testing

Infrastructure Security:
- DNS Security
- Mail Security
- Unified Communications
- Security Information and Event Management
- Logs and False Positive Analysis
- Zero Day Vulnerability Management

System Security:
- Windows/Linux Server Security
- Vulnerability/Patch Management
- Automated Vulnerability Scanning

Application Security:
- WEB Application Security
- OWASP Top 10 and SANS CWE Top 25
- Database Activity Monitoring
- Content Security
- Secure File Transfer
- Secure SDLC practices
- DevSecOps implementation

Know and Control your Environment

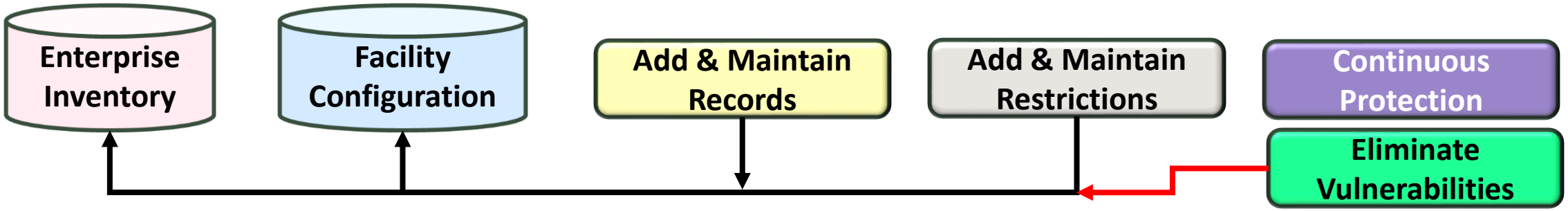
- **HW**AM
- **SW**AM
- **Technology** Management
- **Release** Management
- **Patch** Management
- **End-of-life**

- Facilities, or Locations
- Configuration of equipment
- Services and Applications
- COOP Recovery
- Location Recovery

- **Acquisition** - Order through Delivery
- **Install** and Test
- **Turnover** to User
- **Redeploy** as needed
- **Terminate** within laws and regulations

- **Components** via SBOM RBOM, or AIBOM
- **Identify Countries** parts origin
- Adhere to Laws and **country restrictions**
- Identify Vulnerabilities
- License Management

- **Identify** Vulnerabilities prior to production
- **Apply** Patches and Update Releases
- **Validate** mitigations
- **Vulnerability-free** production
- **CTEM** after Production



Laws and Regulations, by groups

Risk Posture and Audit Preparedness

- Risk Analysis
- Define Domestic and International needs
- Likelihood
- Impact
- Defense Strategies
- Controls
- Insurance
- Audit Universe
- Crosswalks
- Audit Questionnaire and Artefacts
- Audit Schedule
- Reporting & Monitoring
- Improvement & Automation

Domestic Compliance

- **COSO** – Risk Appetite
- **COBIT** – IT Governance Framework
- **RMF** – Risk Management Framework
- **CSF 2.0** – Cybersecurity Framework
- **CIA** – Confidentiality, Integrity, and Availability
- **GRC** – Governance, Risk, and Compliance
- **NIST** – National Institute of Standards and Technology
- **EO** – Executive Orders

International Compliance

- ISO - International Organization for Standardization:
- **ISO 3001 –** Risk Management
- **ISO 9000** – Quality Management
- **ISO 22301** – Business Continuity Management
- **ISO 14000** – IT Environment
- **ISO 20000** – IT Services
- **ISO 27000** – Information Security
- DORA, GDPR. NIS 2,

Industry Compliance

- **PCI DSS** – Payment Card Industry Data Security Standards
- **FDA** – Food & Drug Agency
- **OMB** – Office of Management and Budget
- **SEC** – Securities Exchange Commission
- **FFIEC** – Federal Financial Institutions Examination Council
- "**Whole of World**"
- "**Whole of Nation**"
- "**Secure by Design**"

Existing laws and regulations

- **Gramm Leach Bliley** – Safeguard Act (was Bank Holding Act);
- **HIPAA** – Healthcare regulations (including ePHI, HITECH, and Final Ombudsman Rule);
- **Sarbanes – Oxley Act** (sections 302, 404, and 409) on financial assessment and reporting by authorized "Signing Officer";
- **EPA and Superfund** (how it applies to Dumping and Asset Management Disposal);
- **Supply Chain Management "**Laws and Guidelines" included in ***ISO 24762*** (SSAE 16 for Domestic compliance and SSAE 3402 for International Compliance, and NIST 800-34);
- **Supply Chain Management "**Technical Guidelines" described in ***ISO 27031***;
- **Patriots Act** (Know Your Customer, Money Laundering, etc.);
- **Workplace Safety and Violence Prevention** via OSHA, OEM, DHS, and governmental regulations (State Workplace Guidelines and Building Requirements);
- **Income Tax and Financial Information protection** via ***Office of the Comptroller of the Currency*** (OCC) regulations (***Foreign Corrupt Practices Act***, **OCC-177** Contingency Recovery Plan, **OCC-187** Identifying Financial Records, **OCC-229** Access Controls, and **OCC-226** End User Computing).

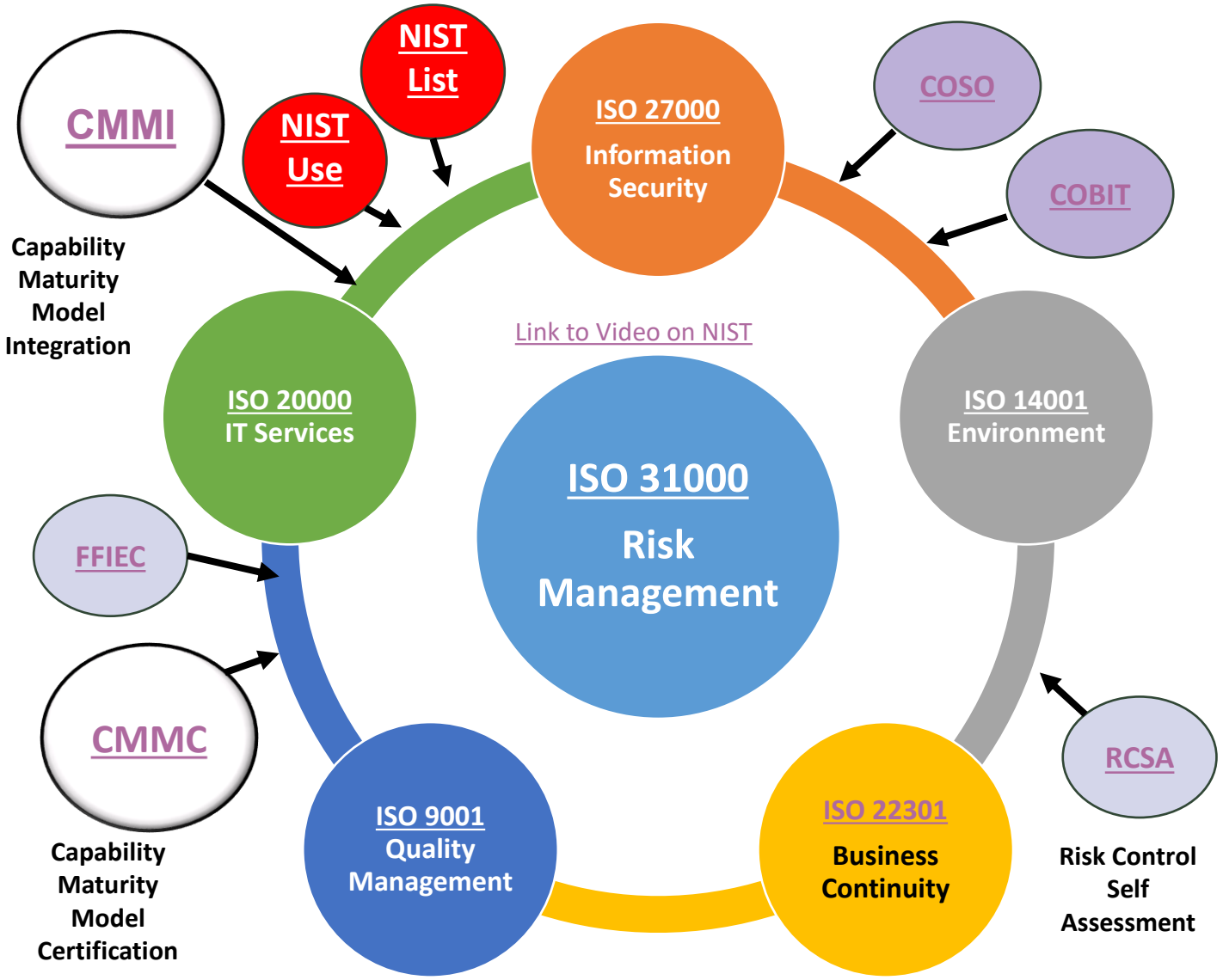
These laws and regulations have been around for many years (Starting with OCC regulations and growing from there) and have served as the basis for Governance Regulations and Compliance (GRC). Additional industry compliance requirements like SEC, FFIEC and HITECH must be adhered to as well.

The CIA (Confidentiality, Integrity, Availability) deals with security and should be adhered to with the same aggressiveness as GRC.

Vulnerability Laws and Regulations requiring SBOMs

- Presently, implementing Applications and Services can include vulnerabilities and malware, which can cost your company in lost revenue, brand reputation, fines and penalties, burdening your staff and resulting in high levels of turnover. DHS/CISA has developed a "Secure by Design" approach to responding to these issues.
- A method must be implemented to catch vulnerabilities and malware prior to production acceptance.
- New Laws have been mandated in the United States and Europe to address the problems, including:
  - **Executive Order 14028** – Improving Nation's Software Security Supply Chain and mandating SBOMs
  - **OMB M-22-18** and M-23-16 – Improving the Defense and Resilience of Government Networks
  - **SEC Rule 2023-139** – Disclosure of Material Cybersecurity breaches to protect shareholders
  - **FDA** – Control over medical device supply chain and cybersecurity problems (**ISO 14971:2019** Risk Management for Medical Devices)
  - **CRA** – European Cyber Resilience Act – Hardware and Software Components cyber requirements
  - **DORA** – Digital Operational Resilience Act – Strengthen the financial sectors resilience
  - **GDPR** – EU Digital Rights of their Citizens
  - **Deploying AI Security Systems** - joint paper from CISA, NSA, and DOJ on employing AI Security
- Once the development process is upgraded and new Standards and Procedures created, an Awareness Program must be developed and the Staff Trained.
- New Procedures must be integrated into the staff's daily process for new and changed applications and services, with automated support through RPAs whenever feasible.

Laws and Regulations with Links



Developing a business optimization approach that combines these ISO Standards (**International**) and NIST Standards (**Domestic**) will achieve certification more quickly.

Implementing the standards separately will result in overlaps and inefficiencies.

Start with **Risk Management** (31000) and ensure that **Information Security** (ISO 27000) is current and best suited to protect your **Data** and **Environmental facilities** (ISO 14001).

Then implement your **Business Continuity** (ISO 22301) Recovery Certification Process for Emergency, Crisis, Business, and IT Disaster Recovery Management.

Integrate Quality Management (ISO 9001) within your processes to ensure the products and services your company delivers will be of the highest quality and capable of protecting your brand and reputation.

Finally ensure your **IT Services** (ISO 20000) are of the highest quality possible and that all ISO standards are adhered to in compliance with existing laws and regulations, so that you never have to fear failing an audited.

Performing and Optimizing Risk Management

- Conduct a Risk Assessment to locate gaps, exceptions, and weaknesses,
- Identify Assets and their importance,
- Ensure adherence to laws and regulations and provide business service continuity.

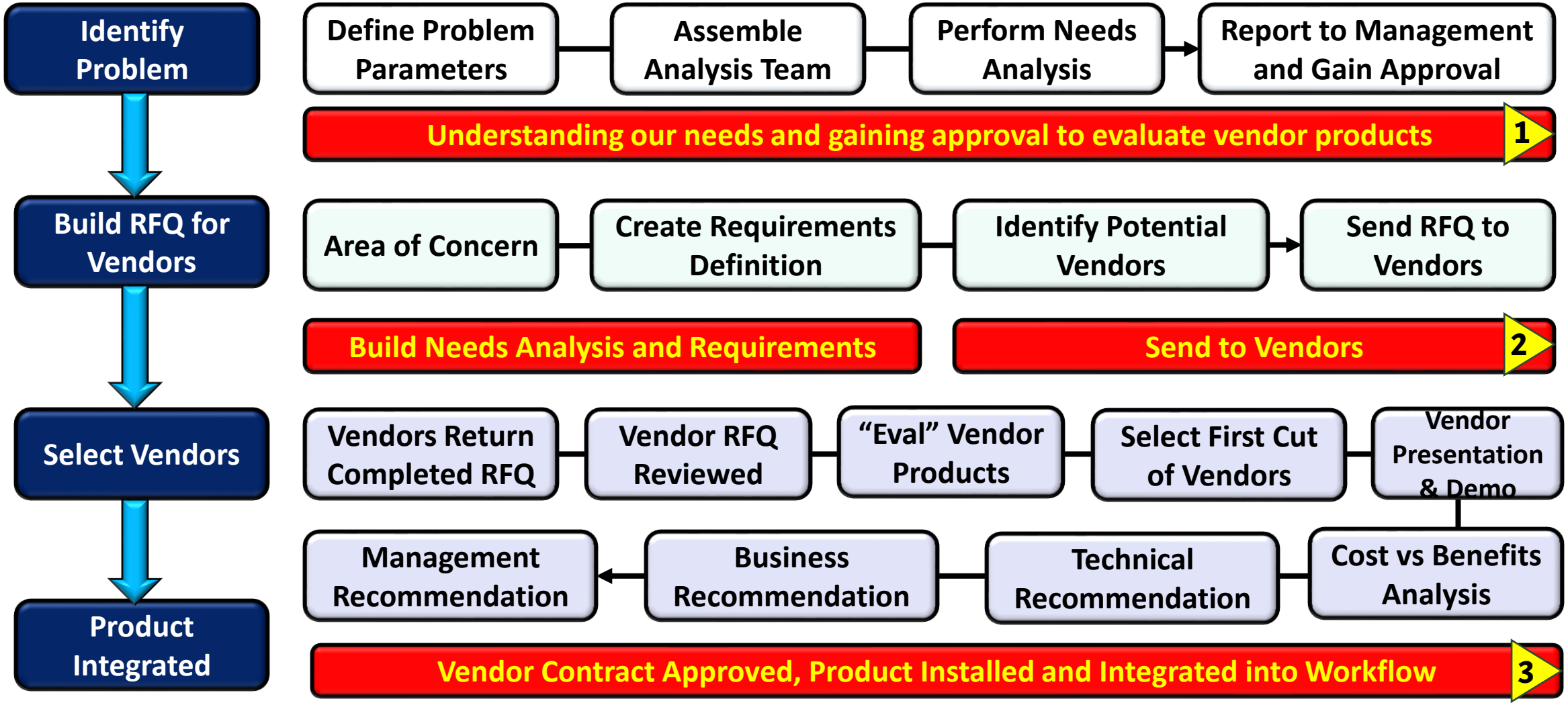
- Identify Gaps, Exceptions, and Weaknesses.
- Rate the Impact and Likelihood.
- Develop Controls and other resolutions.
- Enter into Risk Register.
- Create POA&M to mitigate / mediate risk.
- Validate correction.

- Define Requirements and effort associated with Risk Assessments to ensure compliance to laws and regulations, both domestically and internationally.
- Determine Costs and Efforts.
- Perform an Analysis of Alternatives.
- Select & Implement strategies best suited to enterprise.

- Develop Risk Monitoring Dashboard system.
- Ensure integration with,
- Crosswalks,
- Risk Assessment Audit Guidelines,
- Worksheets,
- Questionnaires,
- Risk Reports,

- Reviews to identify improvements,
- Improve and repeat until optimized.
- Automate process if desired,
- Conduct Cost vs Benefit Analysis to determine best direction.
- Develop POA&M
- Assign Teams and Management

Performing an Analysis of Alternatives (AoA)



Risk Evaluation and Control

- **Identify** the risks/threats and vulnerabilities to the entity and its resources, or impact the entity's image
- **Assess** risk/threat likelihood that they would occur
- **State** the potential impacts
- **Determine** where controls, mitigations or management processes are non-existent, weak or ineffective
- **Locate** obstacles to the ability to achieve recovery
- **Recommend** additional controls, mitigations, obstacle eliminations (e.g., special equipment, capacity, performance) or process improvements

Defining your Enterprise and Workflow

Business Analysis

- Industry
- Functions
- Vendors
- Supply Chain
- Vulnerabilities
- Threats
- Regulations
- Audit Universe
- Resilience
- Continuity
- Compliance
  - Domestic
  - International
- Whole of Nation and Secure by Design protection

C Level Functions

- Board of Directors
- CIO / CTO
- CISO
- COO
- CFO
- CMO
- Auditing
- Legal
- Outside Collaborators
- Supporting Vendors
- Regulators
- Political Advisors

Product Creation & Support

- Concept,
- Engineering,
- Development,
- Data Protection,
- Testing,
- Service Continuity,
- User Acceptance,
- Vulnerability-Free,
- Secure by Design
- Support & Maintain
- Change Management
- Documentation
- Awareness
- Training

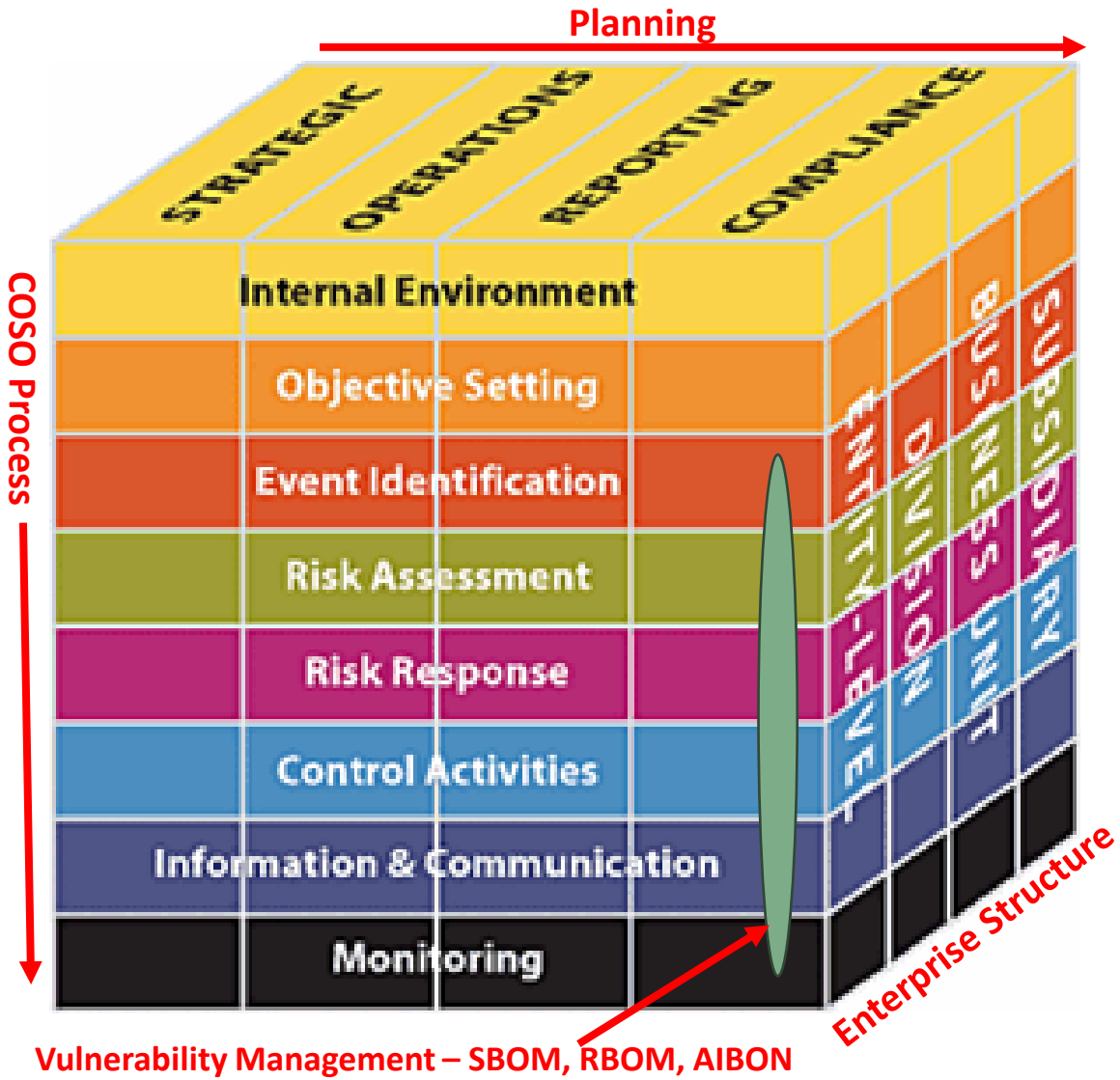
Safeguarding the Enterprise

- **IM** - Identity Management
- **IAC** - Identity Access Management
- **RMM** - Risk Maturity Management
- **CMMI** - Capability Maturity Model Integration
- **CSF 2.0** - Cybersecurity Framework 2.0
- **VMM** – Vulnerability Maturity Model
- **Chaos** Testing
- **Supply Chain** Management
- **UAT** - User Acceptance Testing

Production Operation

- Game Day Testing
- Production Acceptance
- Production Cutover
- Data Management
- Vital Records Management
- Data Backup, Recovery, and Vaulting
- Communications
- Hardening and Physical Safeguards
- ATO – Authorization to Operate
- Production Support, Maintenance, and Change / Release Management

COSO and Enterprise Risk Management



COSO - Committee of Sponsoring Organizations

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

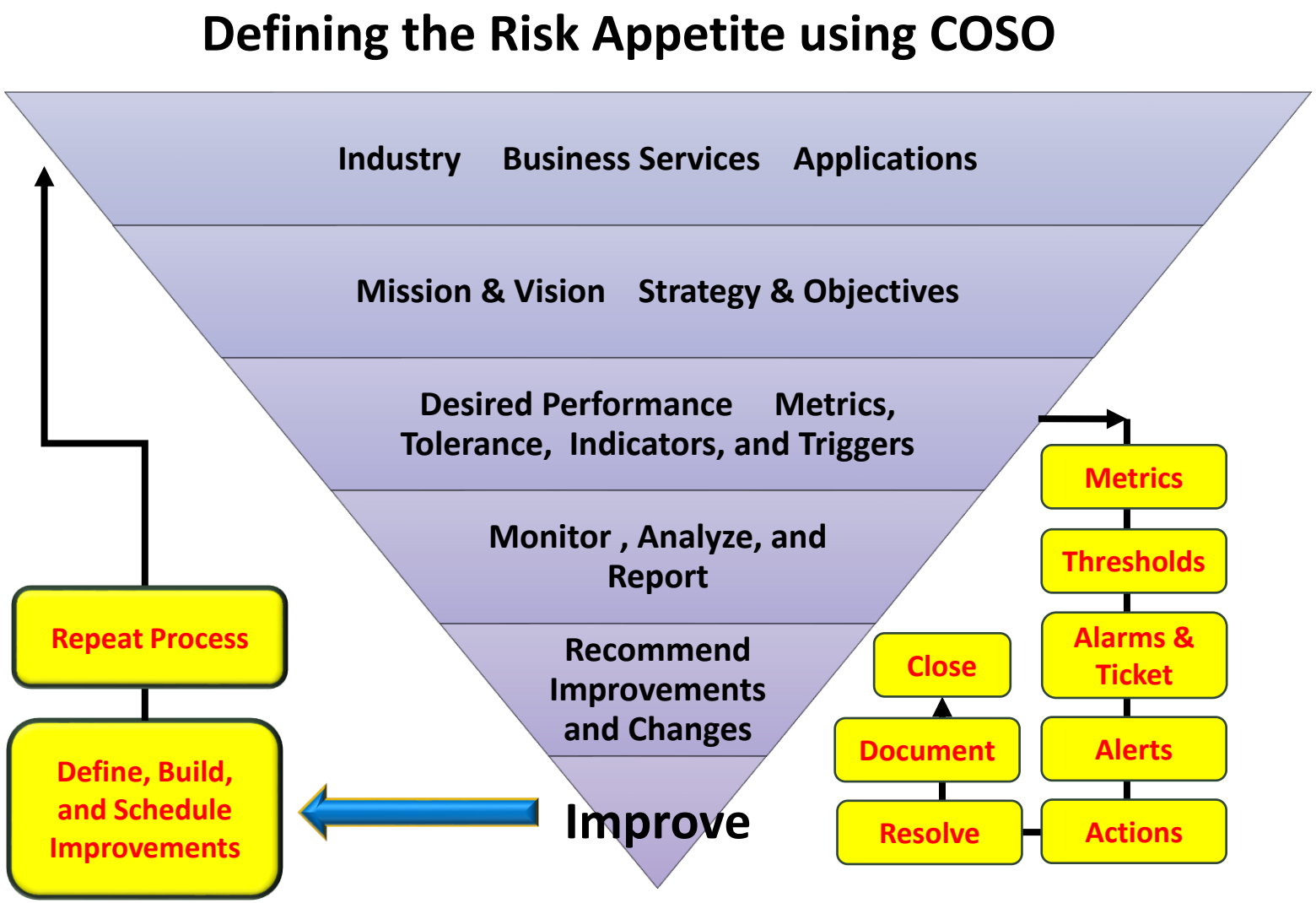
Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Vulnerability Management

21. Install SBOM, RBOM, and AIBOM
22. Apply Patch Fix or New Release update
23. Monitor New Release & CTEM Production Vulnerability-free

The Risk Evaluation Process Using COSO



COSO for Risk Appetite & Evaluation:

1. Review Business Mission and Vision
2. Considers Board and Management perspectives and appetites
3. Incorporates current strategic direction, risk profile, and culture.
4. Identifies and evaluates alternate strategies.
5. Chooses preferred strategy to enhance value.
6. Establishes Business Objectives.
7. Sets tolerance, measures metrics, indicators, and triggers.
8. Changing context of the business culture and competitive environment.
9. Monitors performance and revises appetite or strategy, as needed.

COBIT 5 – Process for Governance of Enterprise IT

Align, Plan, and Organize (APO)
- APO01 – Manage the IT Management Framework
- APO02 – Manage Strategy
- APO03 – Manage Enterprise Architecture
- APO04 – Manage Innovation
- APO05 – Manage Portfolio
- APO06 – Manage Budget and Costs
- APO07 – Manage Human Resources
- APO08 – Manage Relationships
- APO09 – Manage Service Agreements
- APO10 – Manage Suppliers
- APO11 - Manage Quality
- APO12 – Manage Risk
- APO13 – Manage Security

Build, Acquire and Implement (BAI)
- BAI01 – Manage Programs and Projects
- BAI02 – Manage Requirements Definition
- BAI03 – Manage Solutions Identifications and Build
- BAI04 – Manage Availability and Capacity
- BAI05 – Manage Operational Change Environment
- BAI06 – Manage Changes
- BAI07 – Manage Change Acceptance and Transitioning
- BAI08 – Manage Knowledge
- BAI09 – Manage Alerts
- BAI10 – Manage Configuration

Deliver, Service and Support (DSS)
- DSS01 – Manage Operations
- DSS02 – Manage Service Requests and Incidents
- DSS03 – Manage Problems
- DSS04 – Manage Continuity
- DSS05 – Manage Security Services
- DSS06 – Manage Business Process Controls

Evaluate, Direct and Monitor (EDM)

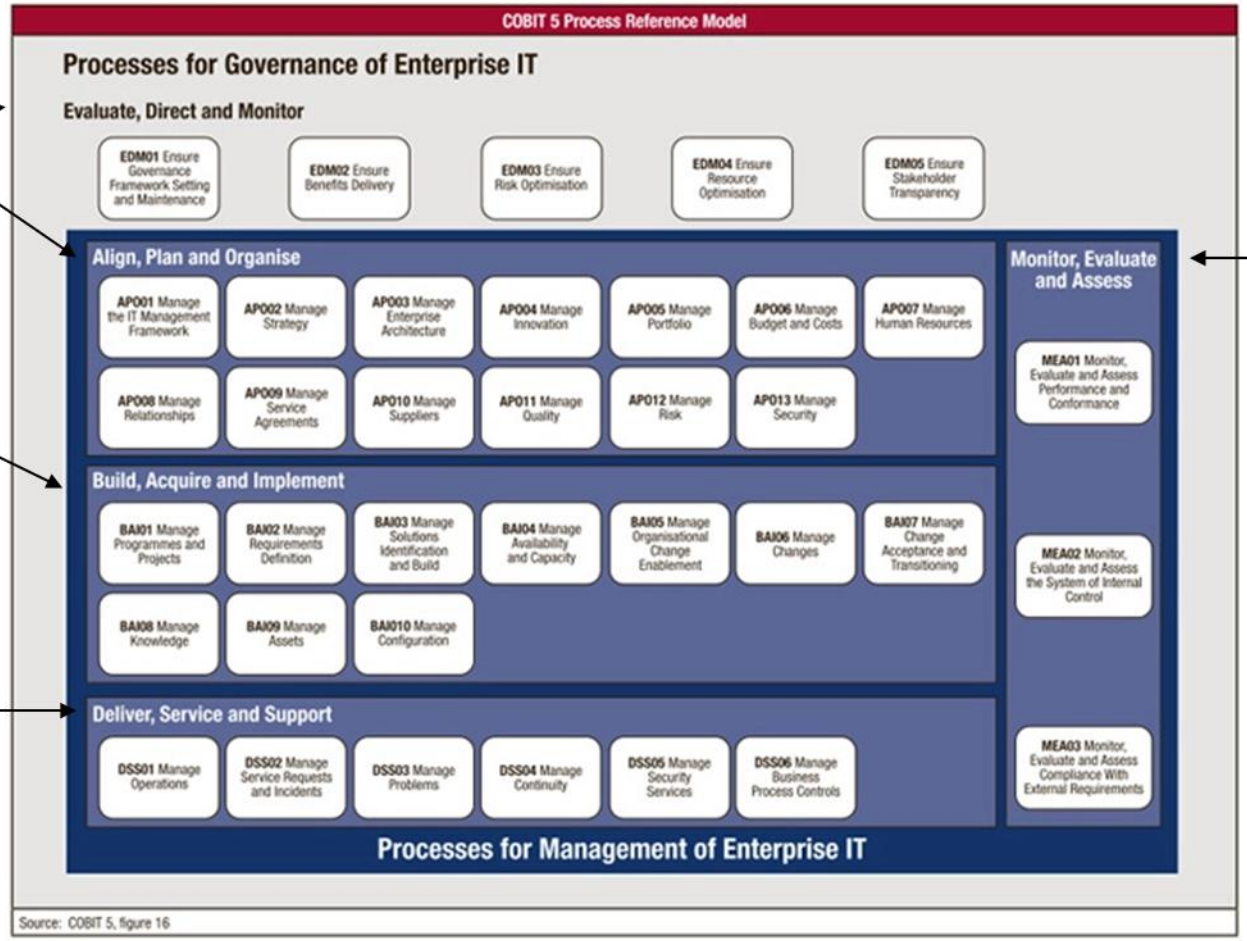
EDM01 – Ensure Governance Framework Setting and Maintenance

EDM02 – Ensure Benefits Delivery

EDM03 – Ensure Risk Optimization

EDM04 – Ensure Resource Optimization

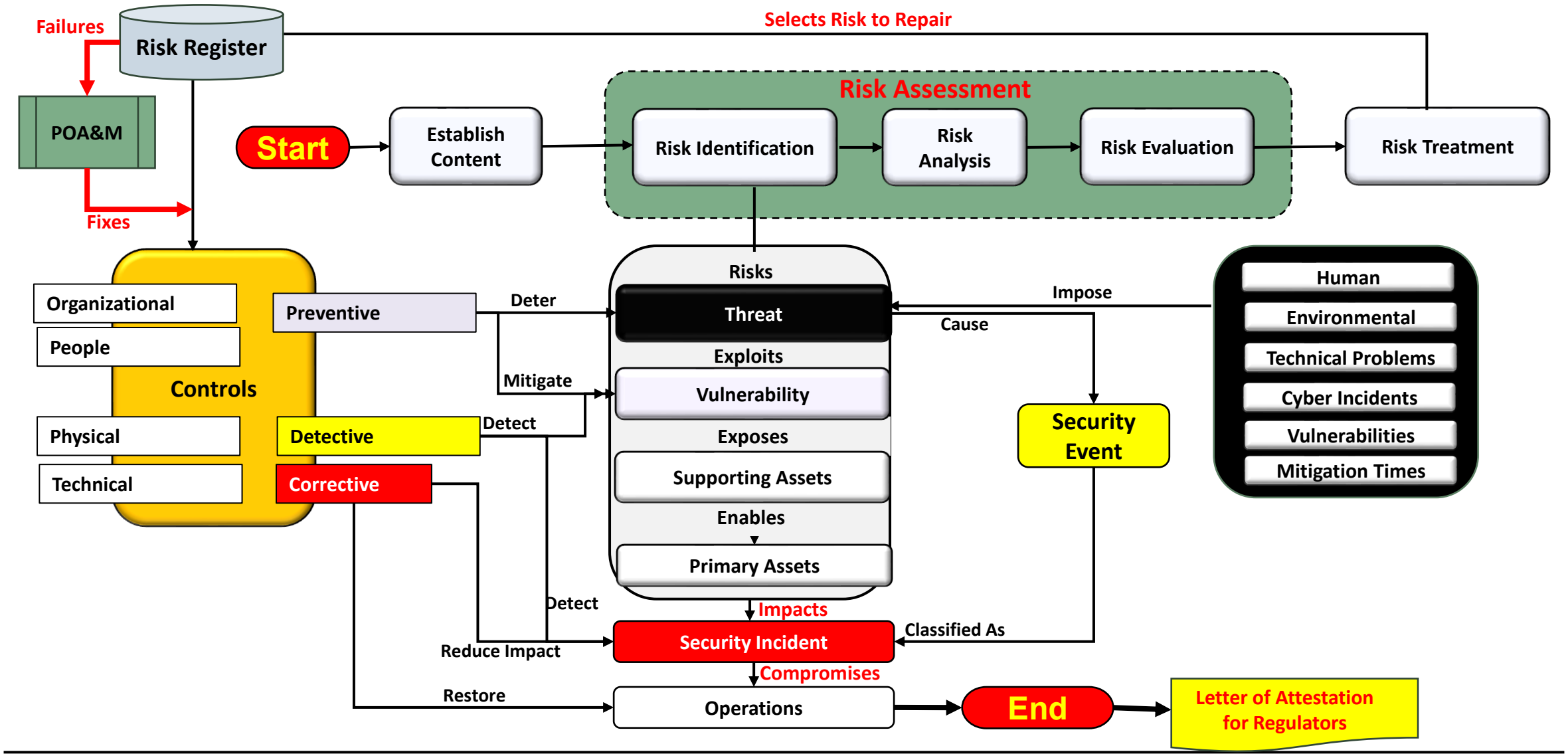
EDM05 – Ensure Stakeholder Transparency



[Get COBIT 5 Toolkit from ISACA]

Monitor, Evaluate and Assess (MEA)
- MEA01 – Monitor, Evaluate and Assess Performance and Conformance
- MEA02 – Monitor, Evaluate and Assess the System of Informal Control
- MEA03 – Monitor, Evaluate and Assess Compliance with External Requirements

Risk Management with ISO 27000: 2022



CMMI – Capability Maturity Model Integration

Overview

CMMI models are an important part of CMMI Solutions for improving your organization's performance and its ability to meet its business objectives. Three CMMI models exist: CMMI for Development (CMMI-DEV), CMMI for Services (CMMI-SVC), and CMMI for Acquisition (CMMI-ACQ), and share 16 core process areas in common. These process areas include practices that cover concepts in project management, process management, infrastructure, and support.

These basic concepts are fundamental to process improvement in any area of interest (i.e., acquisition, development, services). The core process areas of each model express these concepts in the context of that area of interest. In addition to the core process areas, each model also includes process areas found only in that model.

Developed at Carnegie Mellon University and Supported through CMMI Institute, an offshoot of CMU.

Process Areas

Process areas found only in CMMI for Acquisition
- Acquisition Requirements Development (ARD)
- Solicitation and Supplier Agreement Development (SSAD)
- Agreement Management (AM)
- Acquisition Technical Management (ATM)
- Acquisition Verification (AVER)
- Acquisition Validation (AVAL)

Process found only in CMMI for Development
- Product Integration (PI)
- Requirements Development (RD)
- Supplier Agreement Management (SAM)*****
- Technical Solution (TS)
- Validation (VAL)
- Verification (VER)

Process areas found only in CMMI for Services
- Capacity and Availability Management (CAM)
- Incident Resolution and Prevention (IRP)
- Supplier Agreement Management (SAM)*****
- Service Continuity (SCON)
- Service Delivery (SD)
- Service System Development (SSD)
- Service System Transition (SST)
- Strategic Service Management (STSM)

Core Processes

CMMI Model Foundation (16 Core Process Areas)

- Causal Analysis and Resolution (CAR)
- Configuration Management (CM)
- Decision Analysis and Resolution (DAR)
- Integrated Project Management (IPM)*
- Measurement and Analysis (MA)
- Organizational Process Definition (OPD)
- Organizational Process Focus (OPF)
- Organizational Performance Management (OPM)
- Organizational Process Performance (OPP)
- Organizational Training (OT)
- Project Monitoring and Control (PMC)**
- Project Planning (PP)***
- Process and Product Quality Assurance (PPQA)
- Quantitative Project Management (QPM)****
- Requirements Management (REQM)
- Risk Management (RSKM)

* Integrated Work Management (IWM) in CMMI-SVC
** Work Monitoring and Control (WMC) in CMMI-SVC
*** Work Planning (WP) in CMMI-SVC
**** Quantitative Work Management (QWM) in CMMI-SVC
***** Supplier Agreement Management (SAM) is shared between CMMI-DEV and CMMI-SVC

CMMI Model Core Processes and Rating Example

Capability Maturity Model Integration (CMMI) Core Process Areas

Abbreviation	Name	Area	Maturity Level
CAR	Causal Analysis and Resolution	Support	5
CM	Configuration Management	Support	2
DAR	Decision Analysis and Resolution	Support	3
IPM	Integrated Project Management	Project Management	3
MA	Measurement and Analysis	Support	2
OPD	Organizational Process Definition	Process Management	3
OPF	Organizational Process Focus	Process Management	3
OPM	Organizational Performance Management	Process Management	5
OPP	Organizational Process Performance	Process Management	4
OT	Organizational Training	Process Management	3
PMC	Project Monitoring and Control	Project Management	2
PP	Project Planning	Project Management	2
PPQA	Process and Product Quality Assurance	Support	2
QPM	Quantitative Project Management	Project Management	4
REQM	Requirements Management	Project Management	2
RSKM	Risk Management	Project Management	3

Capability Maturity Model Integration:

1. CMU – SEI created to assist organizations optimize their services.
2. Perform an Analysis of the Maturity Level within your organization following CMMI guidelines, as seen in this chart.
3. Decide on which services need to be updated, what must be accomplished, and assign a team with clear goals and scope.
4. Continue until desired Maturity Level is reached.

CMMC 2.0 Framework, by Function and Category

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

- **Mandated by the Under Secretary of Defense for Acquisition and Sustainment (OUSC(A&S)) for all Defense Industry Base (DIB) organizations to enhance the protection of Controlled Unclassified Information (CUI) and Federal Controlled Information (FCI) within the Supply Chain.** (December 2021)
- **The Cybersecurity Maturity Model Capabilities (CMMC) was developed to judge your organization's ability to adhere to these new protection standards for obtaining and continuing business with the United States Government.**
  - The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.
  - The CMMC effort builds upon existing regulation (DFARS 252.204-7012), that are based on trust, by adding a verification component with respect to cybersecurity requirements.
  - The goal is for CMMC to be cost-effective and affordable for small businesses to implement, at the lower CMMC levels.
  - Authorized and accredited CMMC Third Party Assessment Organizations (C3PAOs) will conduct assessments and issue CMMC certificates to Defense Industrial Base (DIB) companies at the appropriate level.

Compliance between CMMC and DFARS

Explanation Links:

- WISP
- DSP
- VCP
- RMP
- CRA
- VPMP
- IIRP
- SPBD
- SSP
- CSOP
- COOP
- SBC
- IAP
- CBP

Area of Responsibility for CMMC Audit Review	DFARS Requirement
Written Information Security Program (**WISP**) or Digital Security Program (**DSP**)	252.204-7008 252.204-7012 NIST 800-171 (multiple NFO controls)
Vendor Compliance Program (**VCP**)	252.204-7008 252.204-7012 NIST 800-171 NFO PS-7
Cybersecurity Risk Management Program (**RMP**)	252.204-7008 252.204-7012 NIST 800-171 NFO RA-1
Cybersecurity Risk Assessment Template (**CRA**)	252.204-7008 252.204-7012 NIST 800-171 3.11.1
Vulnerability & Patch Management Program (**VPMP**)	252.204-7008 252.204-7012 NIST 800-171 3.11.2
Integrated Incident Response Program (**IIRP**) - NIST SP 800-160	252.204-7008 252.204-7009 252.204-7010 252.204-7012 NIST 800-171 3.6.1
Security & Privacy By Design (**SPBD**)	252.204-7008 252.204-7012 NIST 800-171 NFO SA-3
System Security Plan (**SSP**)	252.204-7008 252.204-7012 NIST 800-171 3.12.4
Cybersecurity Standardized Operating Procedures (**CSOP**)	252.204-7008 252.204-7012 NIST 800-171 (multiple NFO controls)
Continuity of Operations Plan (**COOP**)	252.204-7008 252.204-7012 NIST 800-171 3.6.1
Secure Baseline Configurations (**SBC**)	252.204-7008 252.204-7012 NIST 800-171 3.4.1
Information Assurance Program (**IAP**)	252.204-7008 252.204-7012 NIST 800-171 NFO CA-1
Cybersecurity Business Plan (**CBP**)	CMMC - **C034-L4-P1163**

DFARS – Defense Federal Acquisition Regulation Supplement

NIST SP 800-171
NIST SP 800-53 R4

The C3PAO will review and validate each of the plans listed here, plus more, before approving a CMMC certification.

CERT- Resilience Management Model (RMM)

Engineering	
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management	
COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training & Awareness
RISK	Risk Management

Operations Management	
AM	Access Management
EC	Environmental Control
EXD	External Dependencies
ID	Identity Management
IMC	Incident Management & Control
KIM	Knowledge & Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis & Resolution

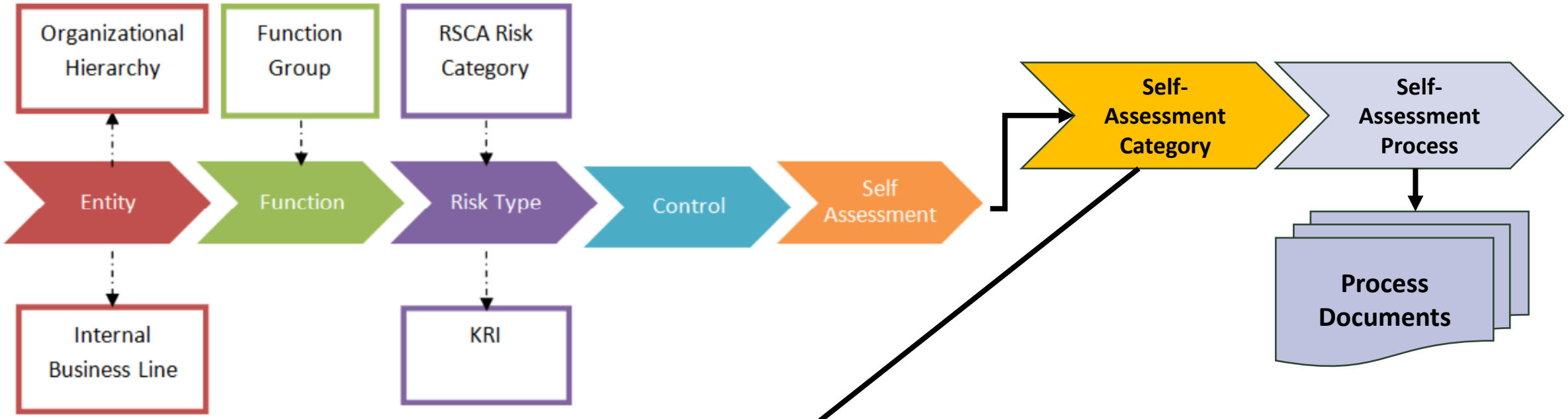
Process Management	
MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus

4 Categories with 26 Process Areas

1. Enterprise Management
2. Operations Management
3. Process Management
4. Engineering

CERT-RMM is a **maturity model** that promotes the convergence of security, business continuity, and IT operations activities to help organizations actively direct, control, and manage operational resilience and risk.

Risk Controls Self Assessment - RCSA

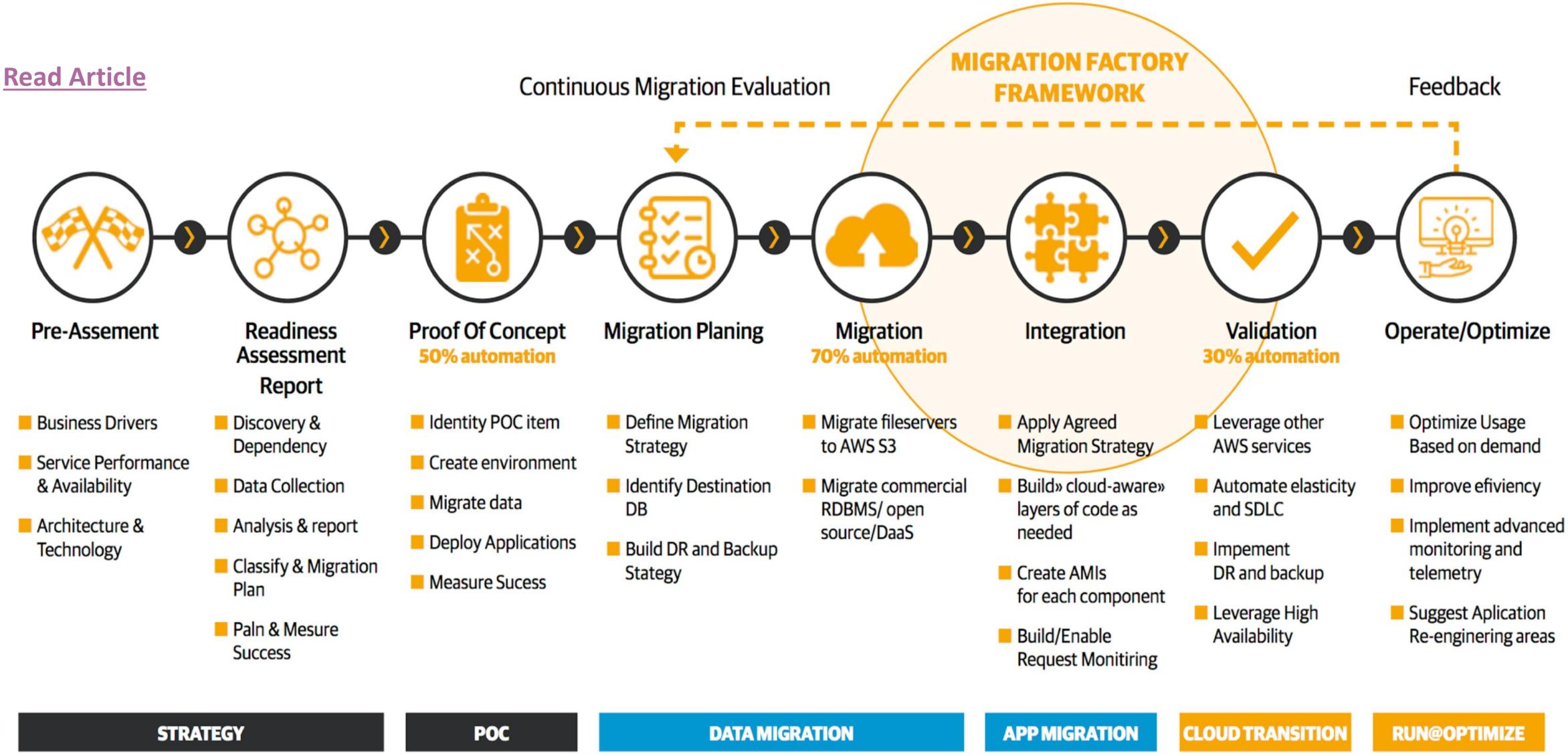


List of Risk Control Self Assessment Possibilities (1-5 / Low to High)

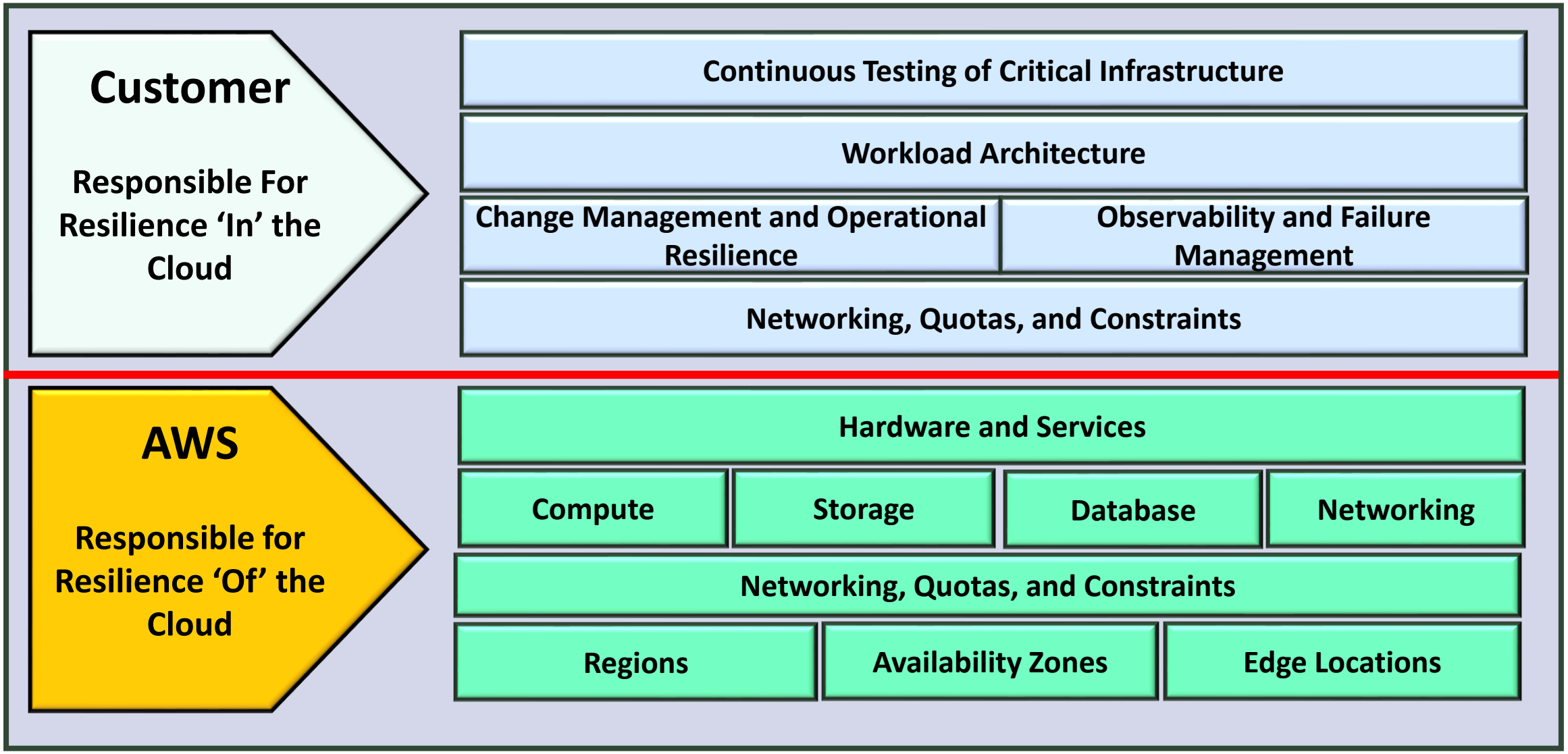
				Internal Risk					Residual Risk					
#:	Entity:	Function:	Risk Category:	Prob.	Impact	Priority	Score	Rank	Prob.	Impact	Priority	Score	Rank	Controls & Measures
	LOB	DEPT	Fire Evacuation	Medium	High	High	5		Medium	High	High		High	Escape Routes / Extinguishers
														Fire Marshal / Drills

Using AI Planning for Migrating Applications to AWS Cloud

Read Article



AWS Shared Responsibility Model

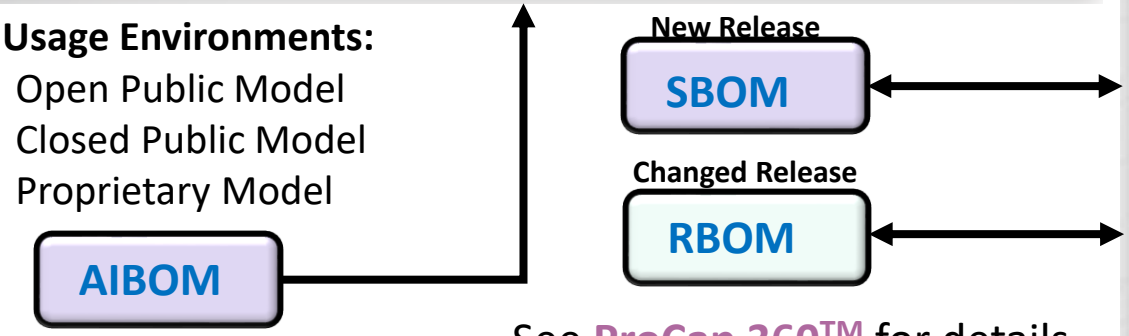


Job Function Responsibilities for AI Development

Cloud and Compute Infrastructure Providers Responsibilities Overview				
A. Secure Environments	**B. Drive Responsible Model and System Design**	**C. Implement Data Governance**	**D. Ensure Safe and Secure Deployment**	**E. Monitor Performance and Impact**
1. Vet hardware and software suppliers 2. Institute best practices for access management 3. Establish vulnerability management 4. Manage physical security	1. Report vulnerabilities	1. Keep data confidential 2. Ensure data availability	1. Conduct systems testing	1. Monitor for anomalous activity 2. Prepare for incidents 3. Establish clear pathways to report harmful activities

AI Usage Environments:

- Open Public Model
- Closed Public Model
- Proprietary Model

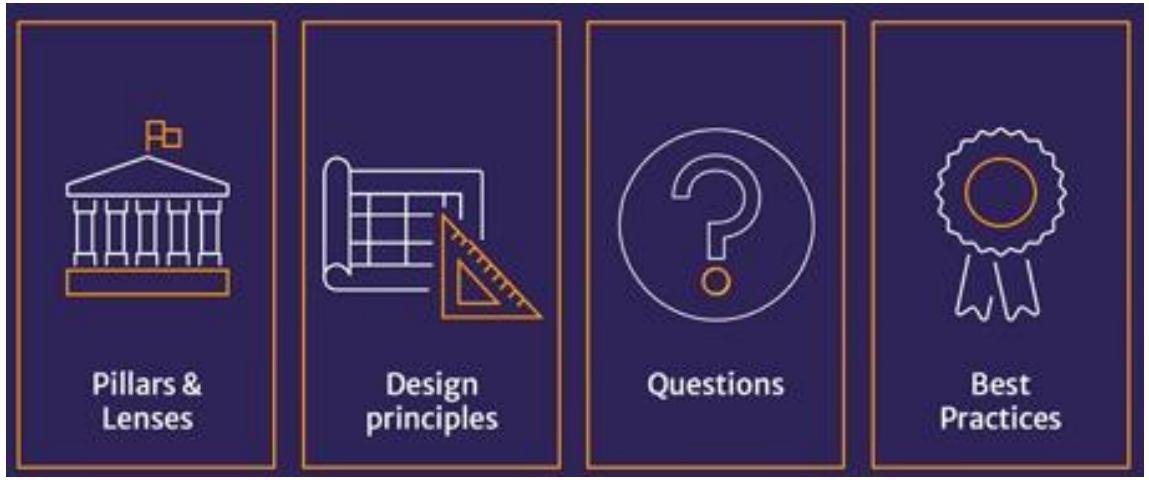


See ProCap 360™ for details

The use of Bill of Materials is recommended to obtain and maintain a Vulnerability-Free environment. AIBOMs work on AI inputs and usage. See CISA AI Roles and Responsibilities paper and see DHS AI Framework guidelines.

AI Developers Responsibilities Overview				
A. Secure Environments	**B. Drive Responsible Model and System Design**	**C. Implement Data Governance**	**D. Ensure Safe and Secure Deployment**	**E. Monitor Performance and Impact**
1. Manage access to models and data 2. Prepare incident response plans	1. Incorporate Secure by Design principles 2. Evaluate dangerous capabilities of models 3. Ensure alignment with human-centric values	1. Respect individual choice and privacy 2. Promote data and output quality	1. Use a risk-based approach when managing access to models 2. Distinguish AI-generated content 3. Validate AI system use 4. Provide meaningful transparency to customers and the public 5. Evaluate real-world risks and possible outcomes 6. Maintain processes for vuln. reporting and mitigation	1. Monitor AI models for unusual or adversarial activity 2. Identify, communicate, and address risks 3. Support independent assessments

What is a Well-Architected Framework & Chaos Testing



Recovery Planning

Build Resilience and Reliability into applications via Gremlin and SBOMs

Systems Design

WAF - Well Architected Application testing

Gremlin Chaos Testing

Error Reports and Corrective Procedures

- Create Experiment
- Run Experiment
- Root Cause Determination
- Problem Resolution
- Problem Runbooks

Improvement plan

AWS / WAF

Improvement item summary

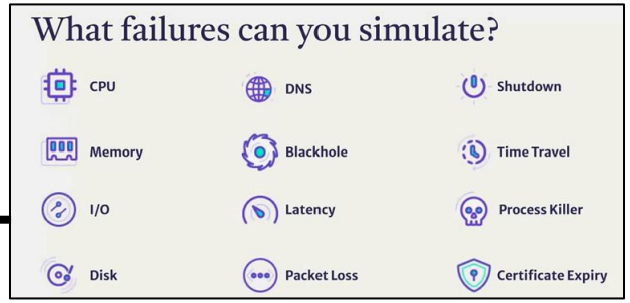
High risk: 11
Prioritized high risk: 11
Medium risk: 0
Prioritized medium risk: 0

Pillar	High risk	Medium risk	Prioritized high risk	Prioritized medium risk
Reliability	11	0	11	0
Operational Excellence	0	0	0	0
Security	0	0	0	0
Performance Efficiency	0	0	0	0
Cost Optimization	0	0	0	0
Sustainability	0	0	0	0

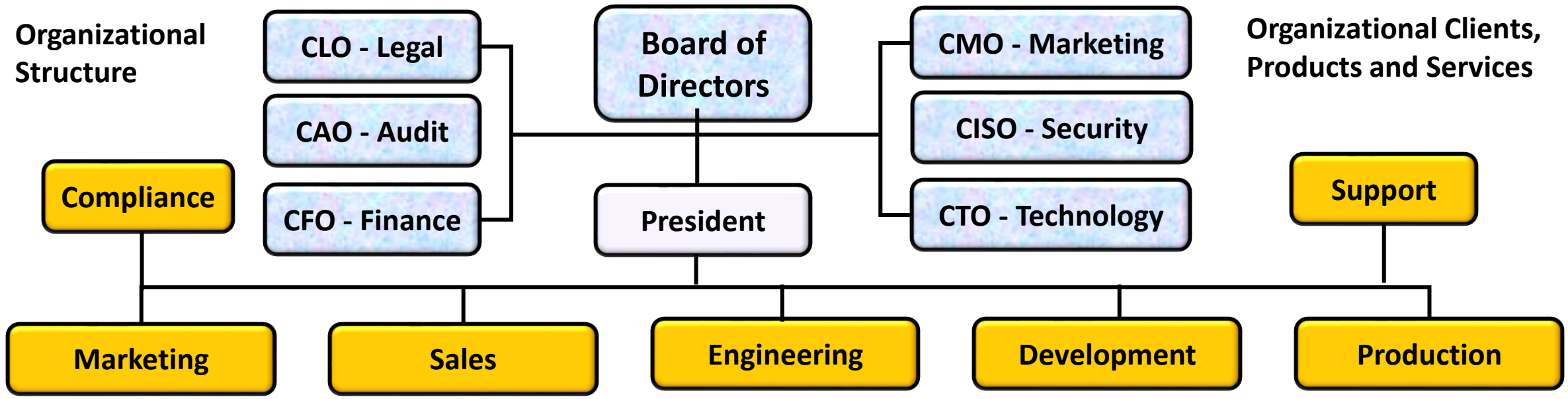
High risk

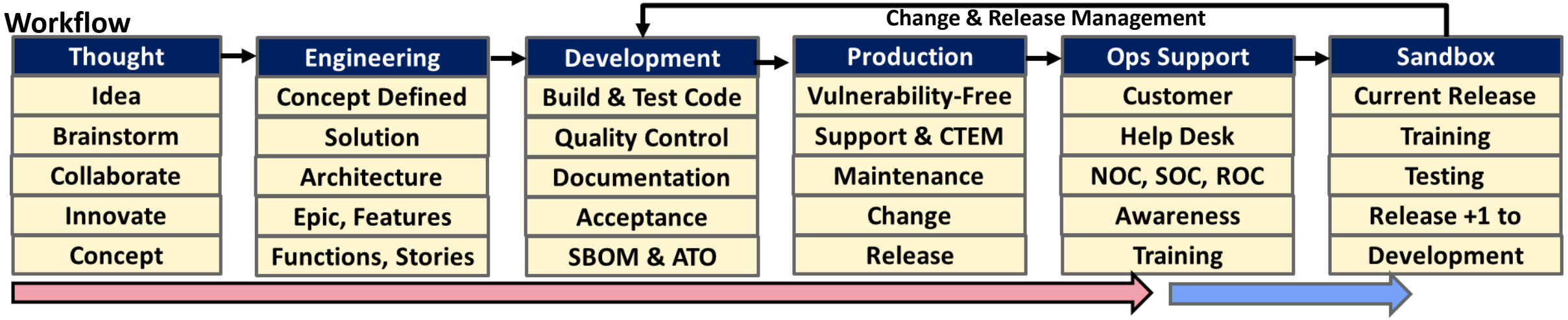
Methods:

- **Chaos Engineering**
  Custom or one-off exploratory testing to find unknown failures modes and new weaknesses within your system.
- **Validation testing**
  Regularly run scenarios and simulate failures to track reliability, verify resilience, and uncover known weaknesses to prevent outages or incidents.



Organization and Functional Responsibilities





What is Enterprise Resilience comprised of?

- Enterprise Resilience requires a Company Culture and Awareness
- Site Reliability Engineering (SRE)
- Metrics, Monitoring & Reporting
- Support & Improvement
- Automation

Enterprise Resilience concists of:

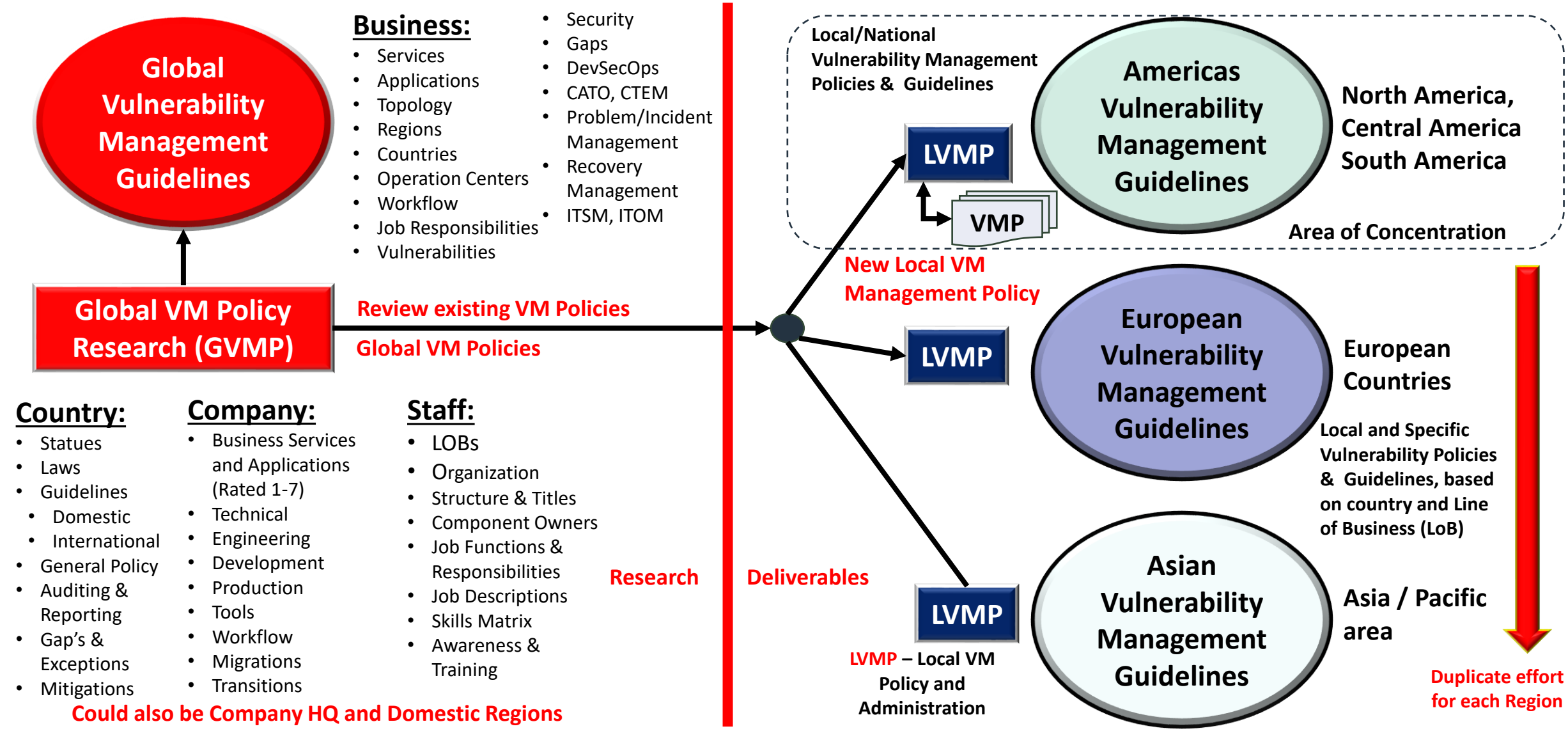
- Enterprise Products & Services (Company Jewels),
- Critical Economic Services, Financial Health, and Visibility,
- Brand and Company Reputation,
- Legal, Audits, & Compliance (Audit Universe - GRC)
- Personnel Protection and Violence Prevention,
- Risk Management Foundation (RMF), Business Impact Analysis (BIA), Identity Management and Access Controls (IM, IAC – Zero Trust and MFA)
- Recovery Groups, RTO, RPO, RTC, Certifications
- Business Continuity / Continuity of Operations/ Disaster Recovery, Emergency Management
- Crisis Management & Communications
- Critical Environments (Domain Management),
- Information Security (CSF),
- Human Resource Management (Personnel Safety & Violence Prevention – Active Shooter),
- Production Operations and Support (ITOM, ITSM),
- Incident & Problem Response, Supply Chain Resilience,
- Organizational Behavior,
- Migrating to the Cloud and hybrid Environments,
- Center of Excellence (COE) implementation.

Business Continuity Management components

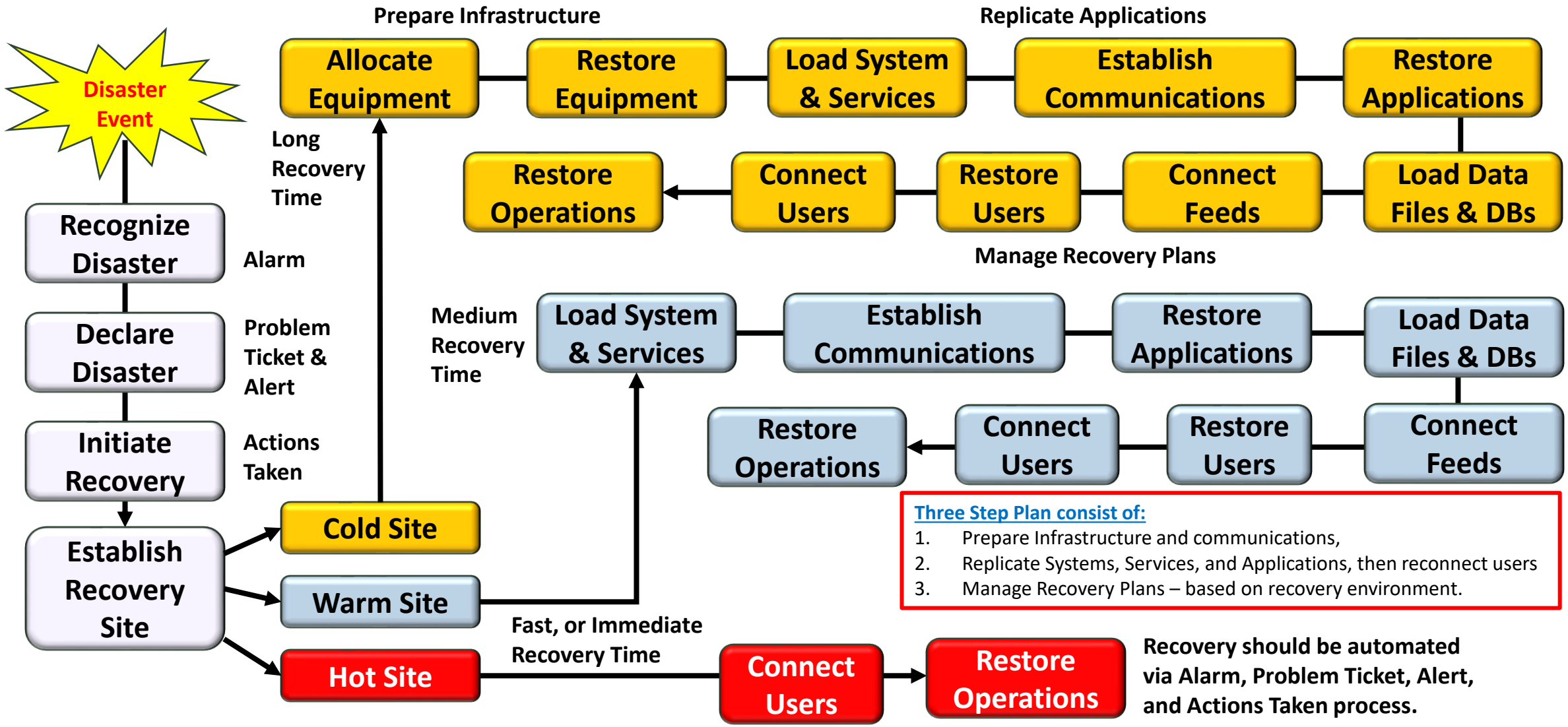
- **Preserve** the company Brand and Reputation, while protecting personnel.
- **Plan** for natural and man-made disaster events to reduce / eliminate outages.
- **Identify** and eliminate Risks and Business Flow Impacts to the company, its people, and resources.
- Adhere to Resilience Management Model (RMM)
- **Eliminate** Single-Point-Of-Failure.
- **Adhere** to regulatory and business requirements.
- **Ensure** continuity of business under catastrophic conditions – problems, incidents, and disaster events
- **Agree on** Recover Strategy and Select Tools
- **Integrate** production, testing, validation and continuous Improvement

Include Emergency Management, Site Protection, Salvage, and Restoration for business locations

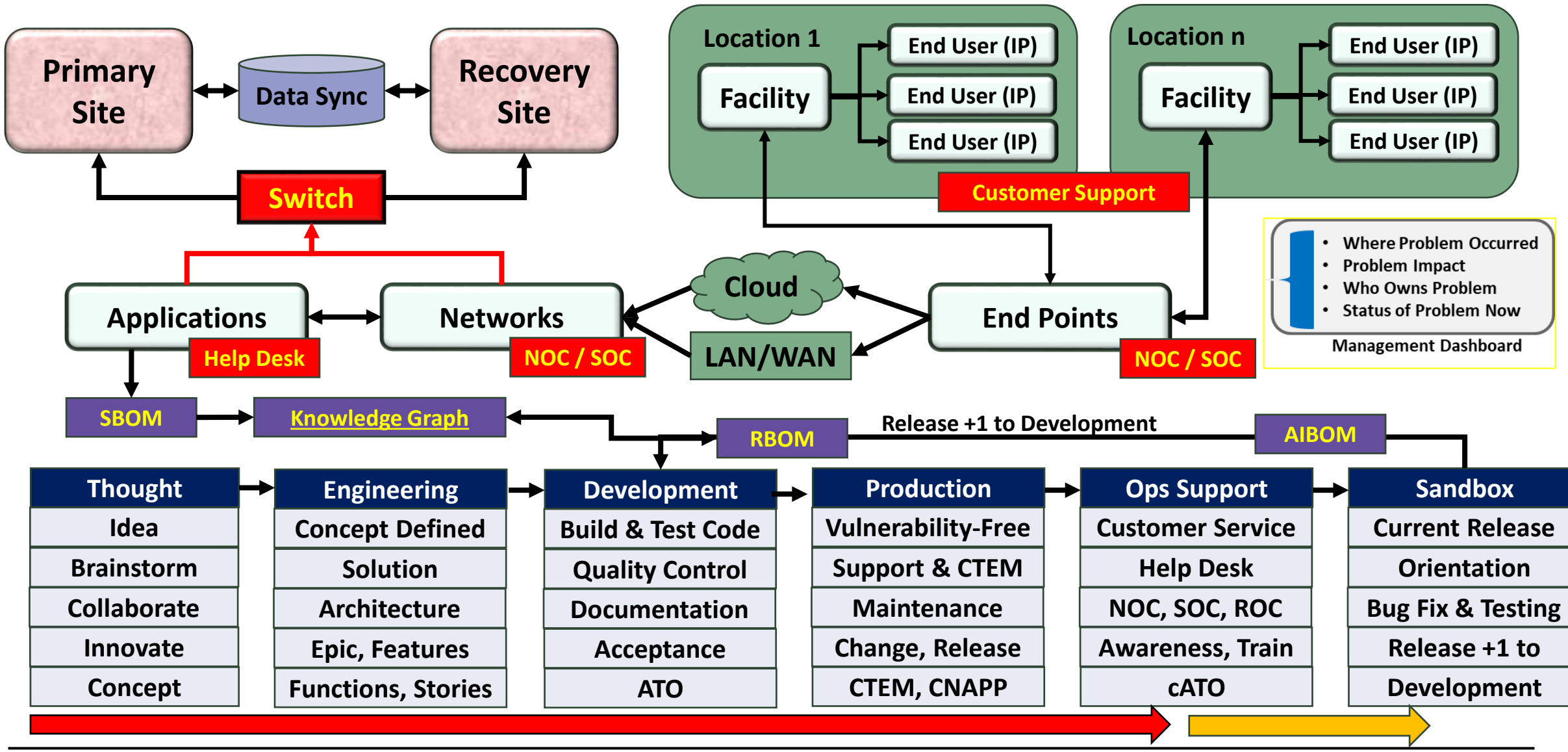
Global Vulnerability Management Policy generation



Sequence of Events to enact a Recovery Operation



From Idea to Product, with Support and Recovery



Overview of Project Plan Example

Initiation

Project Initiation:

- Mission Statement
- Scope
- Goals
- Objectives
- Organizational structure
- Primary Contacts
- Stakeholders
- Kick-Off Letter and Meeting
- Awareness Training

Problem Definition

Needs Analysis:

- Compliance & Risks Management
- Recovery Requirements
- BIA & Audit
- Artefacts
- Assessment
- Analysis
- Tool Needs
- Findings
- Teams & Tools
- Team Training
- Report
- Presentation

Problem Impact

Management Review:

- Gaps, Exceptions, and Weaknesses
- Report & Presentation
- Conclusions
- Recommendations
- Questions & Answers
- Objections & Responses
- Direction Statement
- Recovery Plan and exercise schedule
- Approval
- Funding
- Initiation

Problem Solution

Project Plan:

- Plan of Action
- Milestones
- Resources
- Duration & Metrics
- Costs – CAPEX and OPEX
- Deliverables
- Documentation
- Awareness
- Training
- Integration
- Automation
- Monitoring
- Savings

Integrated Problem Solution

Implementation Plan:

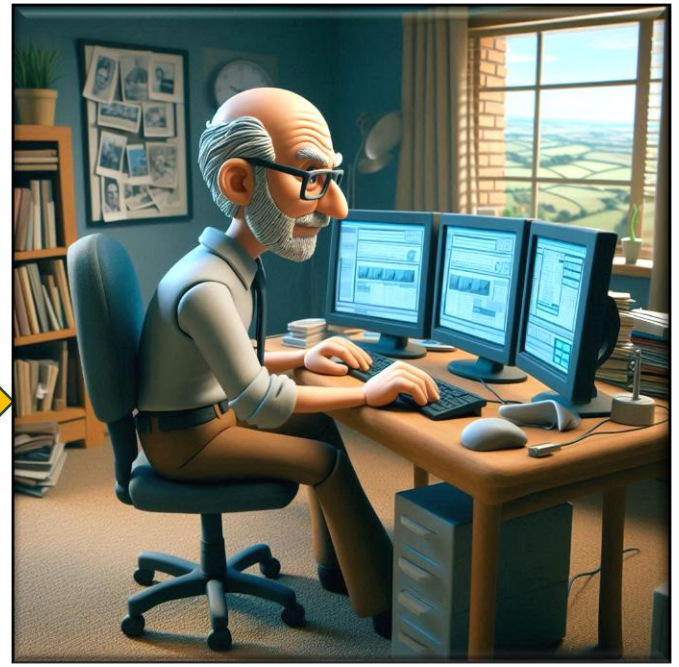
- Risk Management Framework (RMF)
- Software Development Life Cycle
- Software Bill Of Materials (SBOM), also RBOM and AIBOM
- Vulnerability-Free Applications and Services in Production
- Achieve: “Secure by Design”, SecDevOps, Continuous Threat Exploitation Management (CTEM), Continuous Authorization To Operate (CATO)
- Integrated Workflow at reduced costs
- Reduced Toil on Staff

Reaching out to assist our clients

- Discuss
- Define
- Propose
- Achieve

Quality Service at a Reasonable Price

Helping Clients to achieve success



If you find the information included in this presentation of value and want to explore methods to improve the reliability of your enterprise and IT environment, please contact me to discuss your needs and request our assistance.

We look forward to our future relationship.

Thomas Bronack, CBCP
President
Data Center Assistance Group, LLC
Website: http://www.dcag.com
bronackt@dcag.com
bronackt@gmail.com
917-673-6992