Thomas Bronack, CBCP

Presentation Topics

- Why Enterprise Resilience
- Knowing your Company and Compliance to Service Level Agreements
- Identifying and Controlling Risks
- Recovery Management
- Protecting the Company
- Reducing Problems and Costs
- Staff Awareness and Training

Tom Specializes in:

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

Risk Management

Contact Information:

- bronackt@gmail.com
- bronackt@dcag.com
- (917) 673-6992

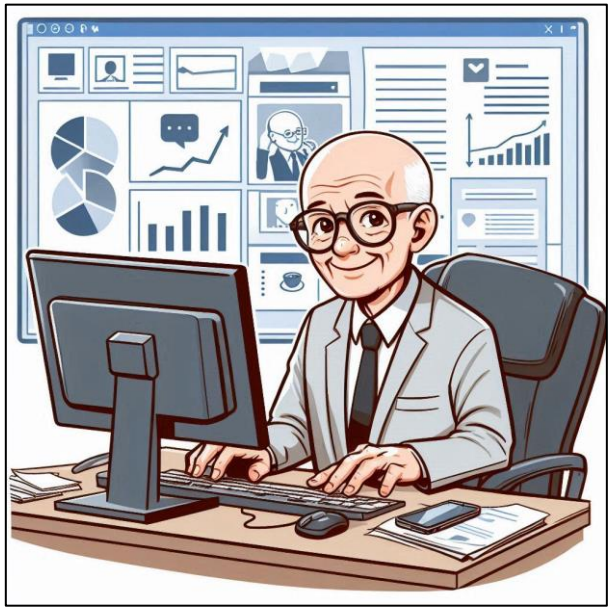
A word from Thomas Bronack

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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 am the founder and president of the Data Center Assistance Group (DCAG).

DCAG provides enterprise analysis, evaluation, recommendations, and planning materials to eliminate weaknesses and optimize operations. We optimize 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.

DCAG follows the "**Whole of Nation**" and "**Secure by Design**" guidelines developed by DHS/CISA to produce vulnerability-free components through 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.

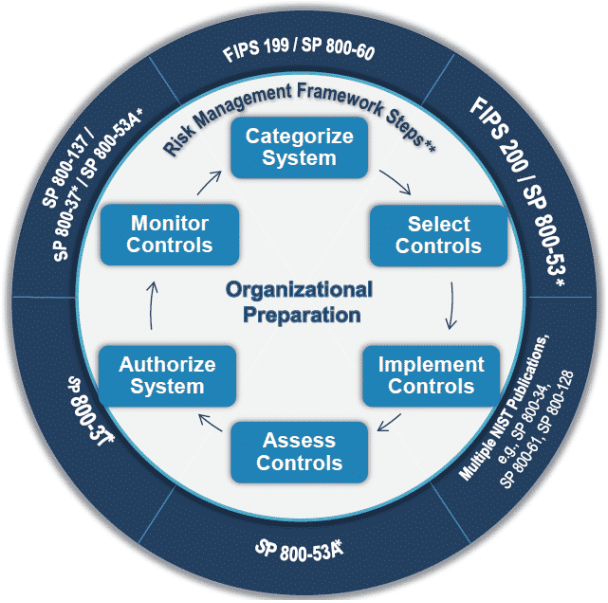


A strong generalist with extensive IT industry experience, ready to help you.

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

What is Risk Management and why is it important

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



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

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

- **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

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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

Know and Control your Environment

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

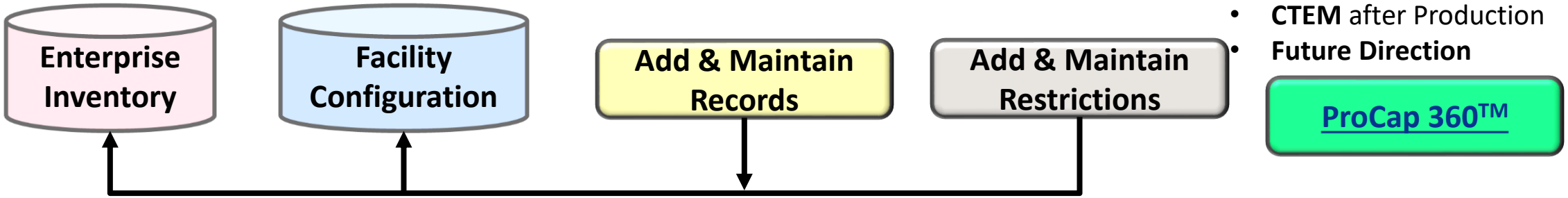
- **HW**AM
- **SW**AM
- **Tech**nology Management
- **Release** Management
- **Patch** Management
- **End-of-life**

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

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

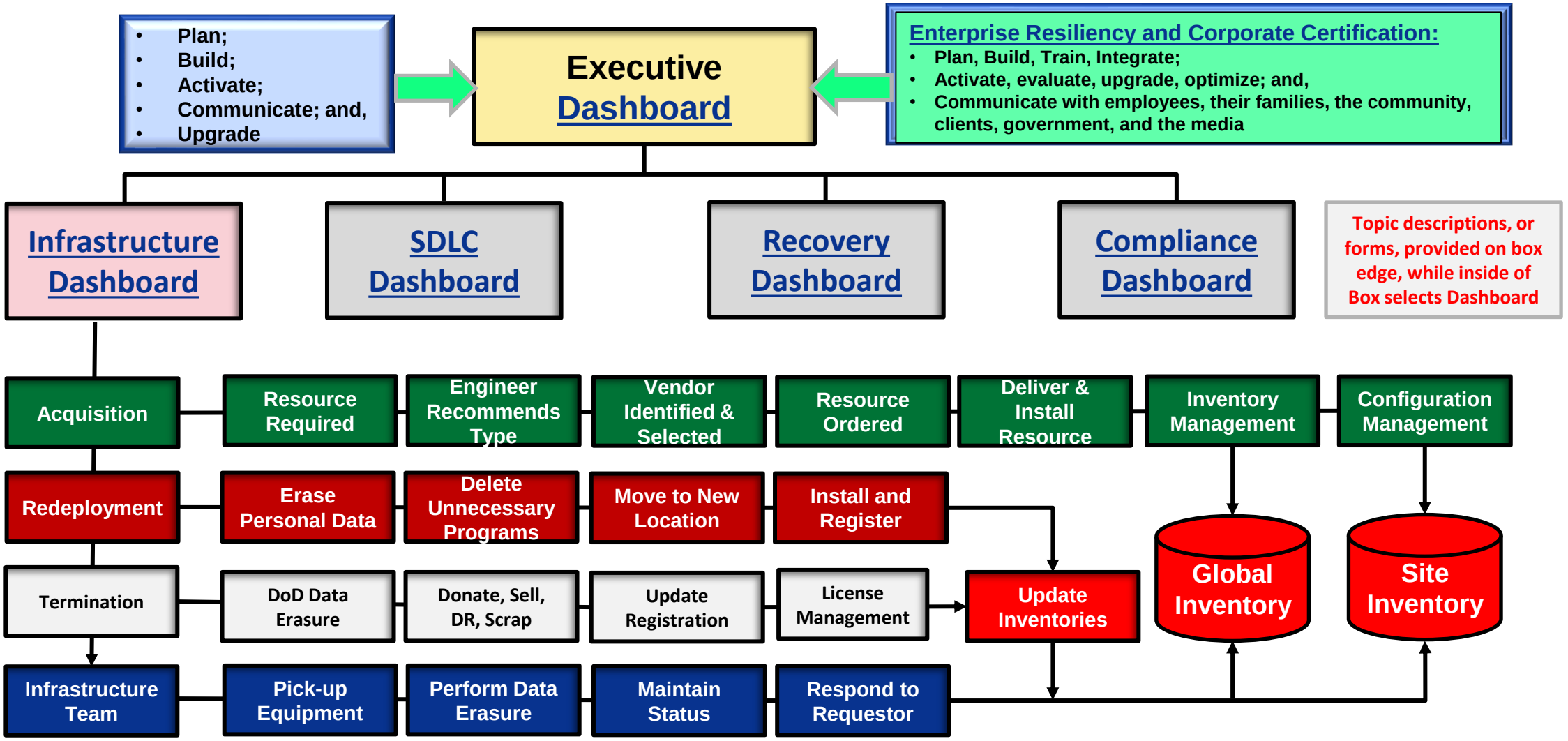
- **Components** via SBOM RBOM, or AIBOM
- **Identify Countries** parts origin
- Adhere to Laws and **country restrictions**
- Identify Vulnerabilities
- License Management

- **Identify** Vulnerabilities prior to production
- **Use SBOMs, RBOMs, AIBOMs, and a Knowledge Graph**
- **Apply** Patches and Update Releases
- **Validate** mitigations
- **Vulnerability-free** production
- **CTEM** after Production
- **Future Direction**



Asset Management Process

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Overview of Project Plan Example

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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

Safeguarding your Enterprise

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Business Analysis

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

C Level Functions

- Board of Directors
- CIO / CTO
- CISO
- COO
- CFO
- CMO
- Auditing
- Legal

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

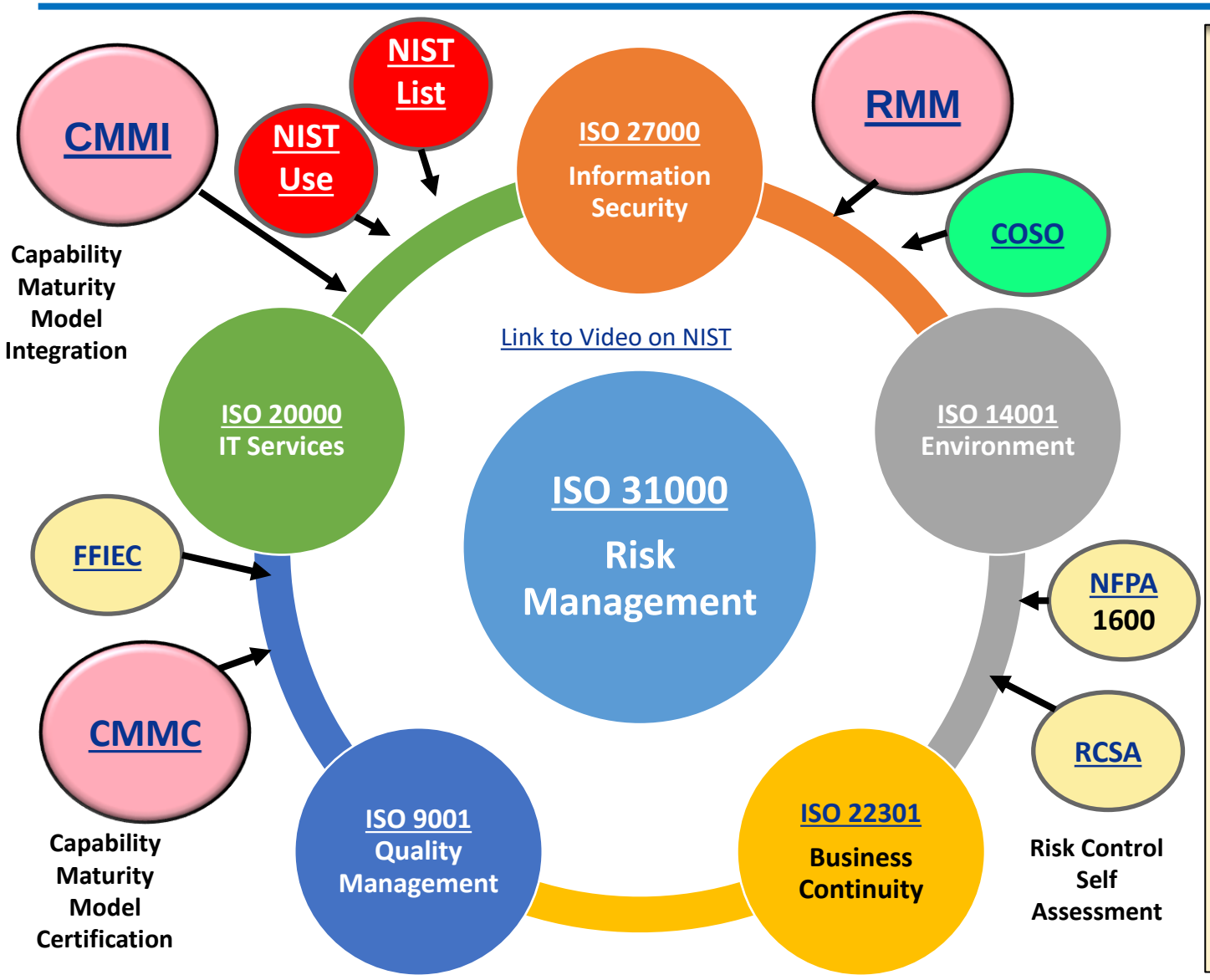
Vulnerability Laws and Regulations requiring SBOMs

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

- 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.

The newest Integration Model – PRIME Approach

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Developing a business optimization approach that combines these ISO Standards (**International**) and NIST Standards (**Domestic**) will achieve certification more quickly. Utilizing RMM (Risk Maturity Model), CMMI (Capability Maturity Model Integration), and a Vulnerability Management System (VMS) like ProCap 360™ will reduce operational errors by delivering Vulnerability-Free applications to production. Consider using (CTEM) Continuous Threat Exposure Management systems after applications are in production to detect and respond to new errors and vulnerabilities.

Implementing the standards separately will result in overlaps and inefficiencies, so develop Crosswalks to reduce toil..

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).

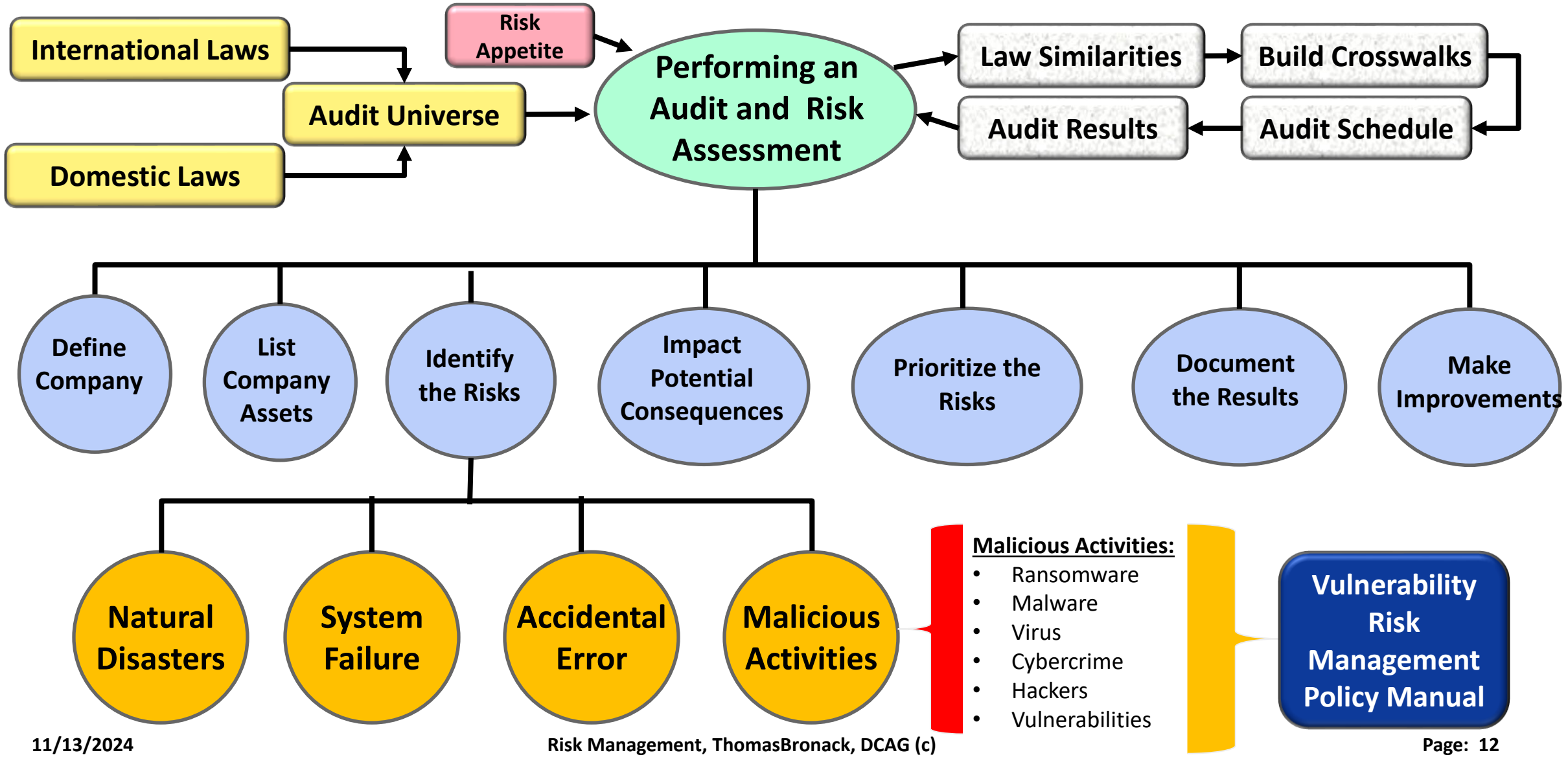
Then implement your **Business Continuity** (ISO 22301) Recovery Certification Process for Emergency, Crisis, Business, and IT Disaster Recovery Management.

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 an Audit and Risk Assessment

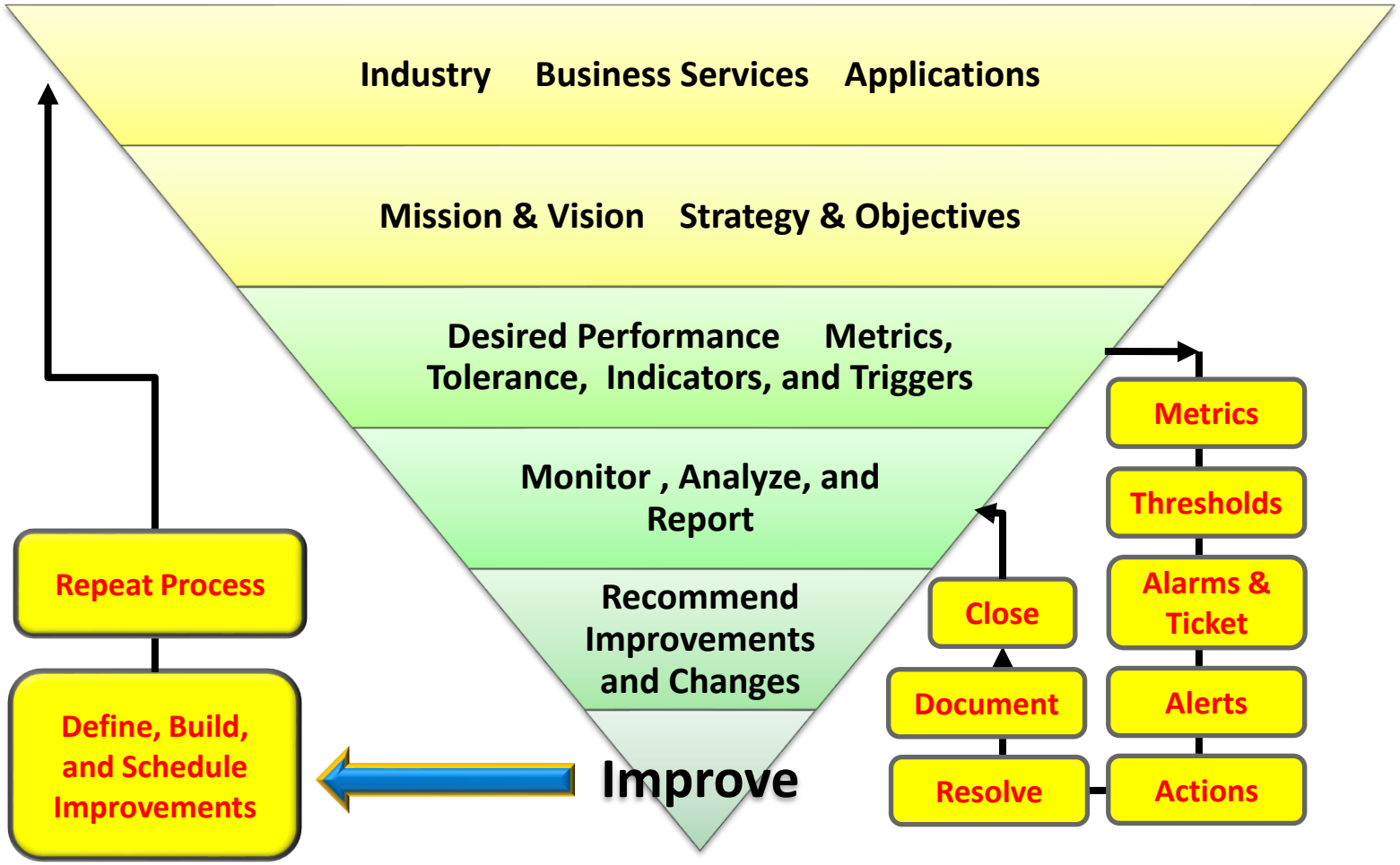
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



The Risk Appetite Process Using COSO

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Defining the Risk Appetite using COSO



COSO for Risk Appetite & Evaluation:

1. Review Business Mission and Vision
2. Consider 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, define and measure metrics, indicators, and triggers.
8. Changing context of the business culture and competitive environment.
9. Monitors performance and revises appetite or strategy, as needed.

Getting started with facts and a defined direction

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Know your company:

1. Most Important Applications & Services (**Family Jewels**).
2. BIA to Define the damage caused if lost and maximum duration of survival without the application or service.
3. Define Requirements, Scope, Risk, Security, DevSecOps, Testing, Recovery, Acceptance, Deployment, and ITSM, ITOM.
4. Define Audit Universe implement legal & auditing functions.
5. Define Ideation, Brainstorming, Collaboration, to Concept cycle.
6. Implement Systems Engineering Life Cycle (SELC) to respond to new ideas or business opportunities.
7. Implement Systems Development Life Cycle (SDLC) to deploy new products and services.
8. Define Company Organization to respond to cybersecurity and technology problems in a timely manner to the appropriate authorities (i.e., SEC Rule 2023-139)

Know your Environment:

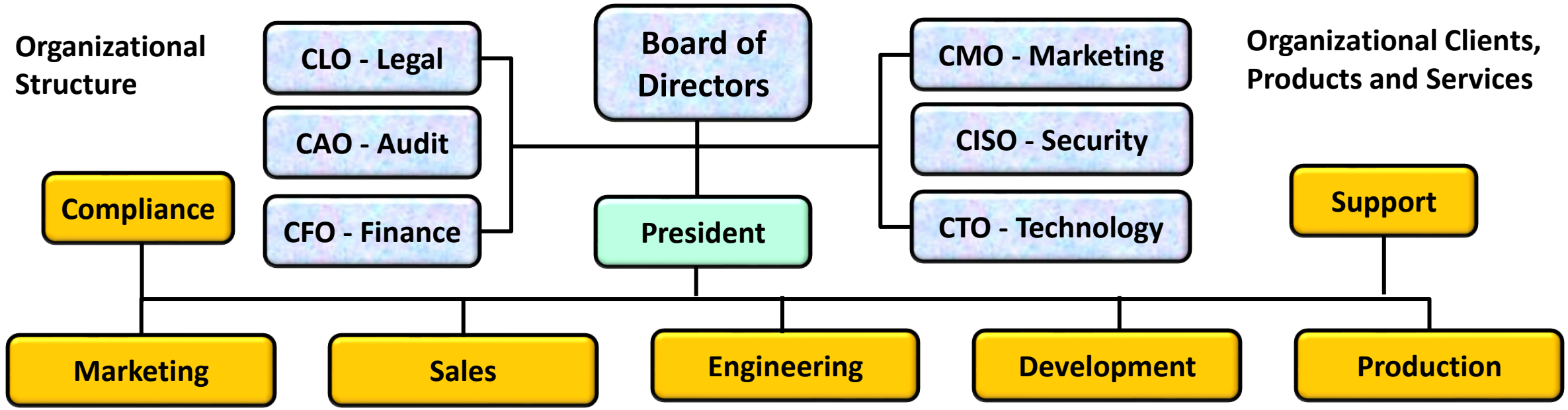
1. Physical and Data Security (Data Sensitivity & Data Flow).
2. Architecture and engineering process.
3. Asset Inventory and Configuration Management.
4. Identify and Access Management.
5. GRC based compliance and attestation, CIA based cybersecurity and elimination of viruses and malware.
6. Development and implementation of DevSecOps.
7. Personnel Titles, Job Functions and Responsibilities, and the integration of sensitive and required services within their everyday work tasks.
8. Staff training and development.
9. Continuous Monitoring and Improvement, along with the adoption of new technologies and processes (i.e., SRE).
10. Deploying error-free products and services (see EO 14028 and OBM M-22-18) and utilize the latest technologies to respond to encountered anomalies and verify compliance.

Set you direction:

1. Most efficient, compliant, and secure production environment, capable of recovering from disaster events and providing continuous vulnerability-free products and services to customers. **Continuity of Succession / Delegation of Authority** must be included along with definition of duties.
2. Integrate guidelines, standard Operating Procedures, skill development, and awareness throughout the organization.

Organization and Functional Responsibilities

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Workflow

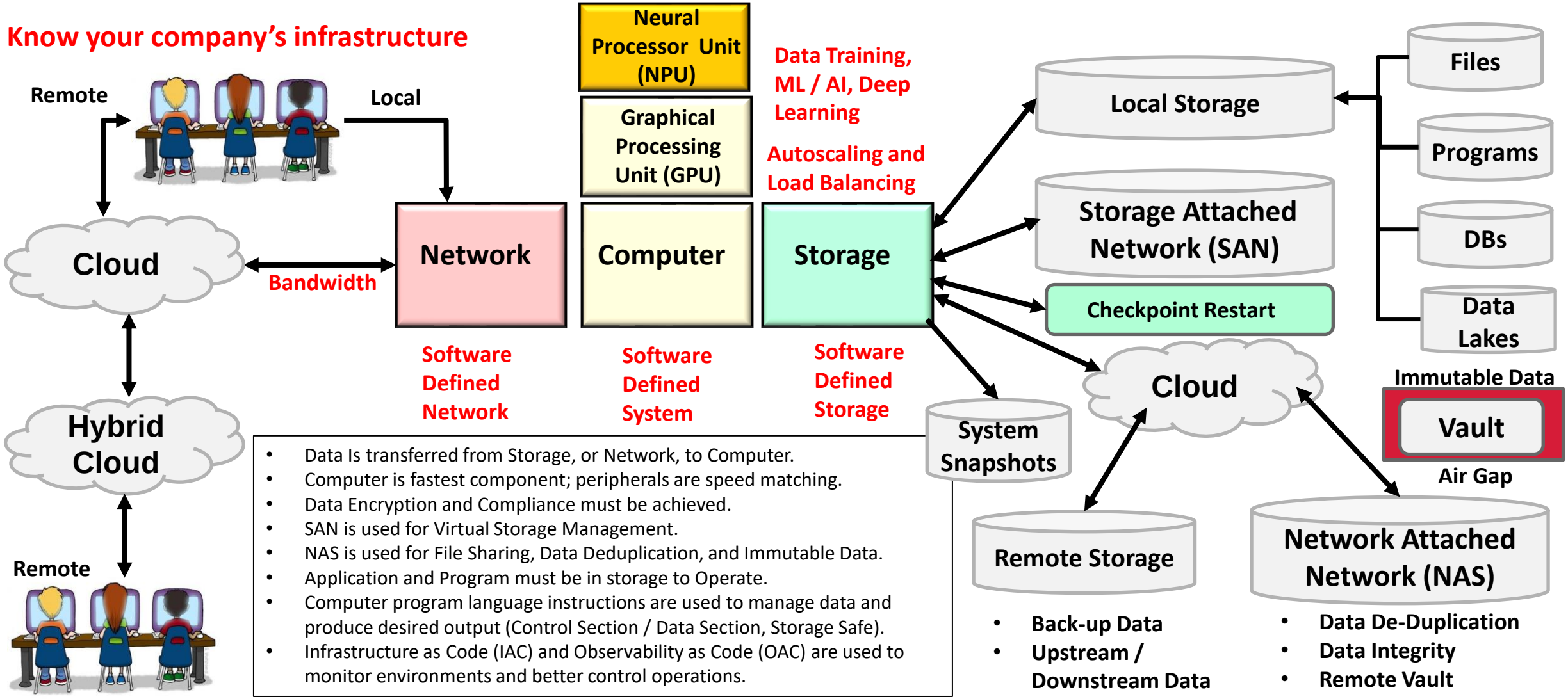
Change & Release Management

Thought	Engineering	Development	Production	Ops Support	Sandbox
Idea	Concept Defined	Build & Test Code	Vulnerability-Free	Customer	Current Release
Brainstorm	Solution	Quality Control	Support & CTEM	Help Desk	Training
Collaborate	Architecture	Documentation	Maintenance	NOC, SOC, ROC	Testing
Innovate	Epic, Features	Acceptance	Change	Awareness	Release +1 to
Concept	Functions, Stories	SBOM & ATO	Release	Training	Development

Monitoring Operations and Controlling Resources

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Know your company's infrastructure



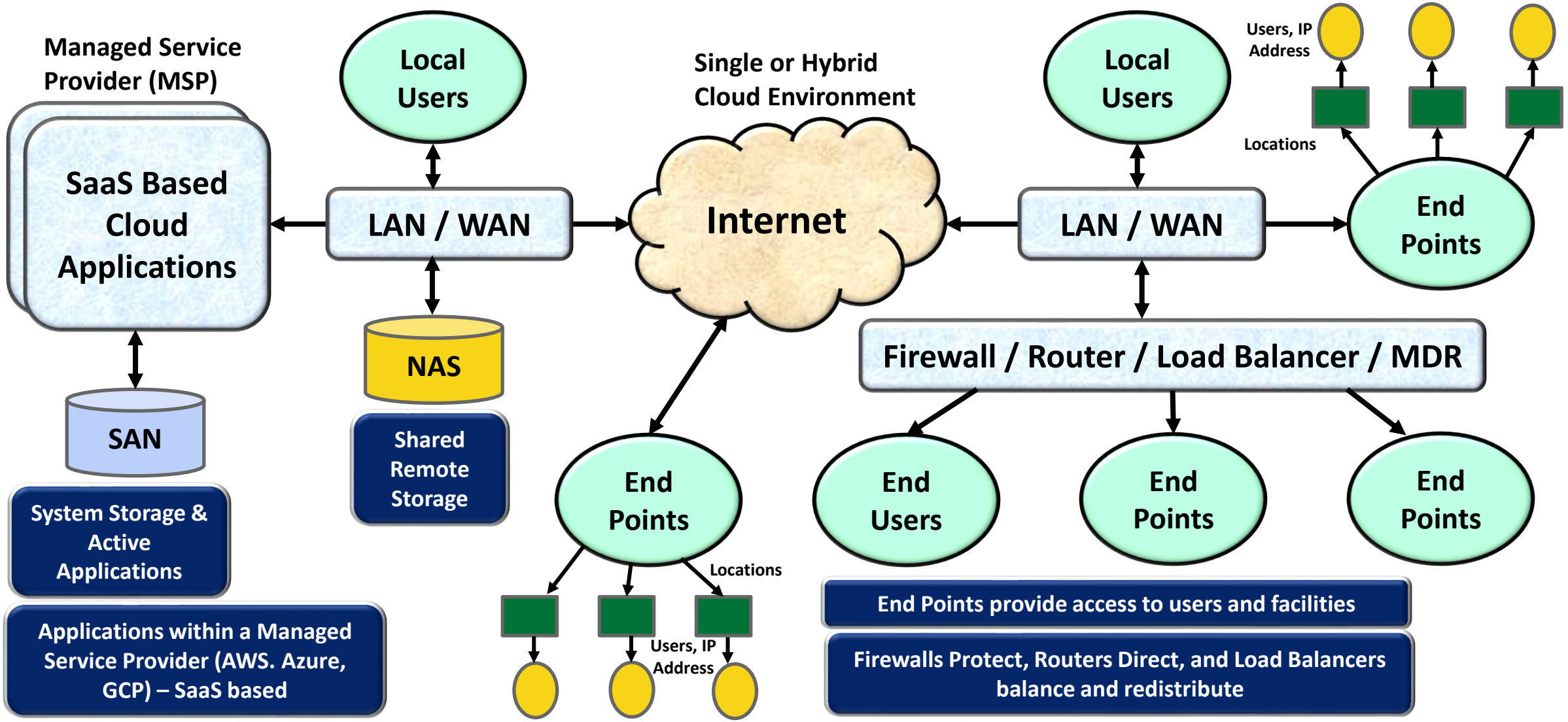
- Data Is transferred from Storage, or Network, to Computer.
- Computer is fastest component; peripherals are speed matching.
- Data Encryption and Compliance must be achieved.
- SAN is used for Virtual Storage Management.
- NAS is used for File Sharing, Data Deduplication, and Immutable Data.
- Application and Program must be in storage to Operate.
- Computer program language instructions are used to manage data and produce desired output (Control Section / Data Section, Storage Safe).
- Infrastructure as Code (IAC) and Observability as Code (OAC) are used to monitor environments and better control operations.

- **Back-up Data**
- **Upstream / Downstream Data**
- **Secure Vaulting**

- **Data De-Duplication**
- **Data Integrity**
- **Remote Vault**
- **Immutable Data**

Active Cloud Environment (MSP to Hybrid Clouds)

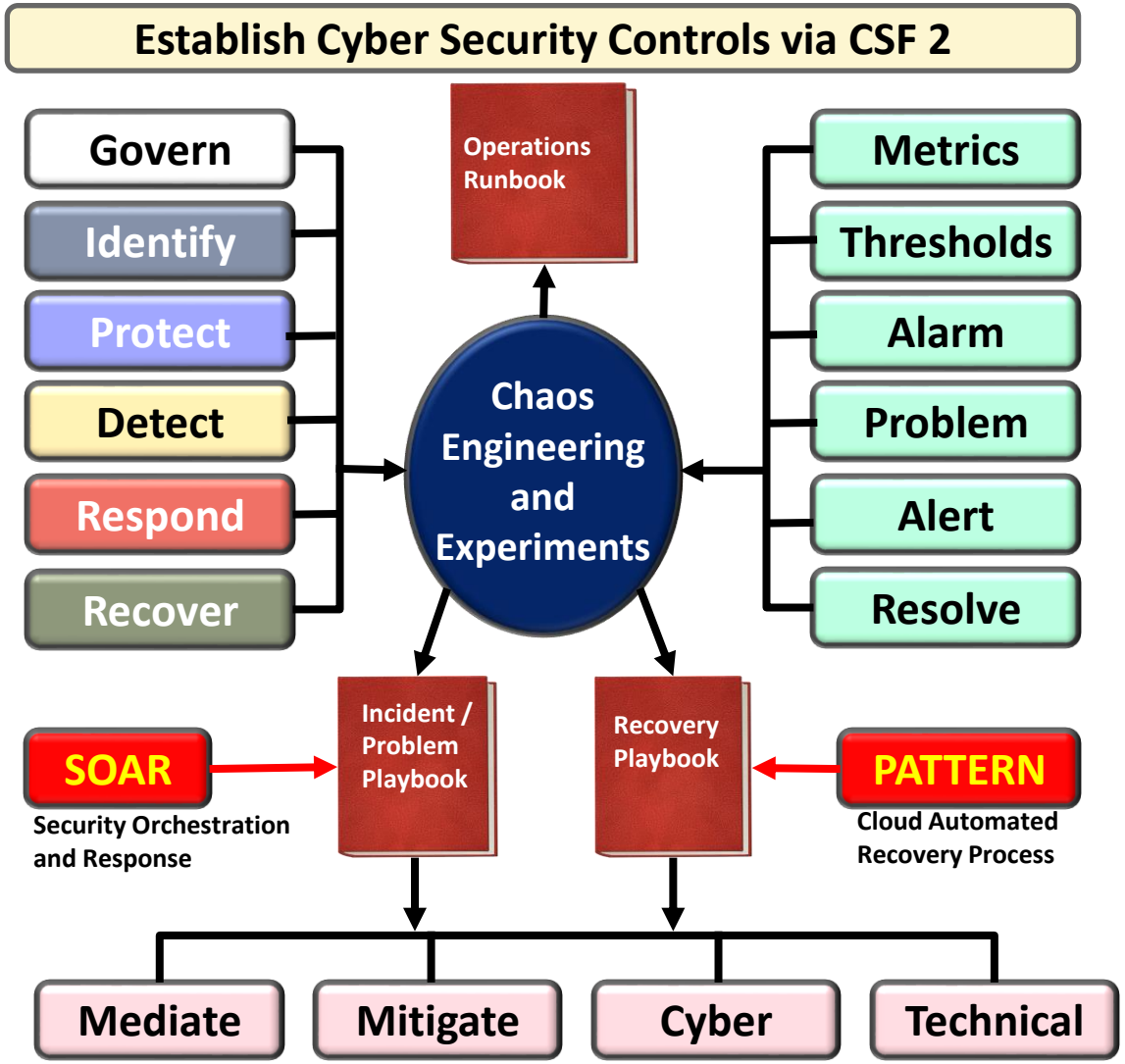
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



NIST CSF 2.0 Categories and Application

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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



Cybersecurity Controls within NIST SP 800-53.r5

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

See Link for NIST SP800-53r5 description detail

See Link for NIST SP 800-34 R1 Latest Detail

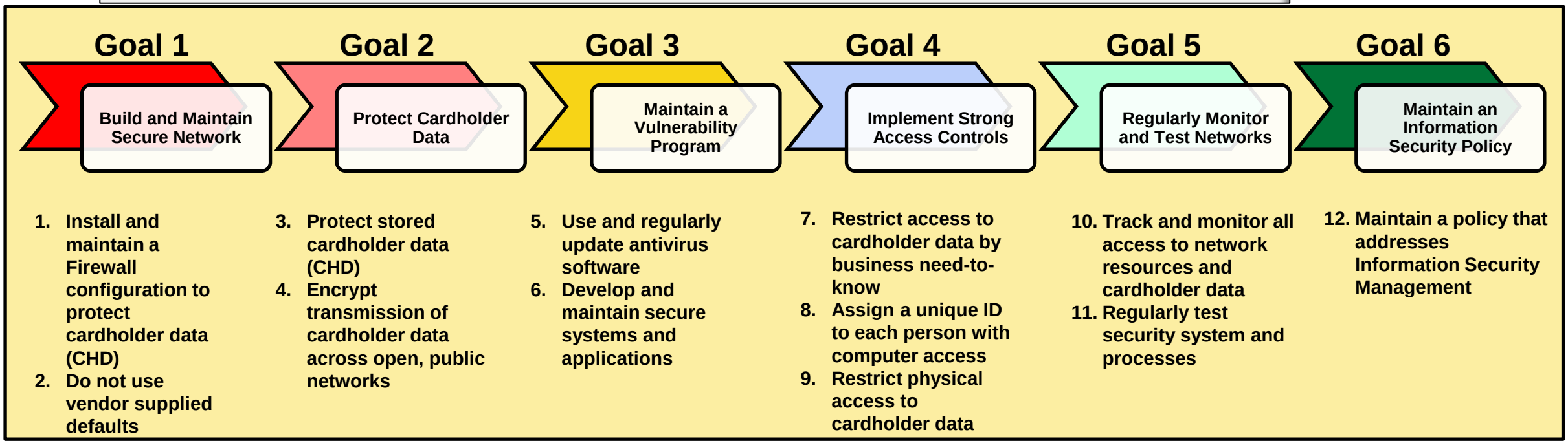
Payment Card Industry Data Security Standard (PCI/DSS)

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Payment Card Industry Data Security Standard (PCI DSS) compliance is adherence to the set of policies and procedures developed to protect credit, debit and cash card transactions and prevent the misuse of cardholders' personal information. PCI DSS compliance is required by all card brands.

The Payment Card Industry Security Standards Council (PCI SSC) develops and manages the PCI standards and associated education and awareness efforts. The PCI SSC is an open global forum, with the five founding credit card companies -- American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. -- responsible for carrying out the organization's work.

The Payment Card Industry – Data Security Standard implementation process



Cybersecurity Testing Steps

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Updates for Improvements

Plan the Exercise
- Format and Type of Exercise
- Announced, or unannounced
- Participant participation, or absent
- Set a Date & Time

Establish Communi-cations Protocol
- Define Protocols
- Ensure Secure Communications

Conduct Pre-Exercise Training
- Provide Team Training
- ensure participants know their role
- Ensure Role Backup is Designated

Conduct Pre-Exercise Testing
- Provide test run-throughs
- Make improvements as needed

Conduct Exercise
- Conduct scheduled test scenario(s)
- Collect Data on exercise performance
- Summarize test performance

Monitor & Analyze
- Continuously monitor & analyze
- Access actual exercise results to planned

Post Test Review
- Review and determine success
- Recommend improvements

Make Improve-ments to Exercise
- Implement exercise improvements and re-run exercise
- Continue until improvements are no longer needed

Cyber Security Exercise Plan

Comm. Plan

- Basic IT Security
- Cybersecurity Framework (CSF)
- Vulnerabilities and SBOMs
- DevSecOps
- VMaaS, CTEM
- Secure by Design
- CISA, NIST, ISO

Cyber Security Exercise Scripts

Test & Monitor

Post Incident Review:
- Problem Analysis
- Plan Anomalies'
- Changes Suggested
- Improvements
- Updates

CMMI – Capability Maturity Model Integration

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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. CM – SEI created to assist organizations ensure 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 has to be accomplished, and assign a team with clear goals and scope.
4. Continue until desired Maturity Level is reached.

CERT- Resilience Management Model

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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

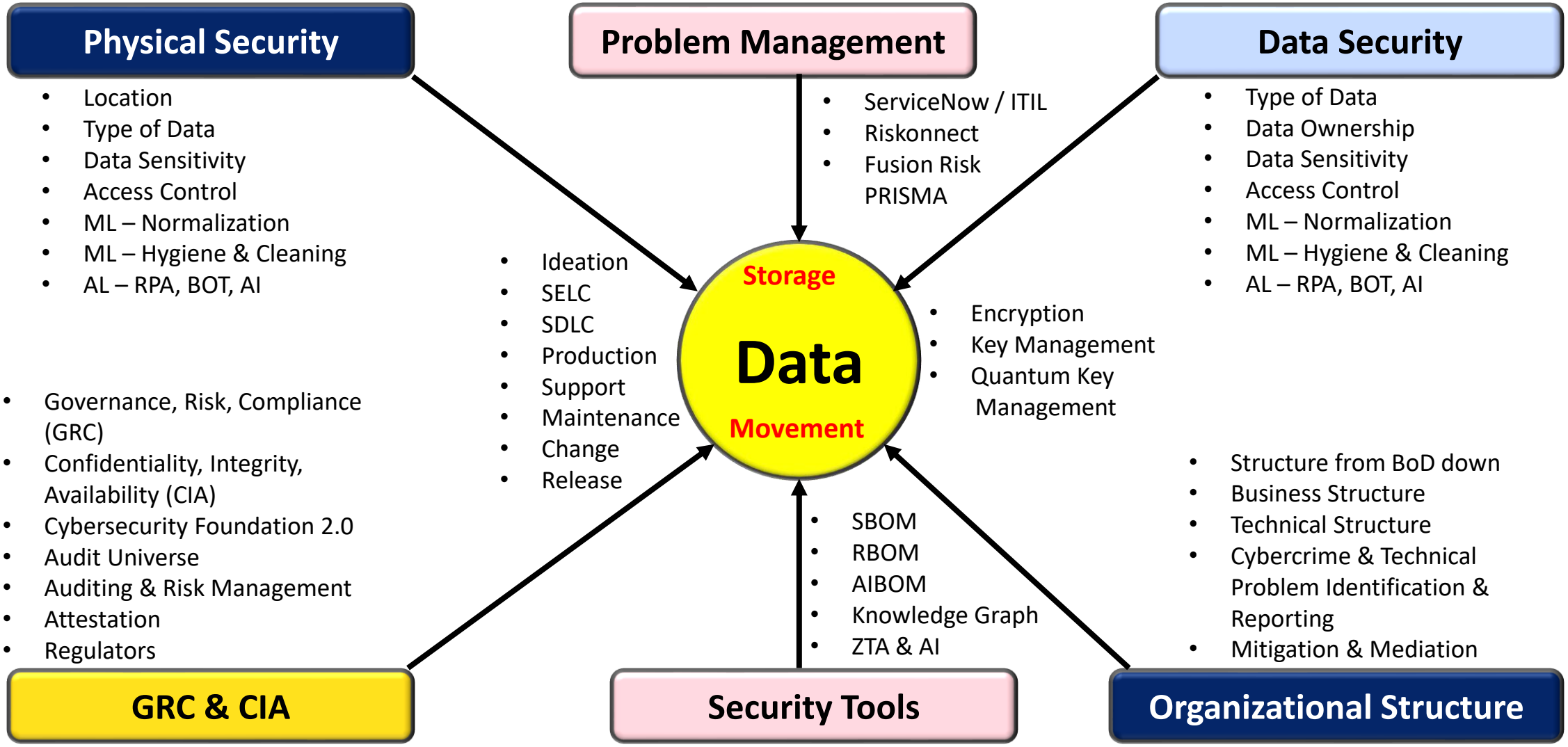
4 Categories with 26 Process Areas

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.

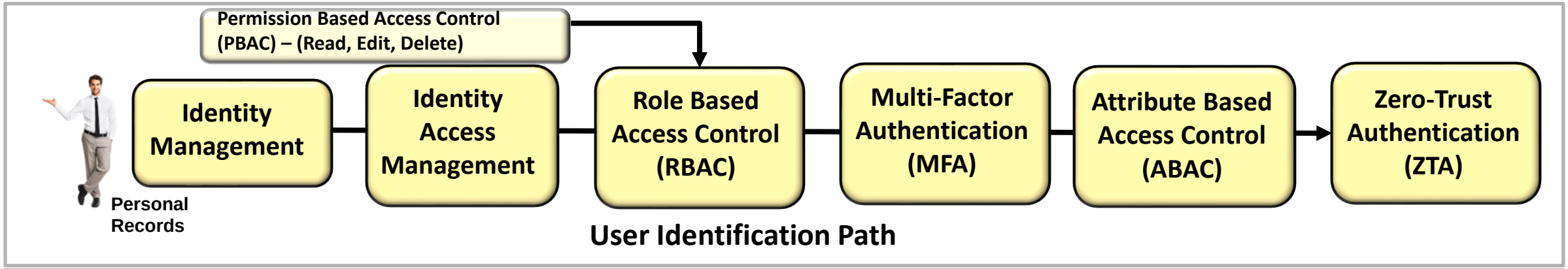
IT Security – Physical & Data

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

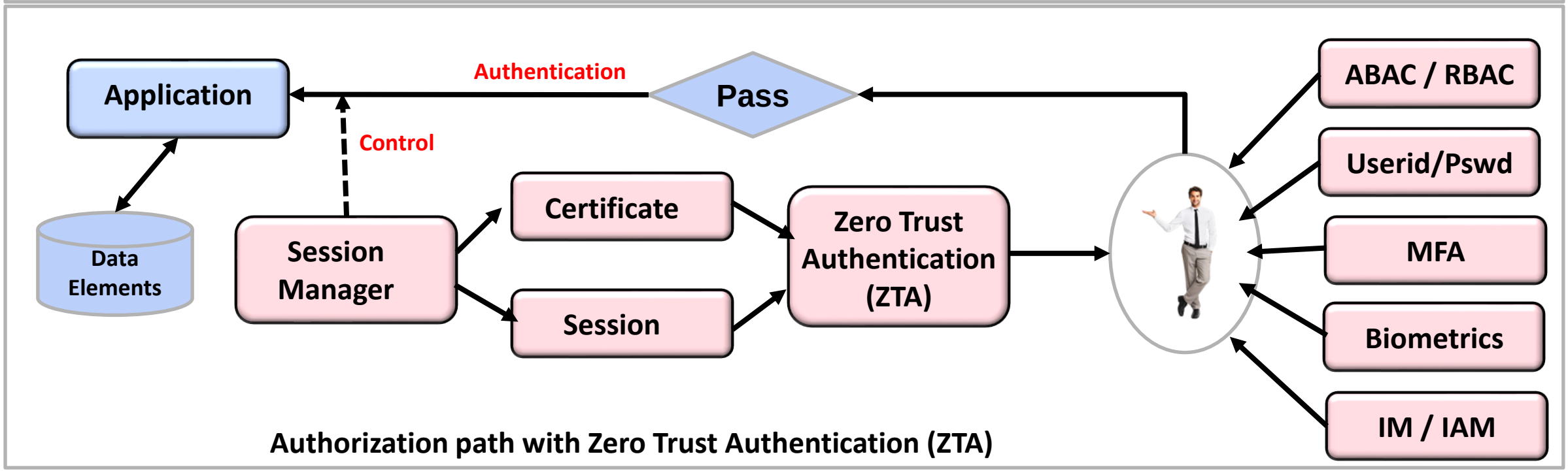


Identity and Access Management technologies

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



User Identification Path



Authorization path with Zero Trust Authentication (ZTA)

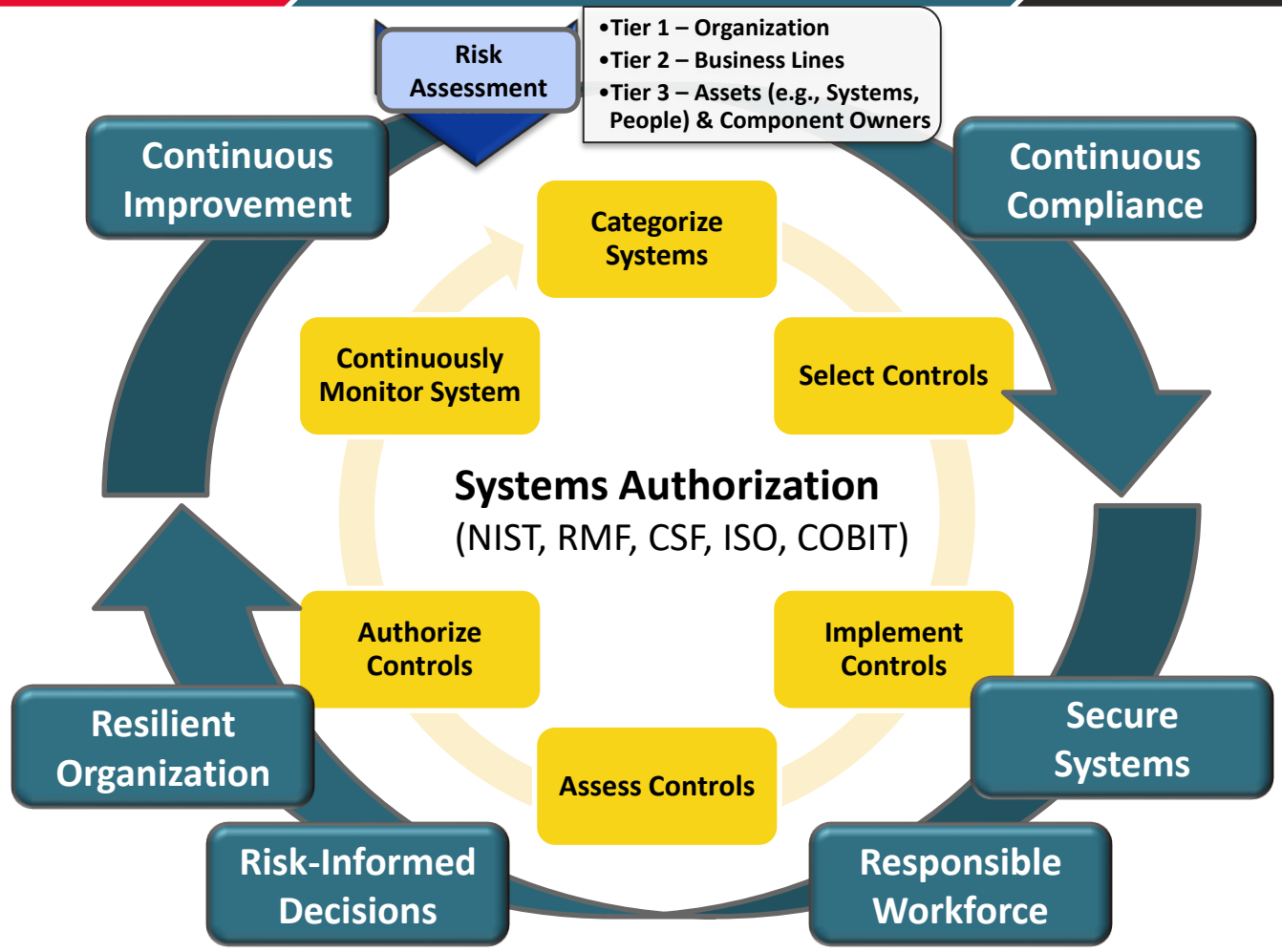
Ensuring Compliance via GRC and Risk Assessment

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Goverance

- **Statutory and Regulatory**
  - Laws
  - Statutes
  - Regulations
- **Standards**
  - ISO
  - NIST
- **Policies**
  - Organizational
  - InfoTechnology
  - InfoSecurity
- **Contracts / Commitments**
  - PCI/DSS
  - Customer Contracts
  - B2B Agreements
- **Processes & Procedure**
  - NIST, CSF, RMF
  - ISO
  - Organizational
- **Contracts**
  - Administrative
  - Physical
  - Technical

Risk



Compliance

- **Monitor**
  - Threat Landscape
  - Implemented Controls
  - Insider Behavioral Analysis
- **Self Assessment**
  - Systems
  - Practices
  - Audit Preparations
- **External Audits**
  - Regulatory Audits
  - Standards Audits (e.g., ISO)
  - Contractual Audits (e.g., PCI)
- **Reporting**
  - Internal
  - Regulatory Bodies
  - Customers

GRC and Risk Controls

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Systems Authorization (NIST, IM, IAM, RMF, CSF, RBAC, ISO, COSO, COBIT, CMMC, ITIL, ServiceNow)

- Identify People and access controls
- Categorize Systems by business needs
- Select Controls
- Implement Controls
- Assess Controls
- Continuously Monitor System

RISK ASSESSMENT

Tier 1- Organization
Tier 2 – Business Lines
Tier 3 – Assets (e.g., Systems, People)

- Secure Systems
- Responsible Workforce
- Risk-Informed Decisions
- Resilient Organization
- Continuous Improvement
- Continuous Compliance

GOVERNANCE:

Statutory / Regulatory:

- Laws
- Statutes
- Regulations

Standards:

- ISO
- NIST

Policies:

- Organizational
- InfoTechnology
- InfoSecurity

Contracts / Commits:

- PCI
- Customer Contracts
- B2B Agreements

Processes & Procedures:

- NIST, CSF, RMF
- ISO
- Organizational

Controls:

- Administrative
- Physical
- Technical

COMPLIANCE

Monitor:

- Threat Landscape
- Implemented Controls
- Inside Behavior Analysis
- Performance and Scalability
- Metrics, Thresholds, Alarms, Alerts, and Actions

Self Assessment:

- Systems
- Processes
- Audit Preparation

External Audits:

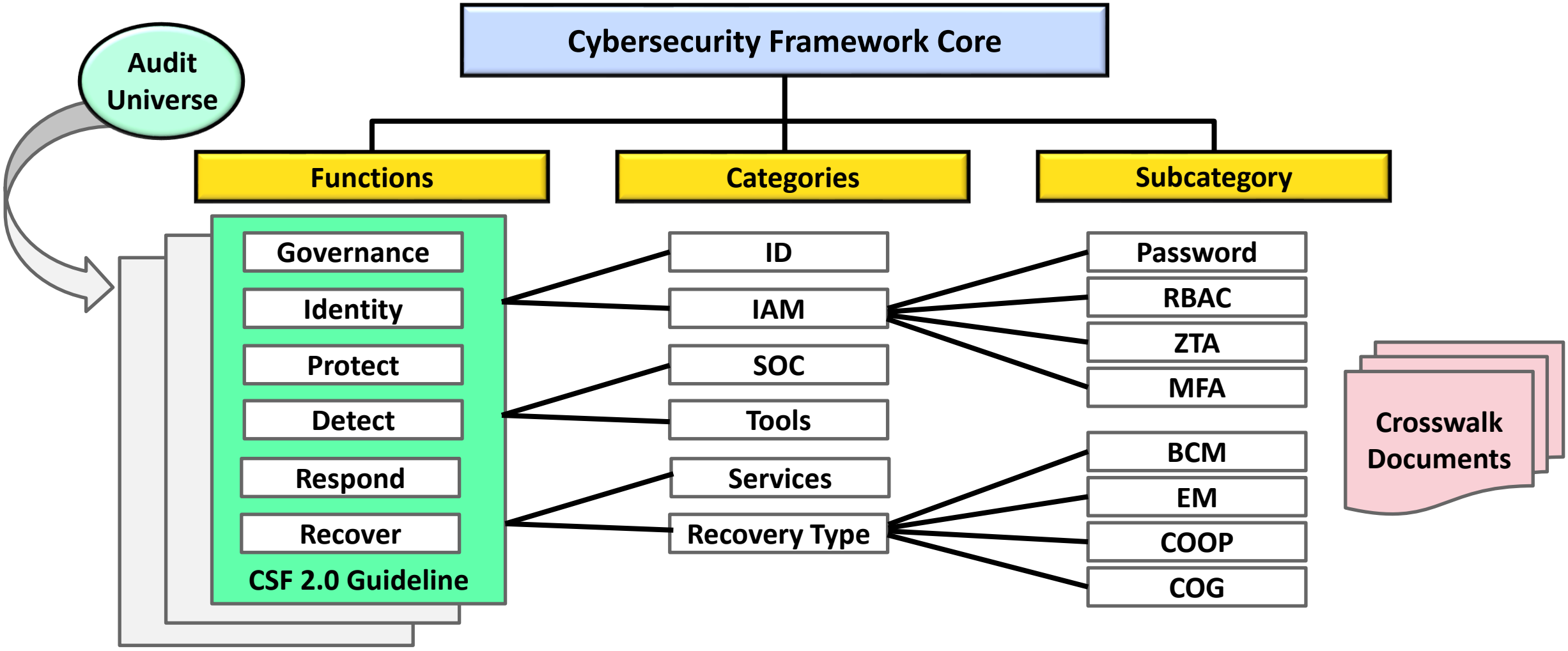
- Regulatory Audits and Attestations
- Risk Register with POA&M
- Standards Audits (e.g., ISO)
- Contractual Audits (e.g., PCI)

Reporting:

- Internal
- Regulatory Bodies
- Customers

Creating a Crosswalk Audit Document

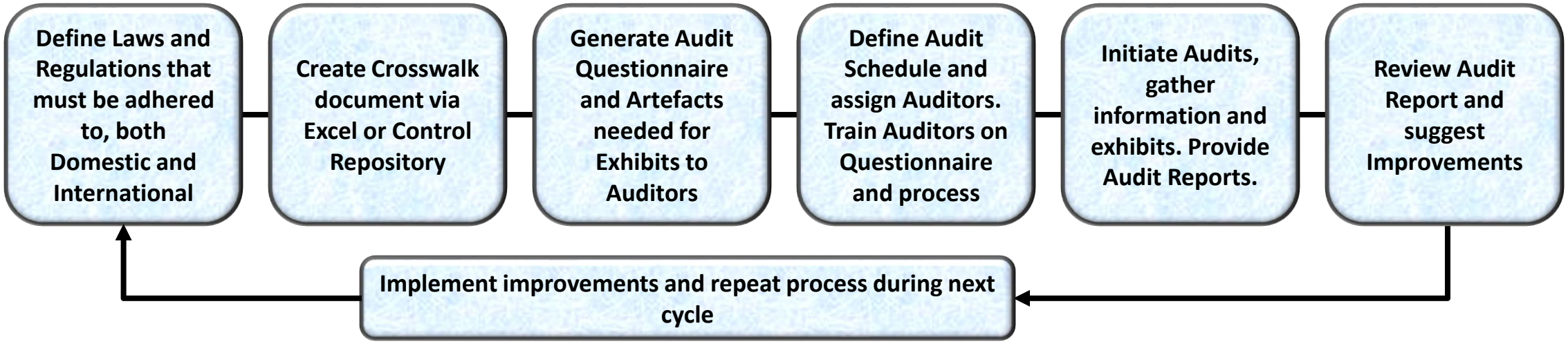
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Defining your Audit Universe and Audit Process

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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

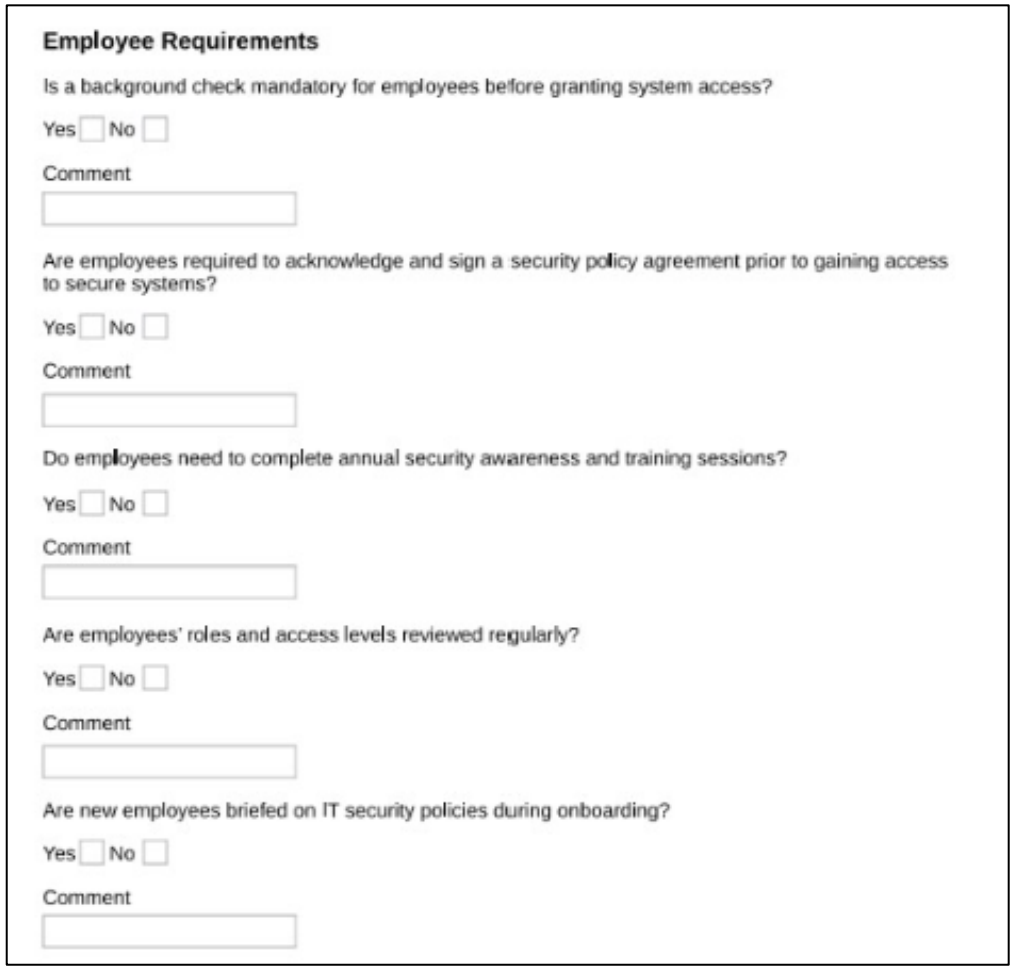


Questions associated with Enterprise Resilience

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Create Questionnaires for each of the categories listed below:

1. Employee Requirements
2. Disaster Recovery and Incident Response
3. Document Disposal
4. Backups
5. Security Protocols
6. IT Logs
7. Incident Reports
8. Outages
9. Storage and Utilization
10. Network Performance
11. Cost
12. Systems Development
13. Testing
14. Implementation
15. Anti-Virus Software
16. Network Firewall
17. Hardware
18. Passwords
19. Accounts
20. Physical Security
21. Alerts



Employee Requirements

Is a background check mandatory for employees before granting system access?

Yes ☐ No ☐

Comment

Are employees required to acknowledge and sign a security policy agreement prior to gaining access to secure systems?

Yes ☐ No ☐

Comment

Do employees need to complete annual security awareness and training sessions?

Yes ☐ No ☐

Comment

Are employees' roles and access levels reviewed regularly?

Yes ☐ No ☐

Comment

Are new employees briefed on IT security policies during onboarding?

Yes ☐ No ☐

Comment

Include these questions within the Audit Script generated from your Crosswalk and define artefacts needed to support answers for audit compliance.

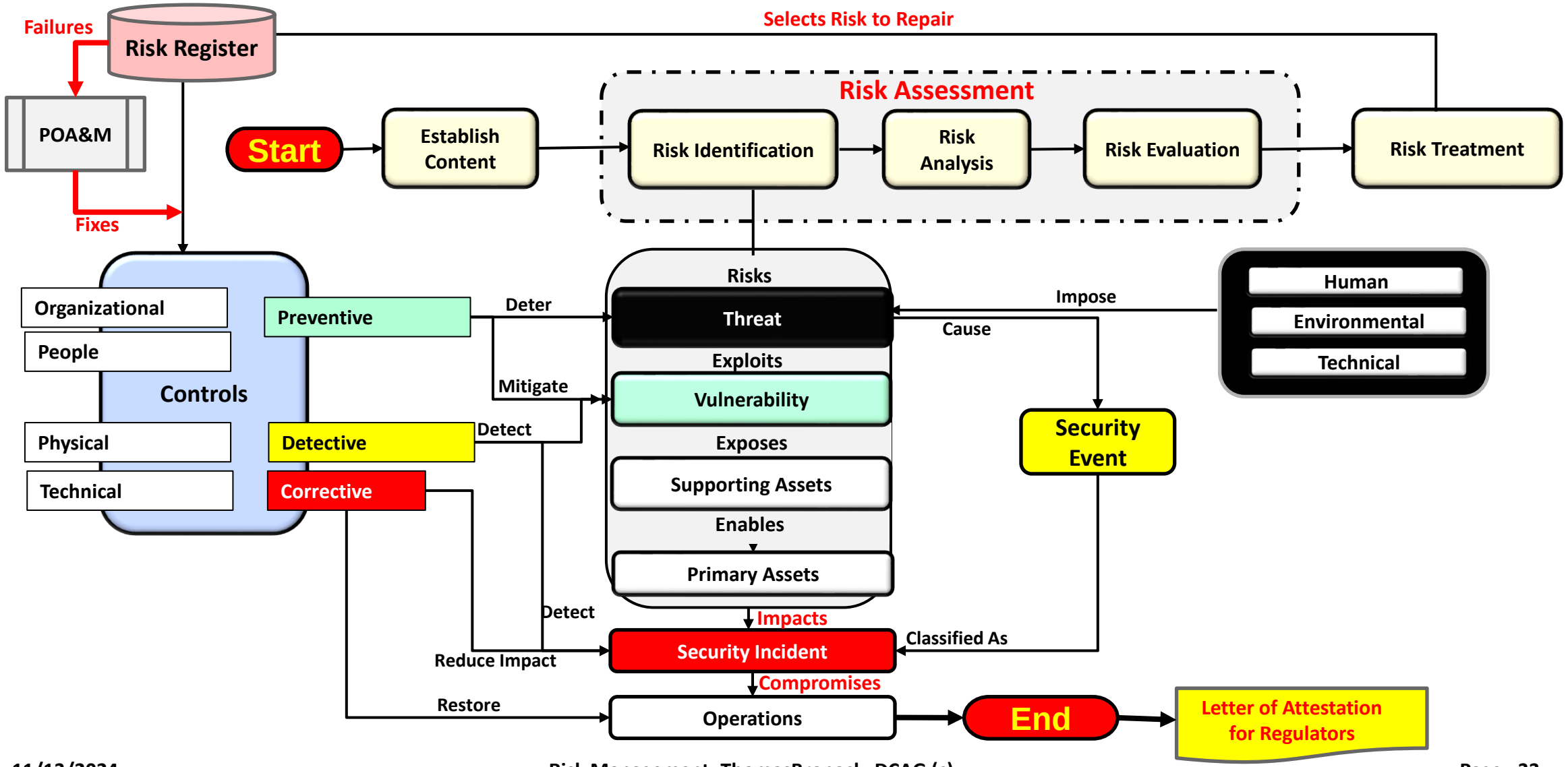
Audit Testing Vigor – Maturity Level

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Audit Testing Schedule - Risk Vigor			
Cost Level:	**Low Rigor:**	**Medium Vigor:**	**High Vigor:**
High ($$$)	Manual Self-Correcting Control Adjustments	Comprehensive External Audits	Advanced (Specialized) External Audit
			Real-Time Sutomated Monitoring
		Semi-Automated Self-Correcting Controls	AI-Driven Detection
			Fully Automated Self-Correcting Controls
Medium ($$)	Automated Risk Control Self Assessment (RCSA)	Regular Internal Audit	Comprehensive Internal Audit (Utilizing Cyber / IT Specialists)
		Regular Line 1 Controls Testing	Quarterly Line 3 Audit
		Bi-Annual Level 3 Audit	
		Periodic Automated Monitoring	
Low ($)	Annual CSA	Bi-Annual CSA	Quarterly CSA
		Bi-Annual RCSA	Quarterly RCSA
	Basic Line 1 Controls Checks	Manual Continuous Monitoring Checks	Monthly Manual Continuous Monitoring Checks
	Attestation	Periodic Attestations	

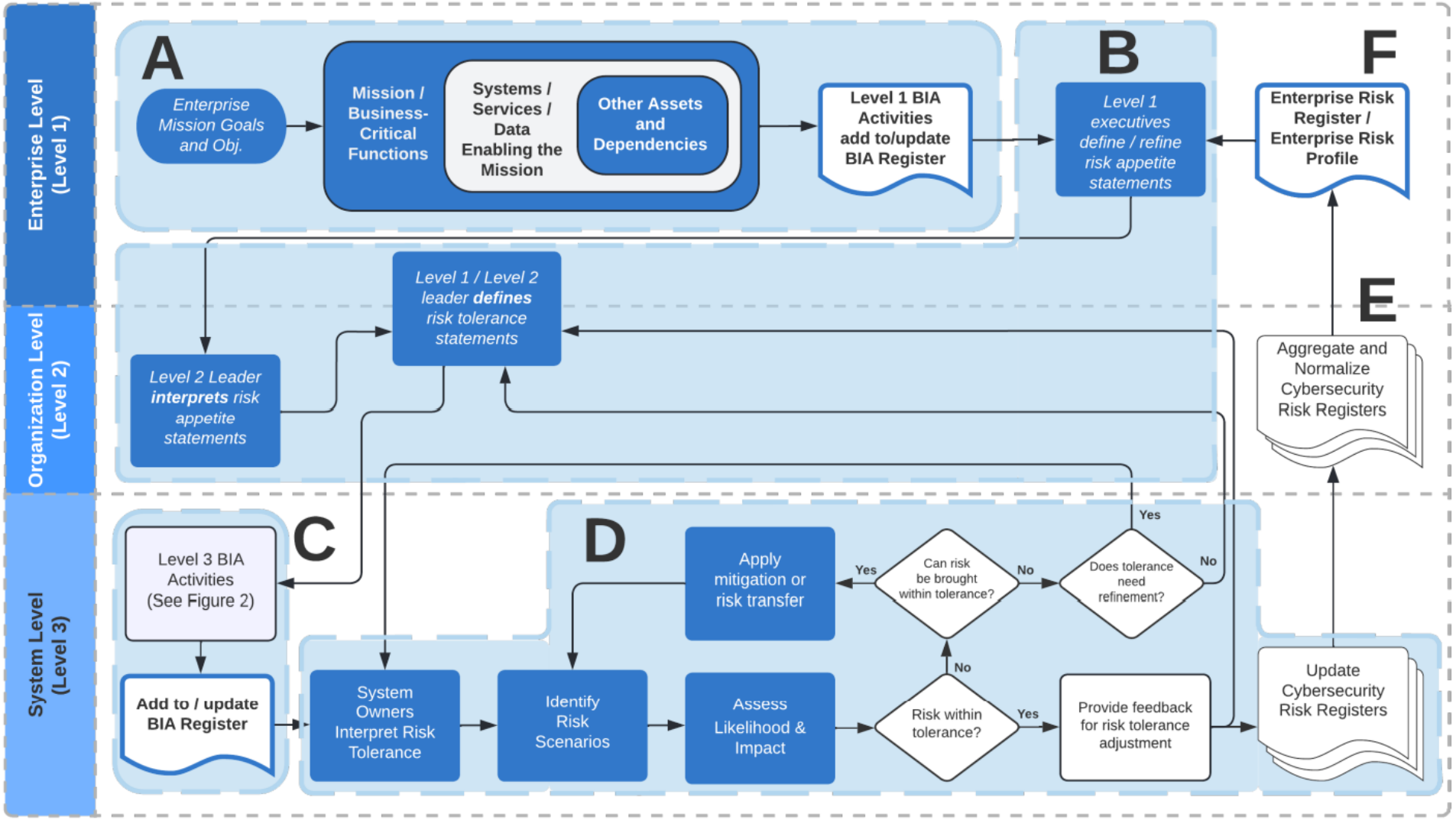
Risk Management with ISO 27000: 2022

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Business Impact Analysis – BIA (NIST SP 800-34, and NIST IR 8286d))

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Link to Document

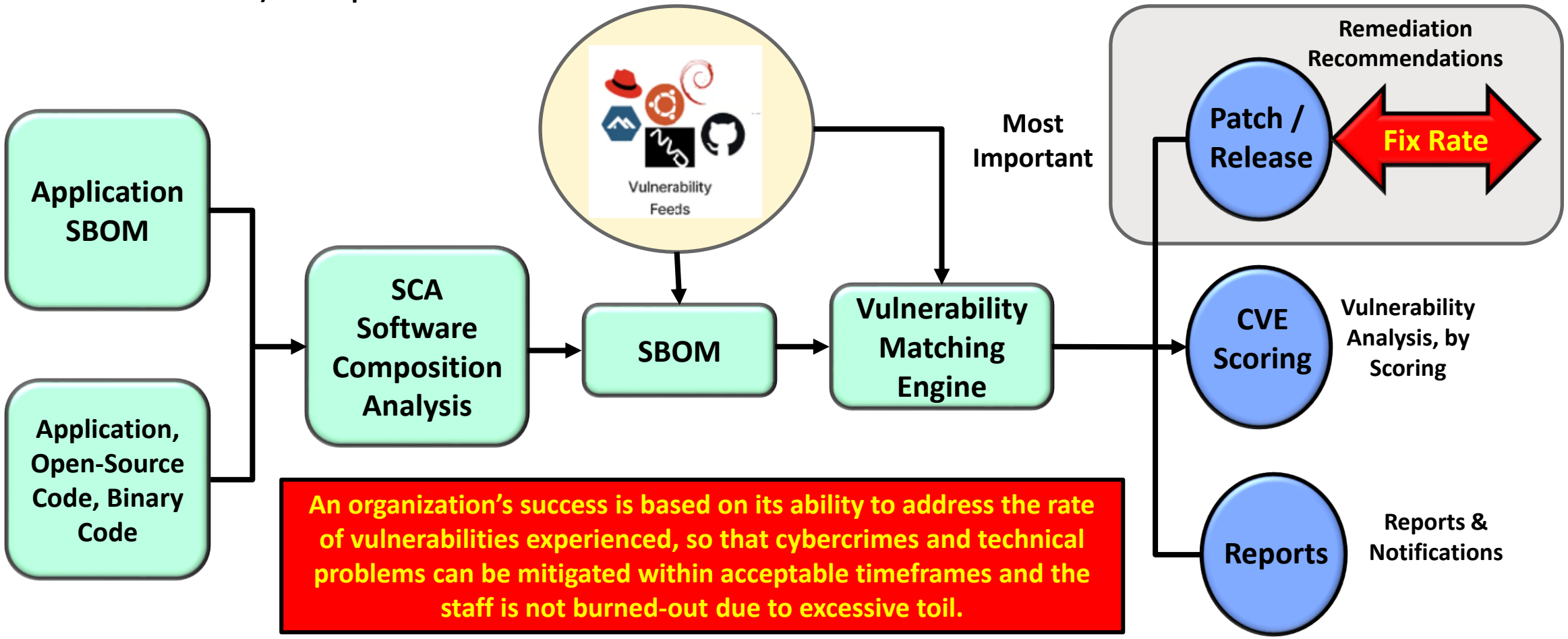
A. Define Goals
B. Risk Appetite
C. BIA Activities
D. Identify Risks
E. Normalize Risks
F. Risk Register with POA&M
G. RTO / RPO
H. Feeds (Upstream / Downstream)
I. Recovery Group
J. Executive Decision Window & Activities
K. Recovery Time Window & Activities

Identifying and Reporting Vulnerabilities

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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

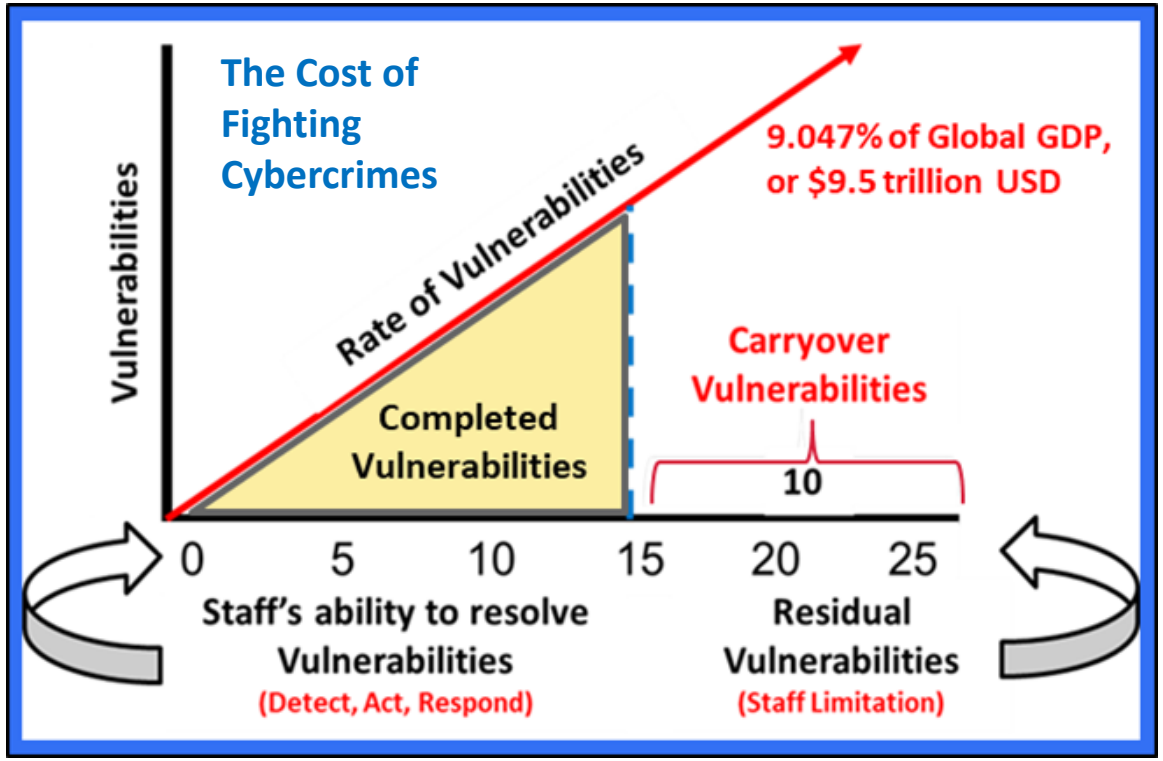
The Fix Rate associated with vulnerability repairs (Patch or New Release) should be equal to or higher than the rate of Vulnerability detection.



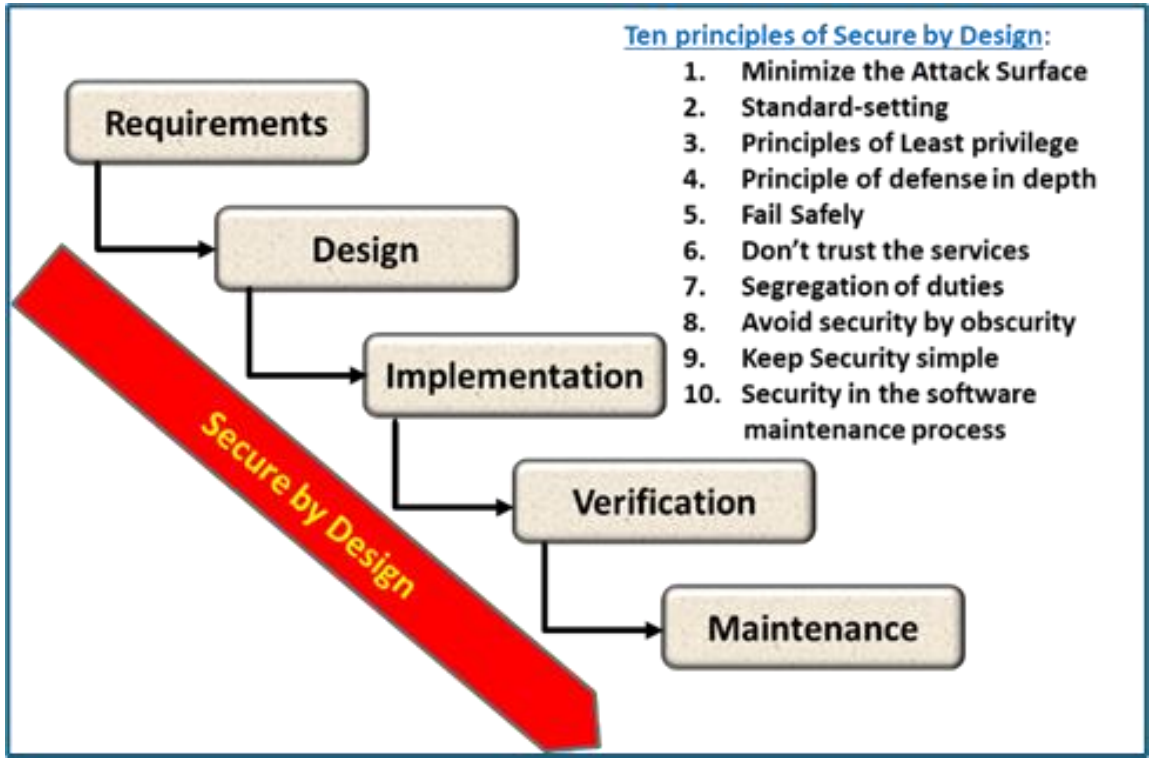
An organization's success is based on its ability to address the rate of vulnerabilities experienced, so that cybercrimes and technical problems can be mitigated within acceptable timeframes and the staff is not burned-out due to excessive toil.

Fighting Cybercrime Costs with Secure by Design

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



The **current cost of fighting cybercrimes** and technology threats is estimated at $9.5 Trillion within the United States and 10.24 % of Global GDP. Improving the vulnerability fix rate will greatly reduce costs and improve business service continuity and resilience.



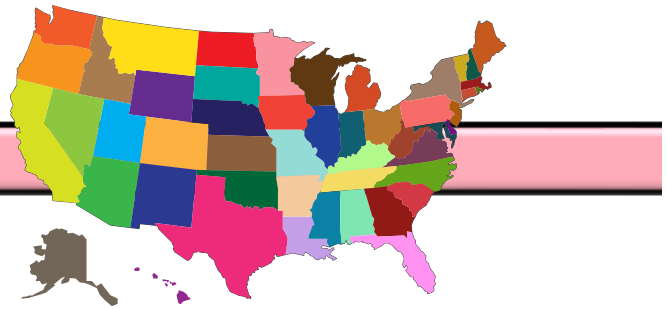
The government has developed a "**Whole of Nation**" approach to combating these costs through the "**Secure by Design**" methodology developed by DHS/CISA to safeguard Government, Business, Infrastructure, and Utilities .

A Whole of World approach to Cybersecurity

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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.

Vulnerability Management definition and process

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Vulnerability management is a **continuous, proactive, and often automated process** that keeps your computer systems, networks, and enterprise applications safe from cyberattacks and data breaches. As such, it is an important part of an overall security program.

Process:

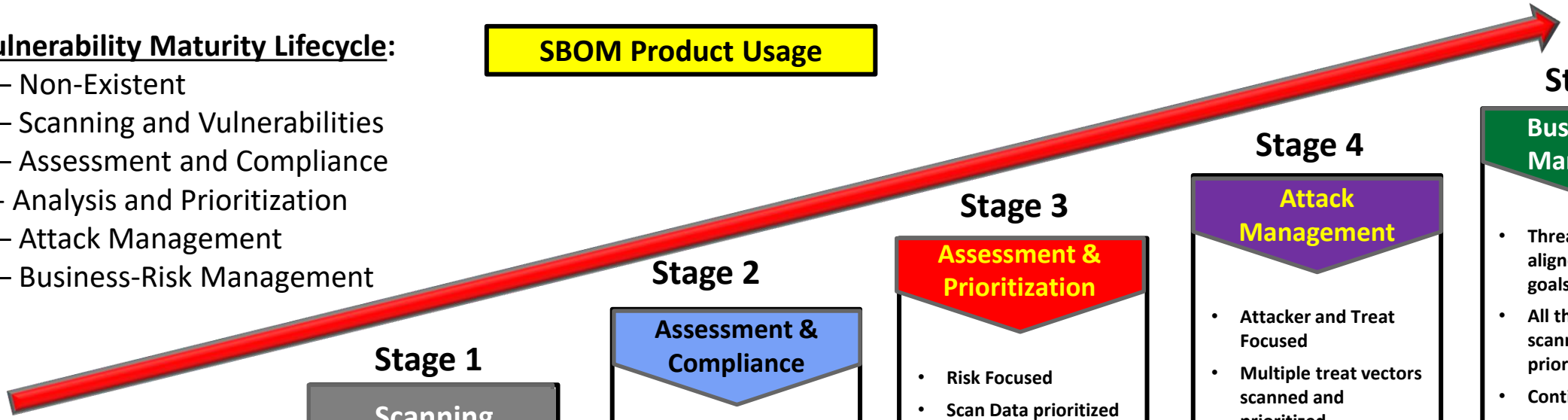
- **Plan** how to use Vulnerability Management
- **Discover** where your vulnerabilities exist
  - Vulnerability-Free Production Applications
  - Continuous Scanning for new Vulnerabilities impacting production applications via Continuous Threat Exploitation Management (CTEM)
- **Scan** applications with SBOMs (Software Bill of Materials)
- **Report** vulnerabilities, their symptoms, and mitigations via patches and new releases
- **Deploy** patches and new releases to mitigate vulnerabilities

Vulnerability Management Maturity Lifecycle

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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

SBOM Product Usage



Stage 0
Non-Existent
- No vulnerability Scanning
- Manual Vulnerability Assessments
- Haphazard Patching
- No processes / metrics

Needs Analysis

Stage 1
Scanning
- Vulnerability Assessment Solution in place/ metrics
- Ad-Hoc Vulnerability Scanning
- Basic Patching, Processes, and Metrics identified

Proof of Concept

Stage 2
Assessment & Compliance
- Driven by Regulatory Framework
- Scheduled Vulnerability Scanning
- Scan to Patch Lifecycle
- Emergency Processes
- Little measurability, metrics need to be developed and monitored
- GRC adherence

Contract

Stage 3
Assessment & Prioritization
- Risk Focused
- Scan Data prioritized through analytics
- Vulnerability Scoring
- Patching is Data Driven by priority
- Measurable Processes
- Emerging metrics and trends detected and reported
- Extended protect and reduction in vulnerability workload

Tailoring

Stage 4
Attack Management
- Attacker and Treat Focused
- Multiple treat vectors scanned and prioritized
- Pathing bases on risk to critical assets
- Efficient metrics-based processes
- Threat driven metrics and trends
- Protection over vulnerabilities, network, and endpoints achieved

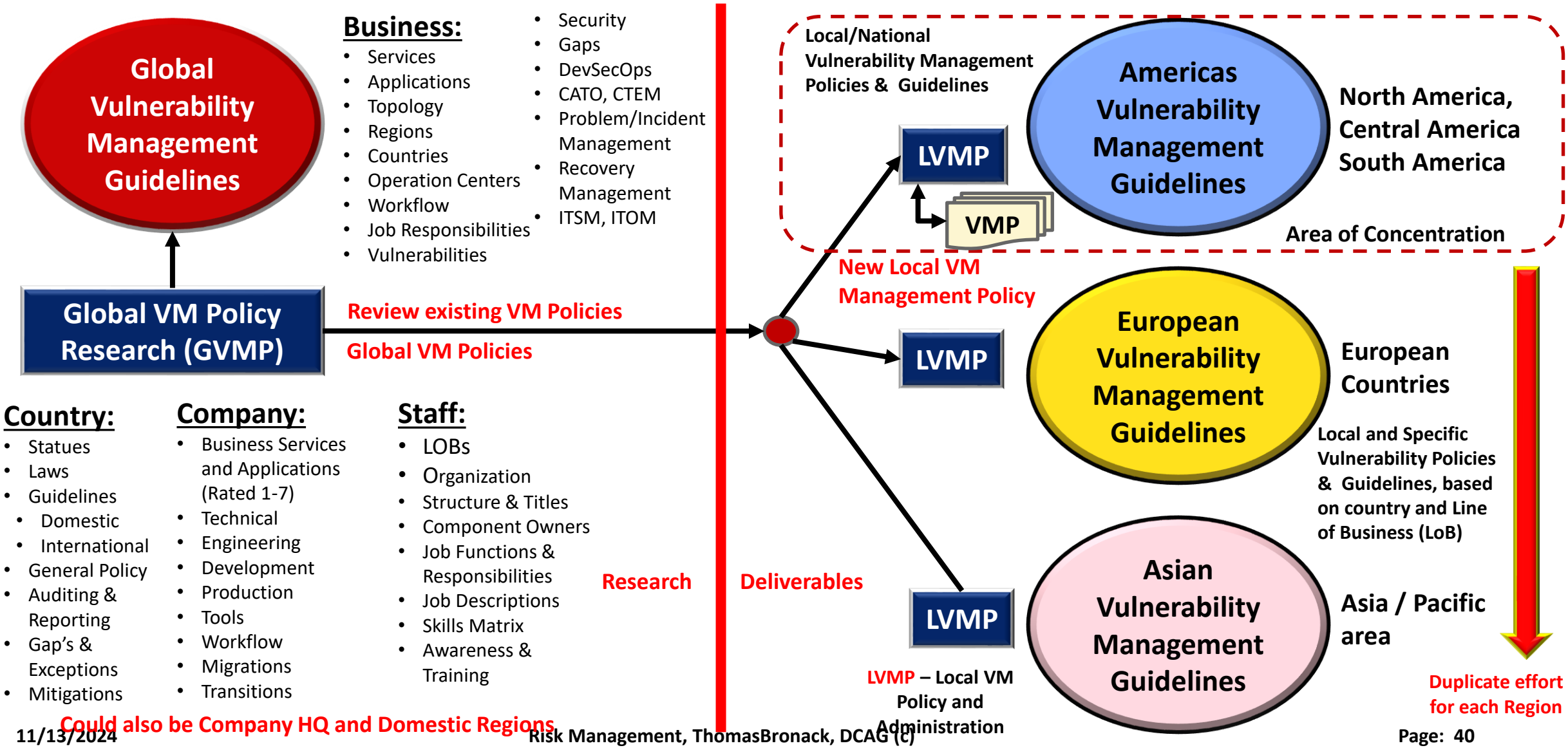
Integration

Stage 5
Business-Risk Management
- Threat and Risk aligned with business goals
- All threat vectors scanned and prioritized
- Continuous patching
- Unified business and IT processes
- Measurement integrated to enterprise risk
- Executive Dashboard for organizational and continuity of services
- Documentation, Awareness and Training

Fully Deployed

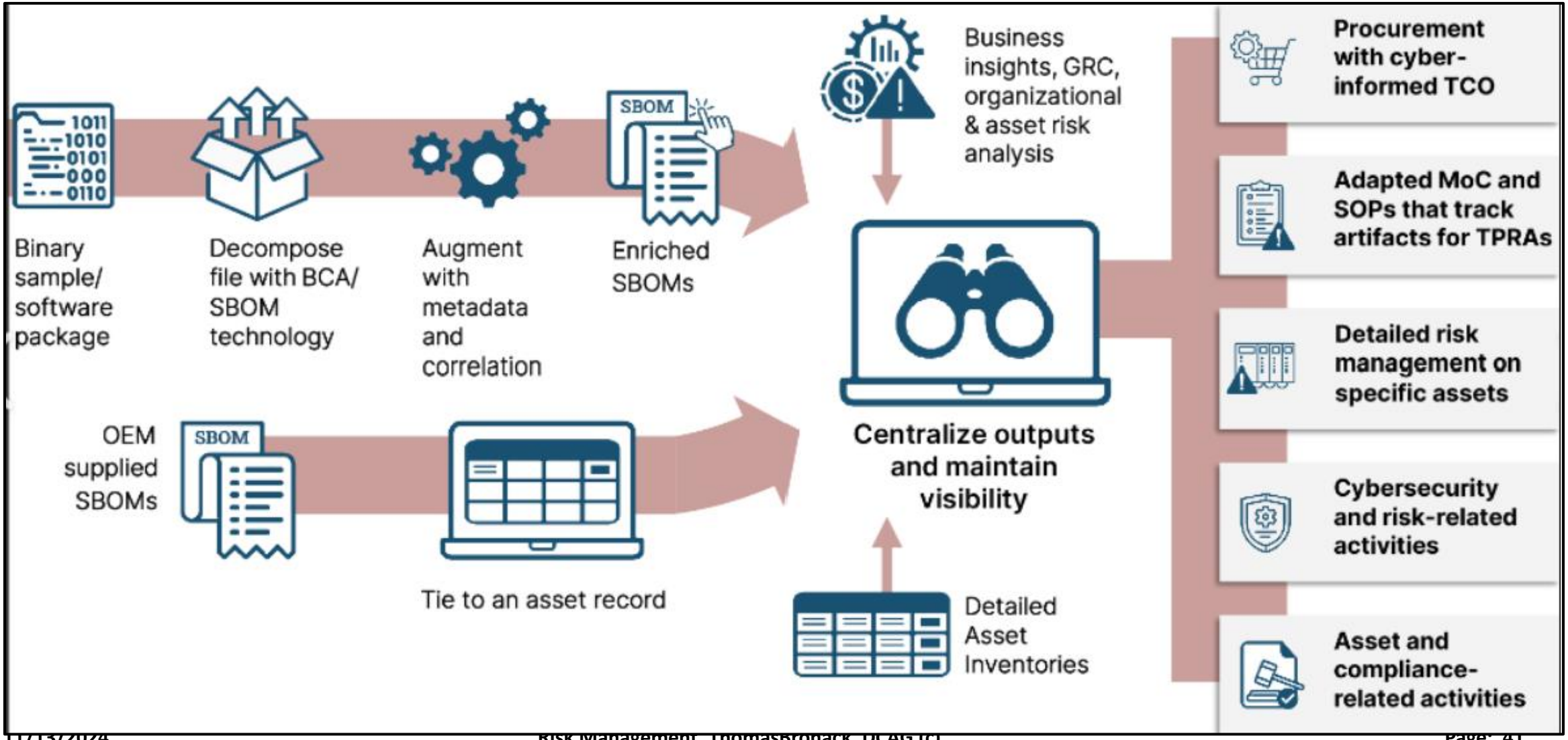
Global Vulnerability Management Policy generation

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



How SBOMs are created and their benefits

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Scaling SBOM, RBOM, and AIBOM Operationalization

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Training and Awareness Process Definition

- SBOM, RBOM, and AIBOM understanding
- Applicable Regulations
- Vulnerability Management
- Requirements and Use Cases
- Policies and Guidelines
- Contract and processes for vendor SBOM, RBO, AIBOM collection
- Internal training

SBOM, RBOM, AIBOM Creation / Collection

- SBOM, RBOM, AIBOM generation through build process and pipeline
- Data Collection from vendors
- Post-production SBOM, RBOM, AIBOM generation through Binary Composition Analysis (BCA)
- SBOM, RBOM, AIBOM inventory (secure asset management)

SBOM, RBOM, AIBOM Management & Compliance

- SBOM, RBOM, AIBOM accuracy and compliance
- Coverage of assets
- License Management
- Vulnerability detection
- Integrate with Incident Response process
- Version Control and auditability

SBOM, RBOM, AIBOM Monitoring & Vulnerability Management

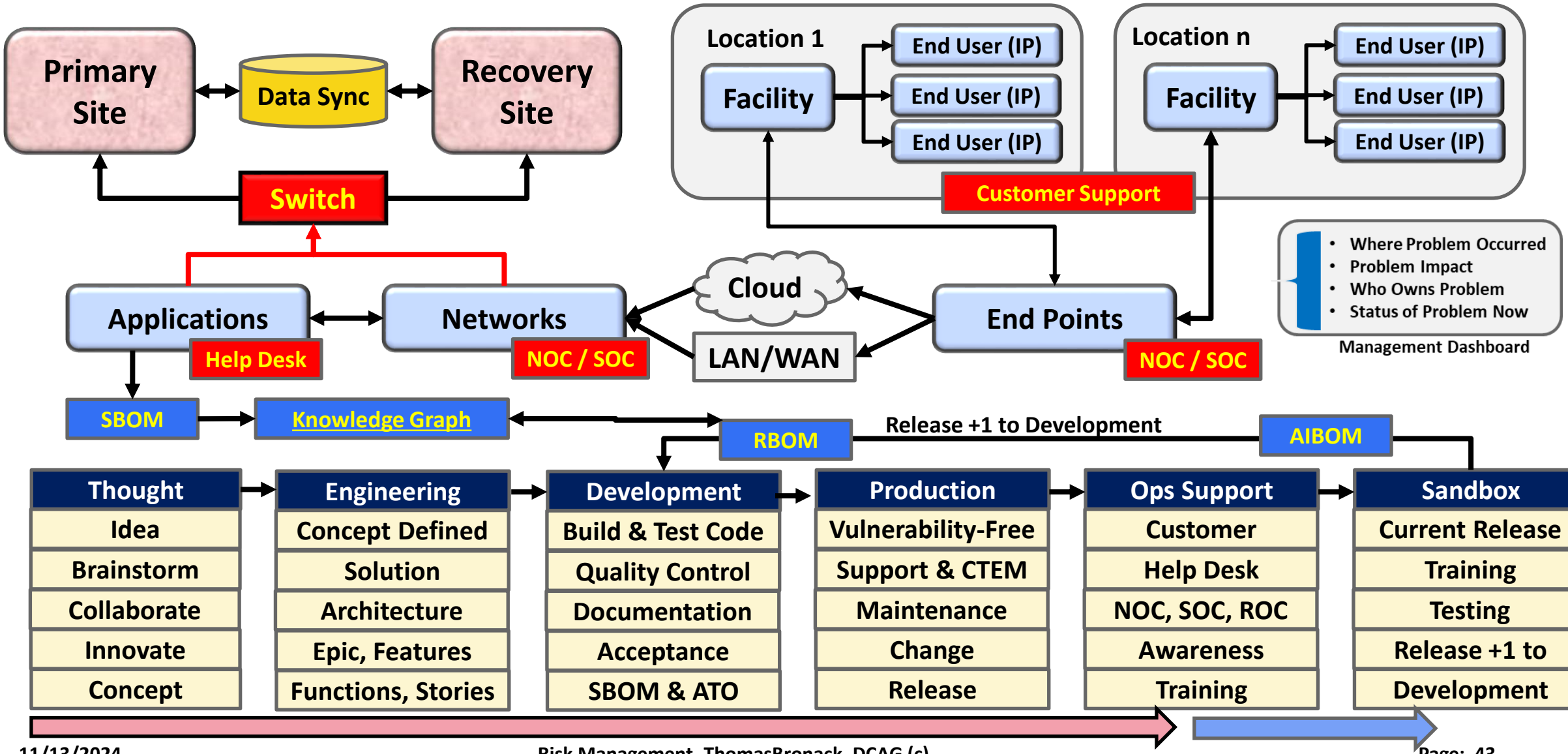
- VEX integration
- Alerts and automated workflows
- OSS usage and risk management
- SBOM, RBOM, AIBOM completeness and additional use cases support
- Software provenance and risk assessment for 3rd party components

Process Optimization

- Automation of policies (policy as code) for supply chain risks
- Real-time monitoring
- Integration with threat intelligence and predictive analysis
- Supply chain security incorporation into software acquisition process
- Continuous improvement and auditing

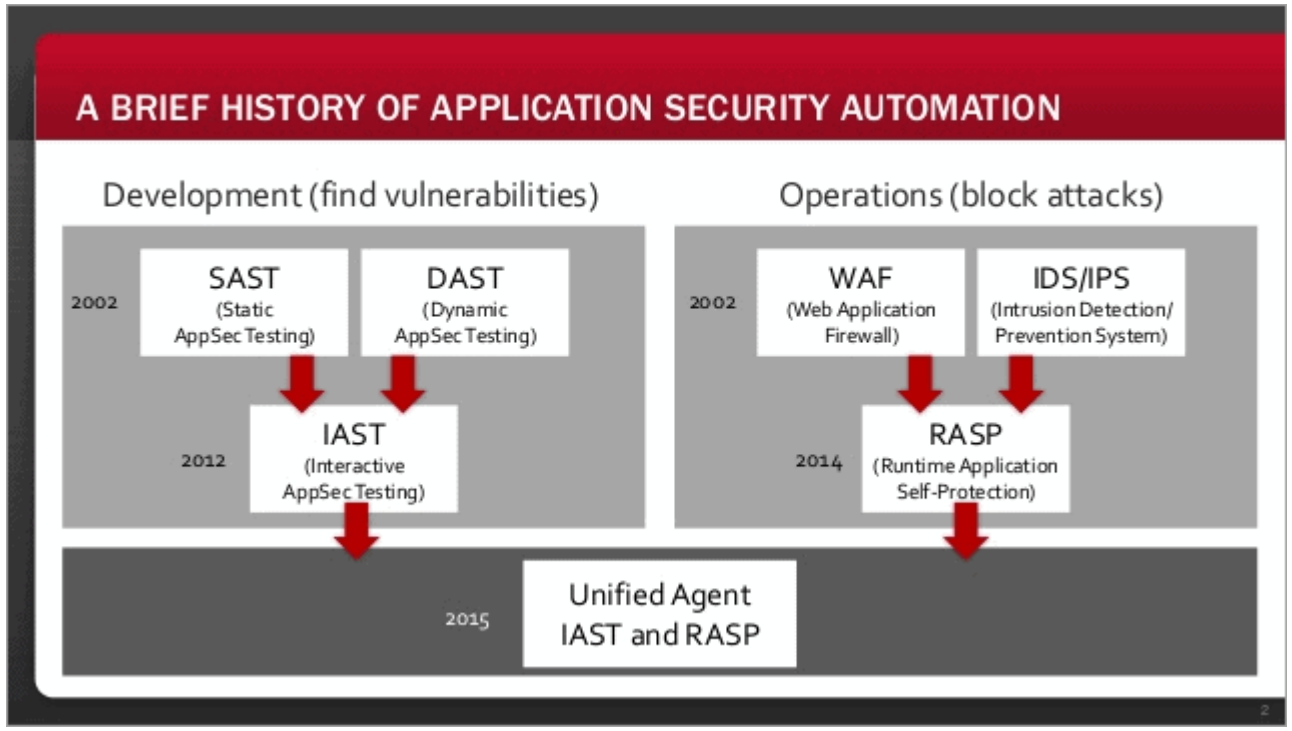
From Idea to Product, with Support and Recovery

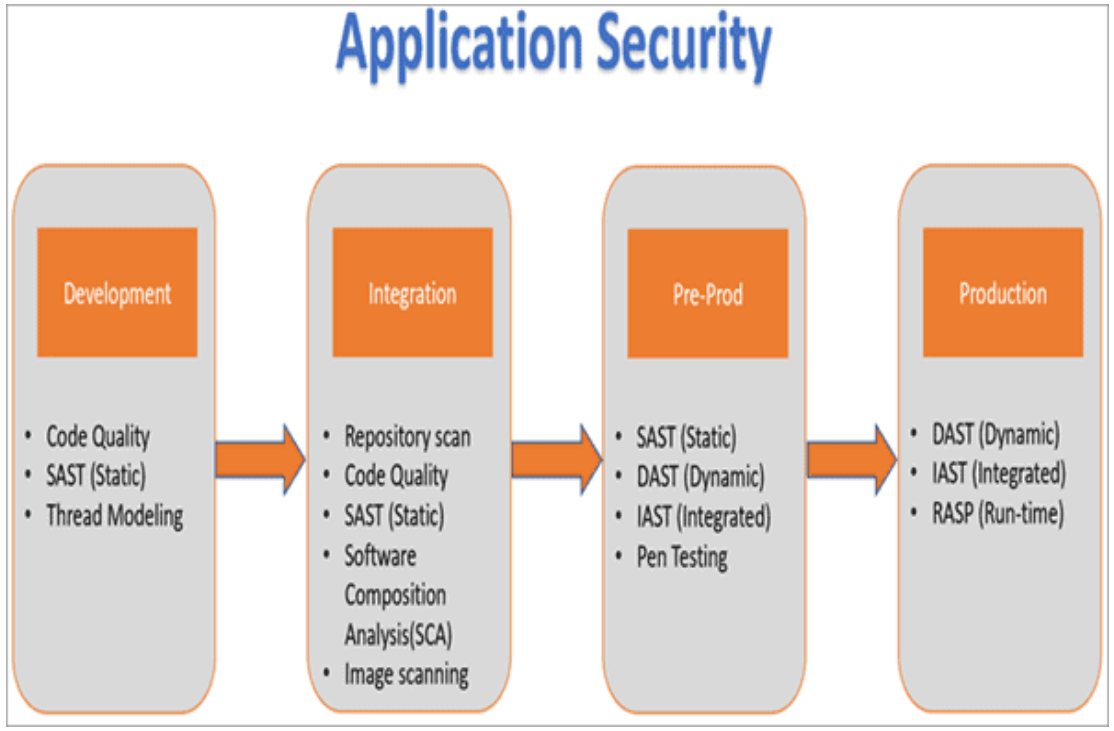
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Application Security Testing – Dev/Sec/Ops

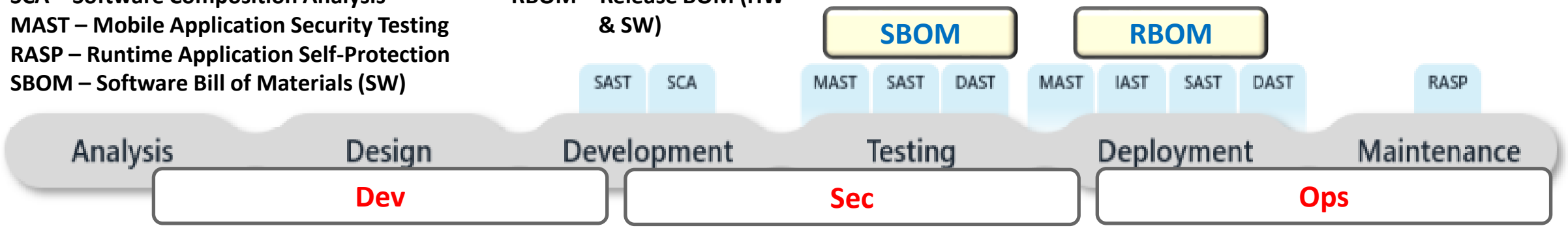
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992





SCA – Software Composition Analysis
MAST – Mobile Application Security Testing
RASP – Runtime Application Self-Protection
SBOM – Software Bill of Materials (SW)

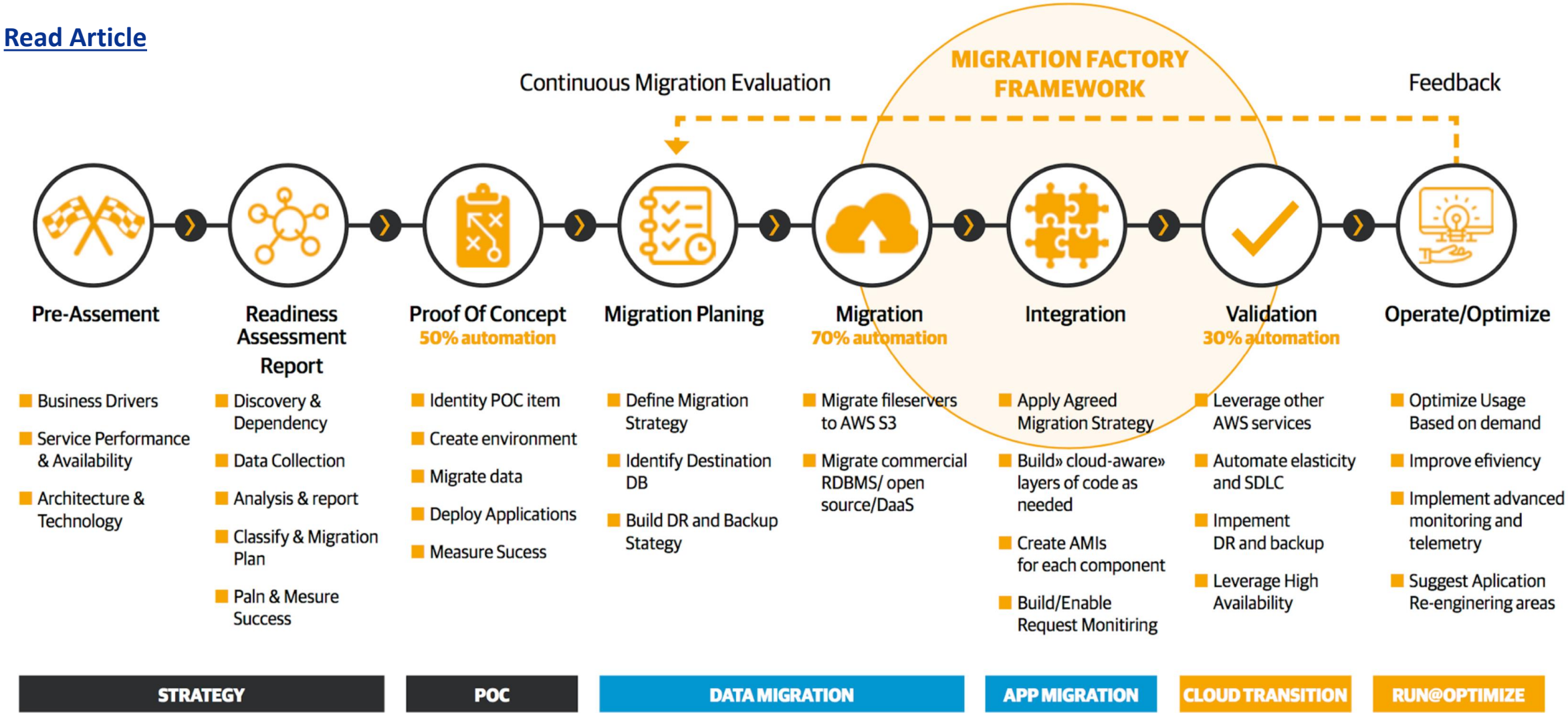
RBOM – Release BOM (HW & SW)



Using AI Planning for Migrating Applications to AWS Cloud

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Read Article



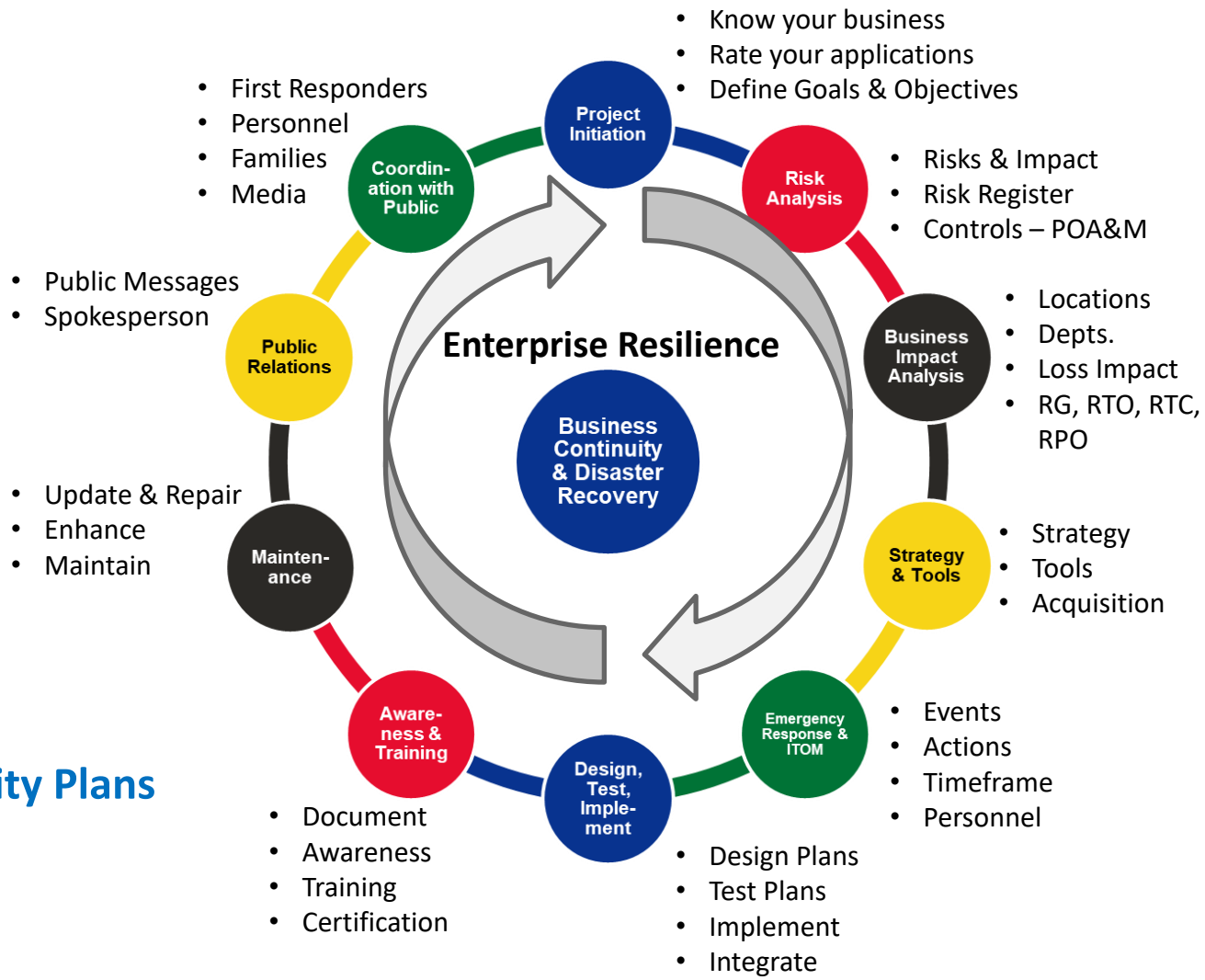
Ten Step Process to establish BCM/DR Practice

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

1. Project Initiation and Management
2. Risk Evaluation and Controls Improvement
3. Business Impact Analysis
4. Developing Business Continuity Strategies
5. Emergency Response and Operations

   Restoration (Backup, Vaulting, Restoration)
6. Designing and Implementing Business

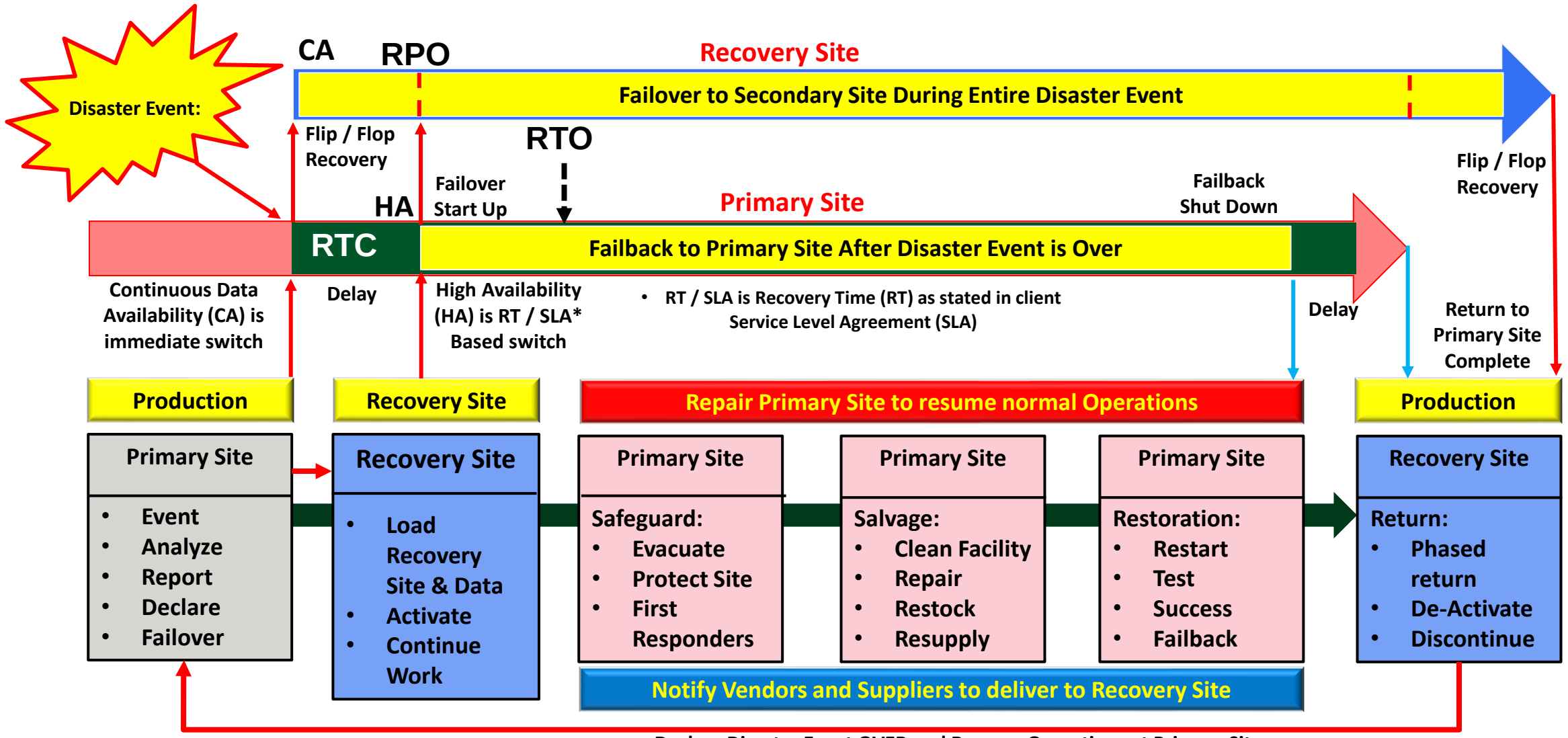
   Continuity Plans
7. Awareness and Training
8. Maintaining and Exercising Business Continuity Plans
9. Public Relations and Crisis Communications
10. Coordinating with Public Authorities



The Disaster Event Life Cycle

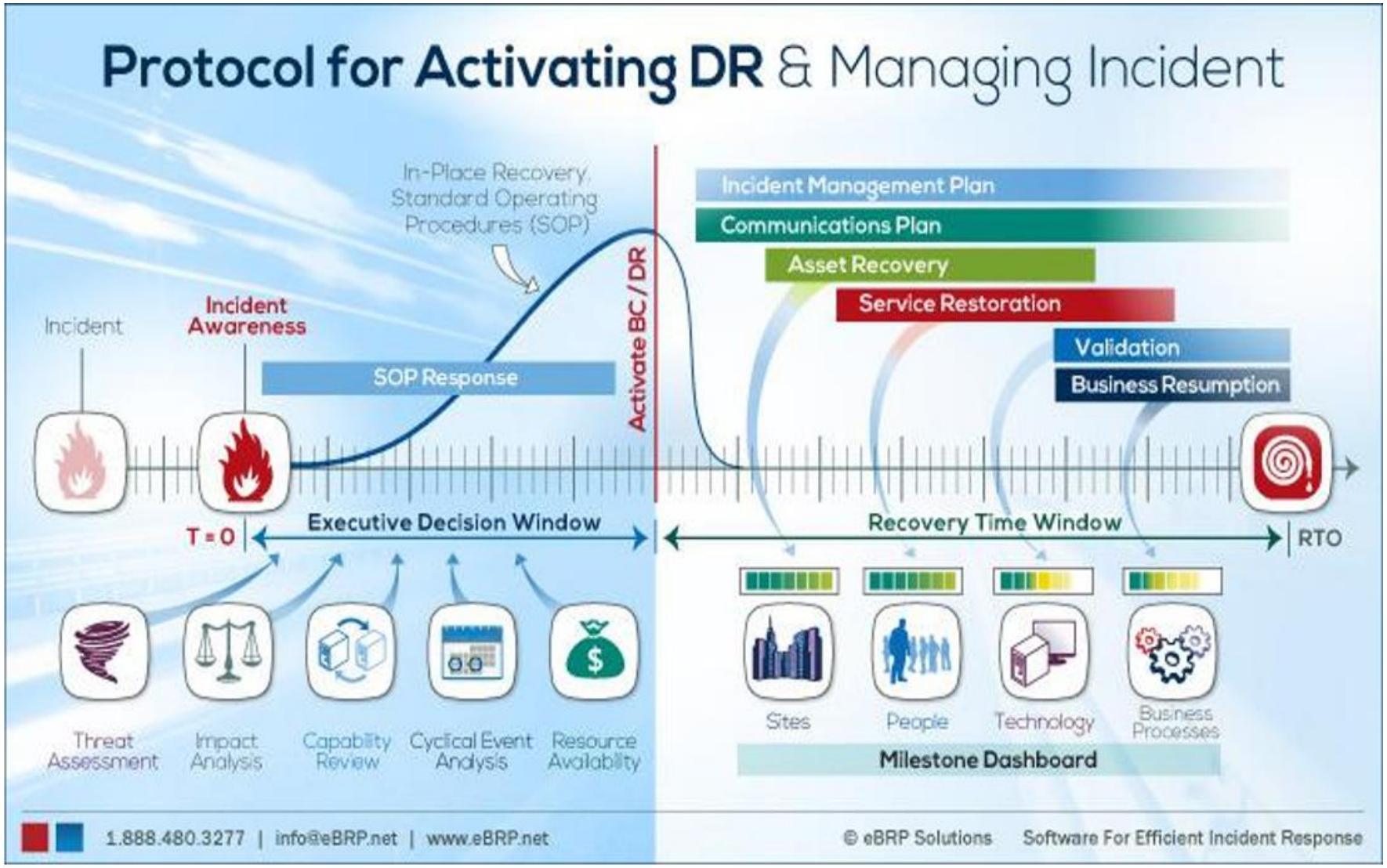
CA is Continuous Availability
HA is High Availability
RTO – Recovery Time Objective
RPO – Recovery Point Objective
RTC – Recovery Time Capability

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



The Business Recovery Life Cycle

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

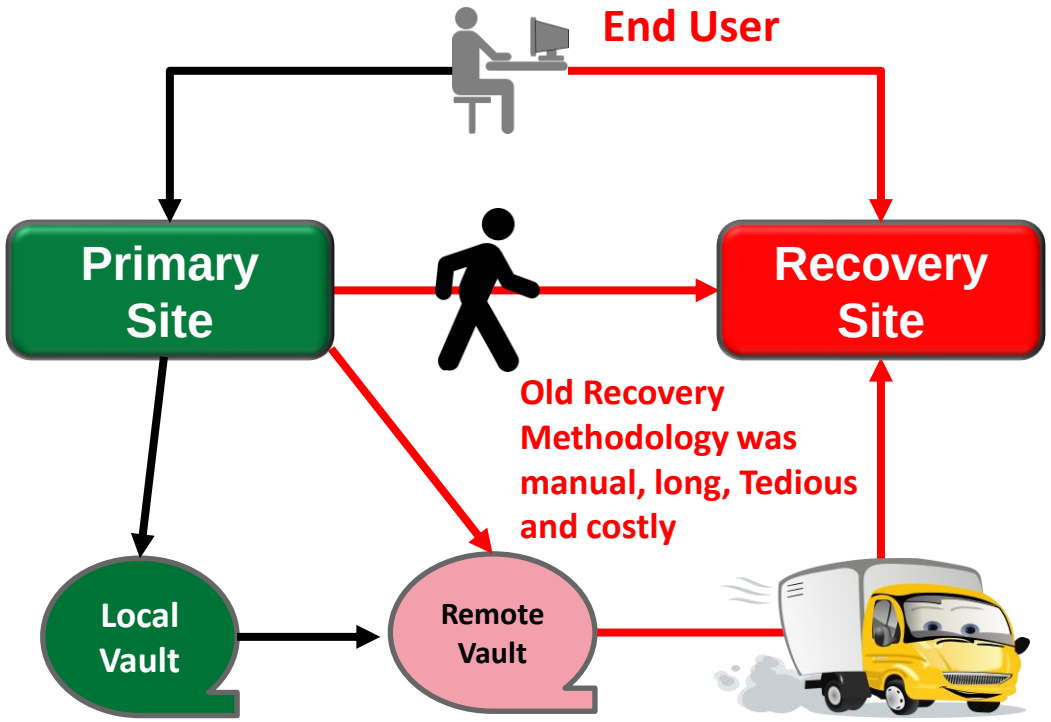


DR Life Cycle:

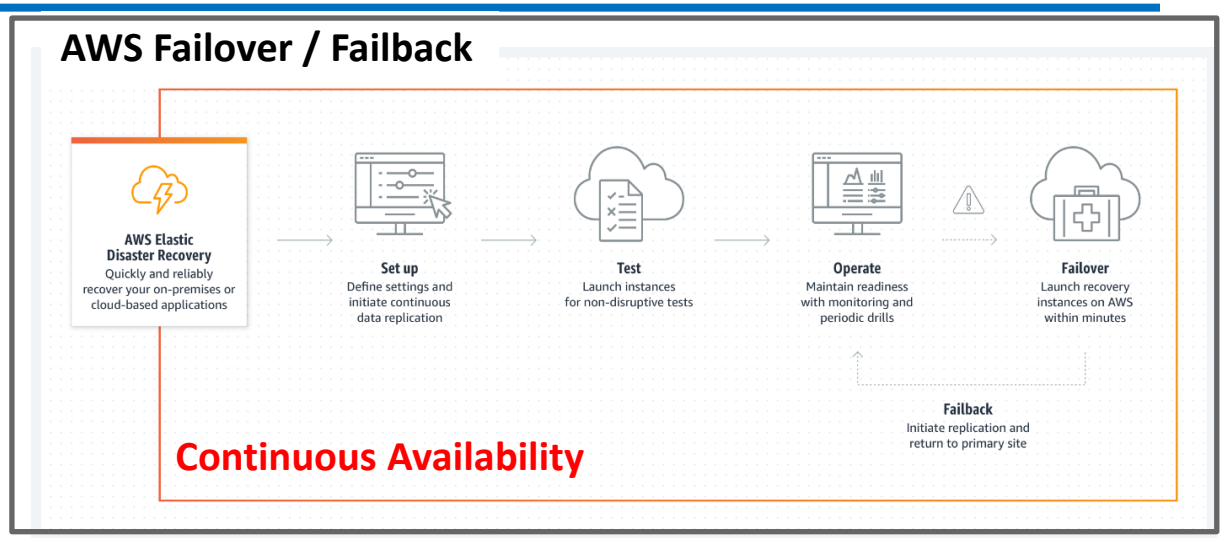
1. **Executive Decision Window**
   a. Incident occurs
   b. Incident awareness (RPO)
   c. Threat Assessment
   d. Impact Analysis
   e. Capability Review
   f. Cyclical Event Analysis
   g. Resource Availability
   h. SOP Response
   i. Activate BC/DR Plan
2. **Recovery Time Window**
   a. Incident Management
   b. Communications
   c. Asset Recovery
   d. Service Restoration
   e. Validation
   f. Business Resumption (RTO)
3. **Milestones Dashboard**
   a. Sites (Primary / Recovery)
   b. People
   c. Technology
   d. Business Processes

Evolution of Recovery Management

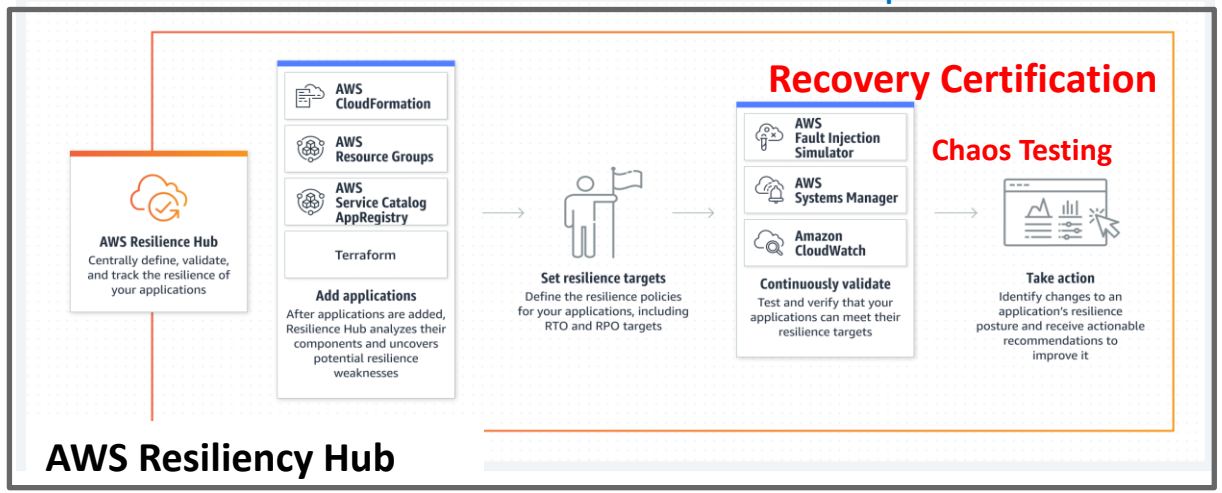
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



1. Primary Site sends backups to local and remote vaults
2. Primary Site Fails
3. Disaster Declared ($)
4. Tapes moved from vault to Recovery Site
5. People moved to recovery site
6. Configure Systems & Networks
7. Load Data & Applications
8. Initiation Recovery Operations
9. Connect Users
10. Initiate Production Operations
11. Reverse process when disaster event is over
12. Duration can be in days, but certainly hours

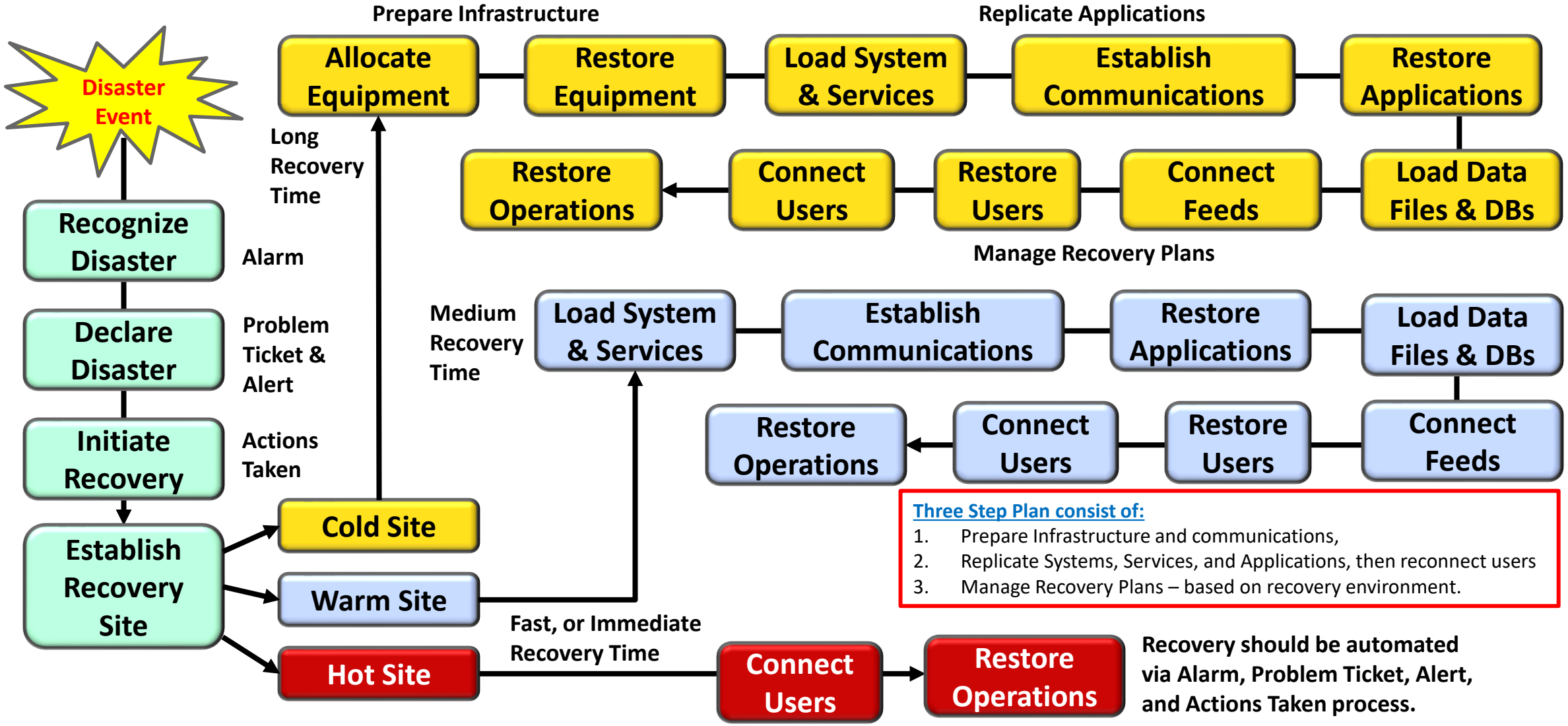


The new Recovery Methodology is quick & automated via Failover / Failback. CloudWatch performs Health Checks, and the Resilience Hub allows for Failover / Failback and continuous validation without disruption



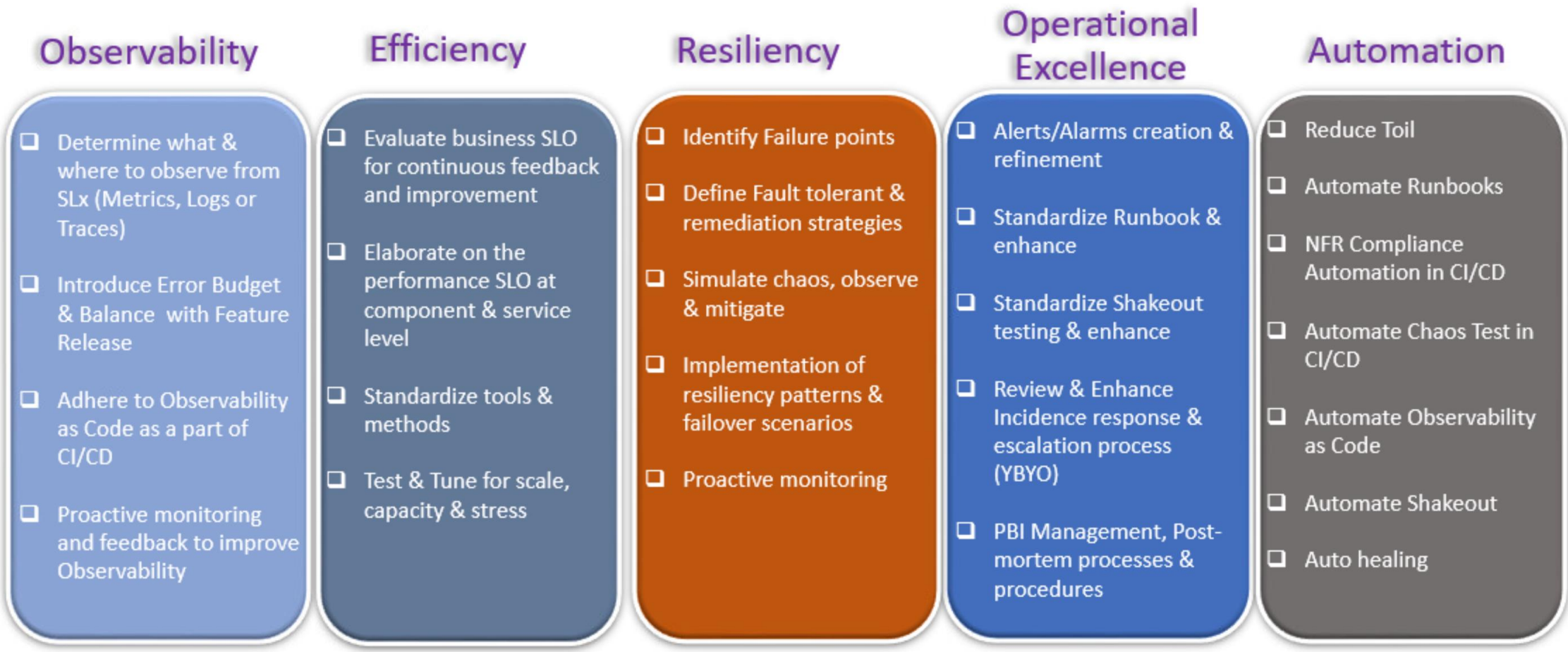
Sequence of Events to enact a Recovery Operation

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Five Pillars of Site Reliability Engineering (SRE)

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

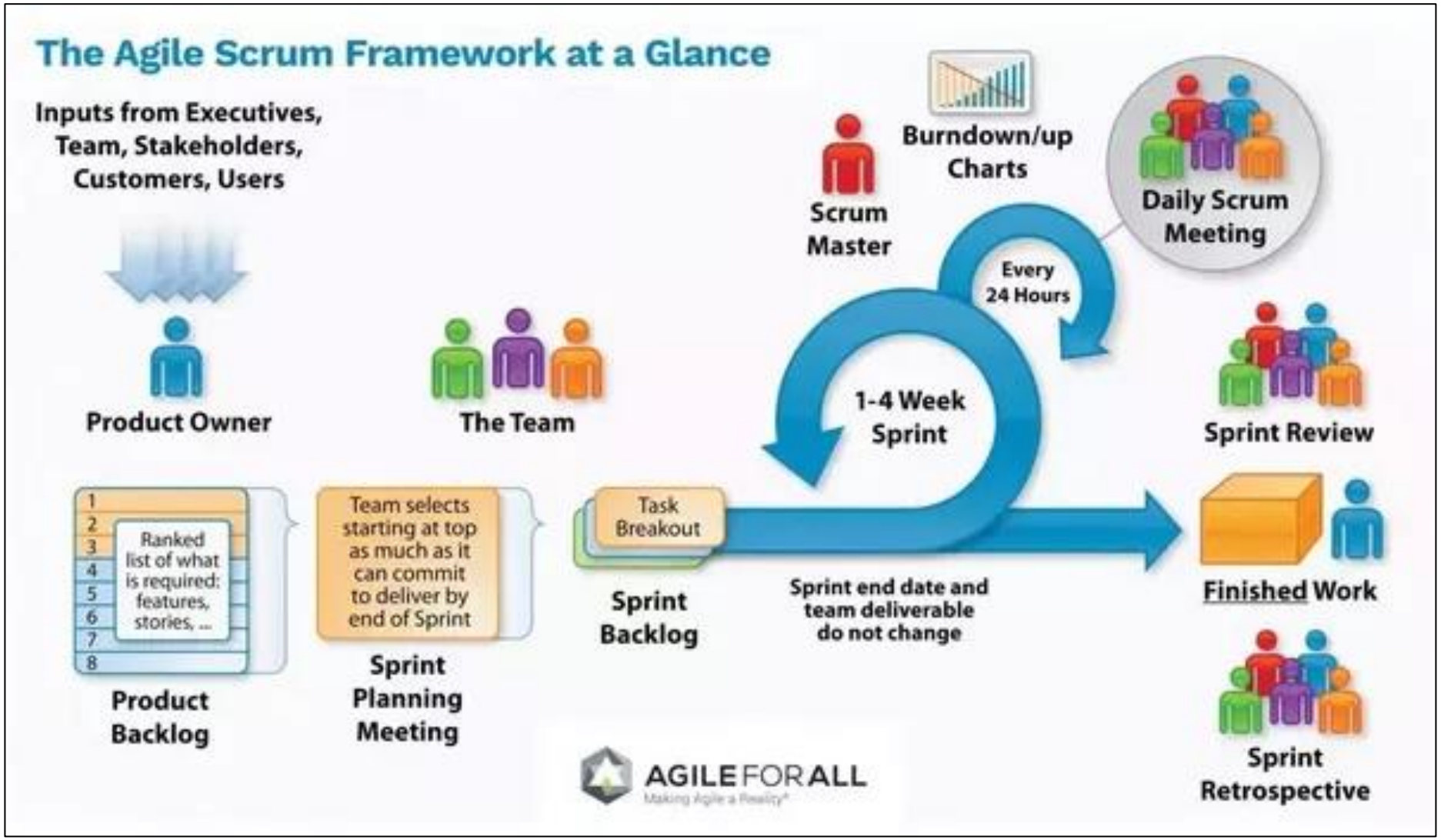


Google – Site Reliability Engineer Handbook

NFR – Non-Financial Reporting

Agile vs Waterfall Systems Development

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

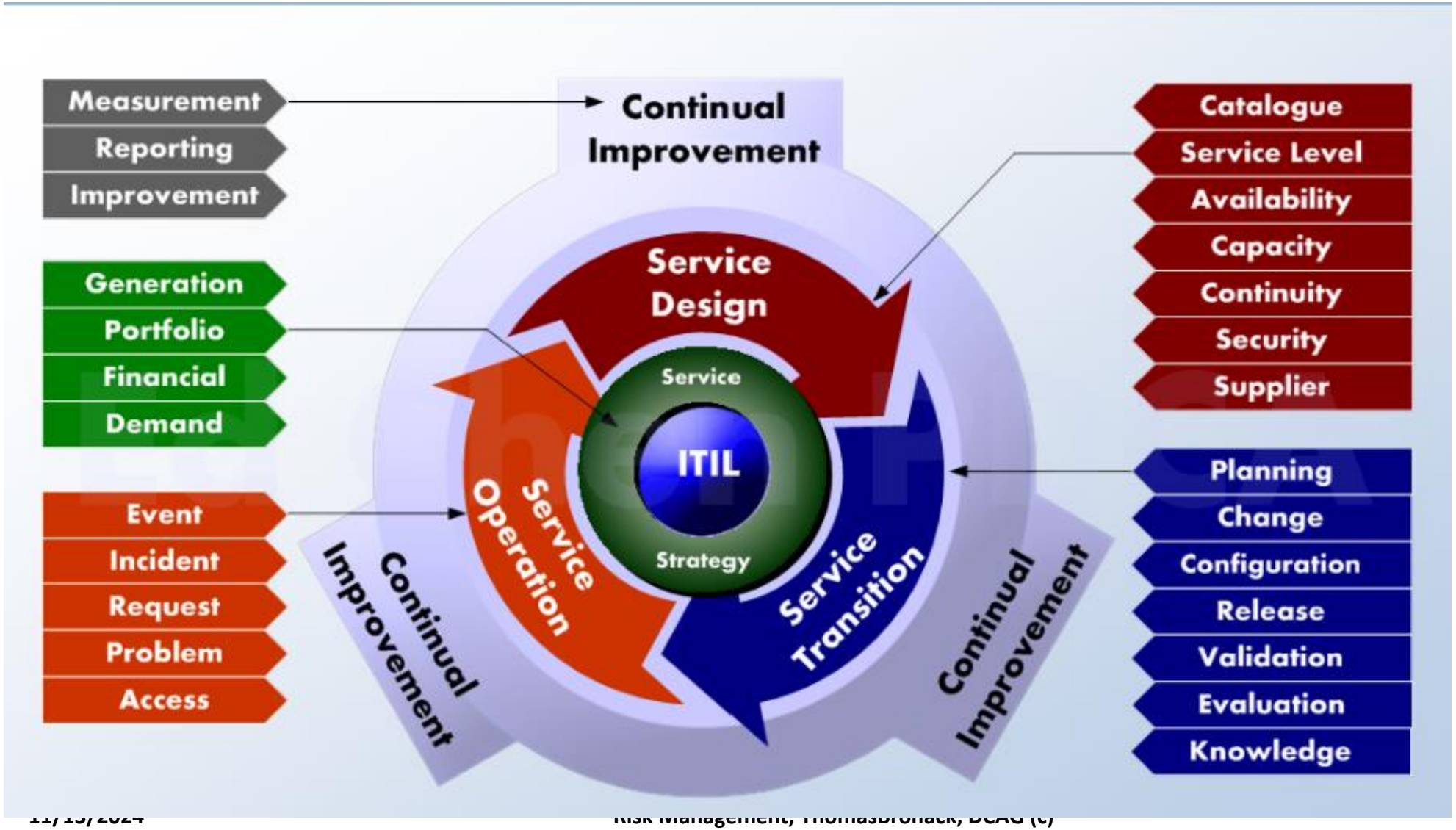


- Conception
- Initiation
- Analysis
- Design
- Construction
- Testing
- Deployment

Waterfall Model

Information Technology Infrastructure Library (ITIL)

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

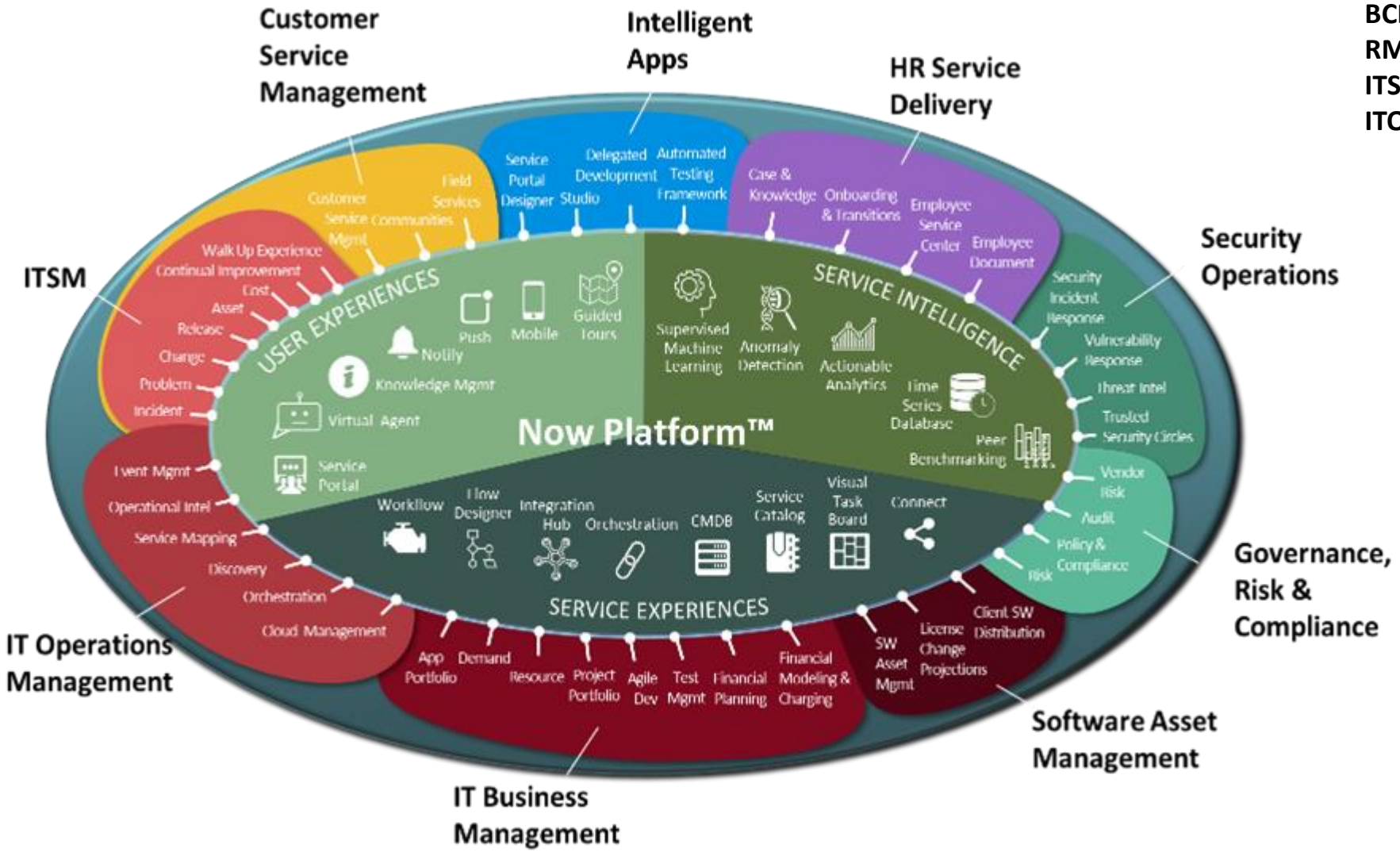


ITIL assists in:

- Planning,
- Defining,
- Obtaining,
- Installing,
- Implementing,
- Documenting,
- Training,
- Utilizing,
- Monitoring,
- Supporting,
- Maintaining, and
- Changing your IT environment to meet the needs of your business and support IT Operations.

ServiceNow Overview of Functions

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



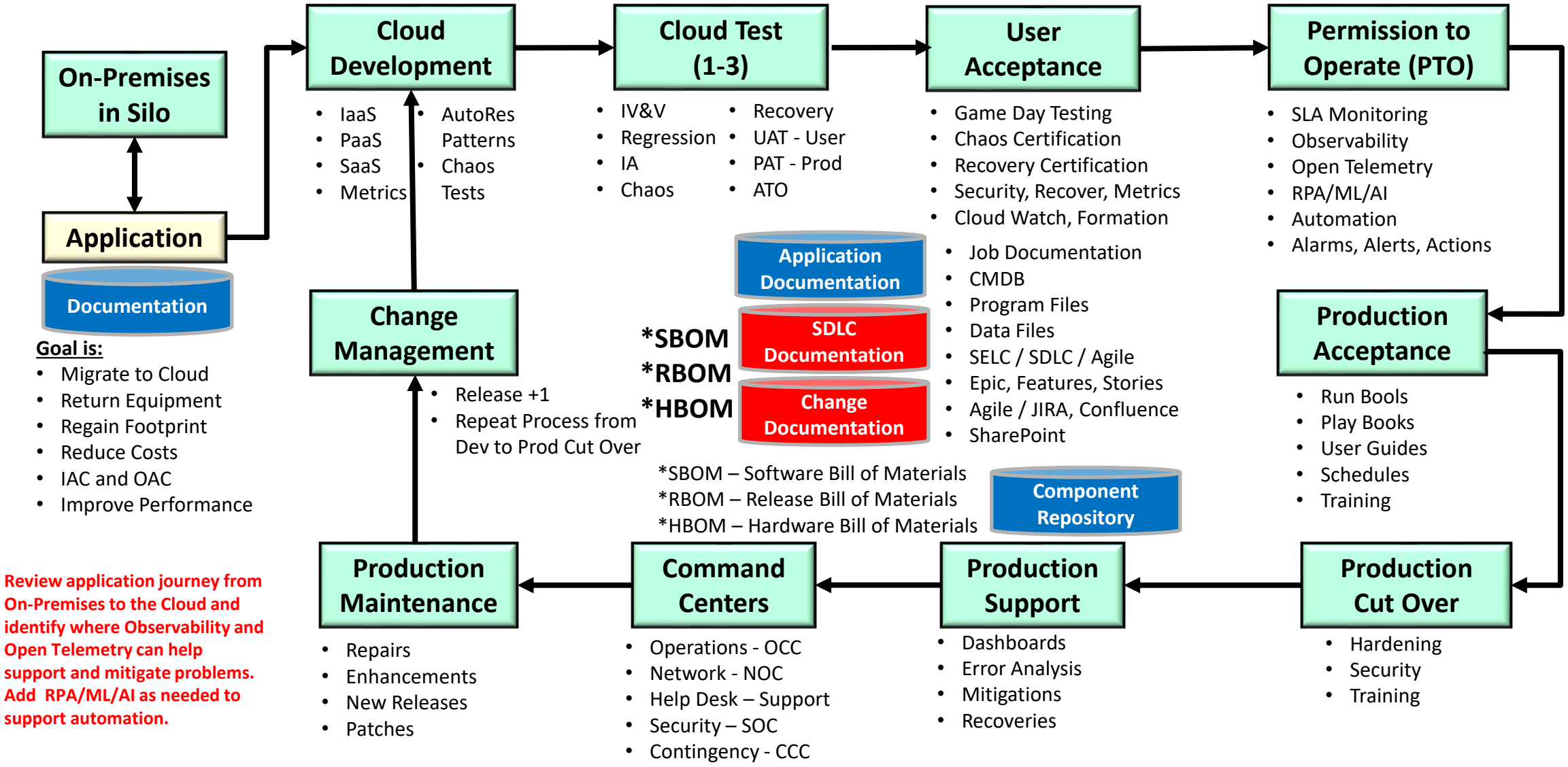
BCM – Business Continuity Management
RM – Risk Management
ITSM – IT Service Management
ITOM – IT Operation Management

Forms Management & Control:

1. I know a form is required to get this work done, but I don't know which form.
2. I found the form, but I don't know how to fill it our.
3. I know how to out the form, but who should I give it to for approval.
4. Once it is submitted, who do I notify if I have a change.
5. Is the form tracked until its completion.
6. How can I accomplish repeat work faster.
7. Are there reports available to track forms and work?

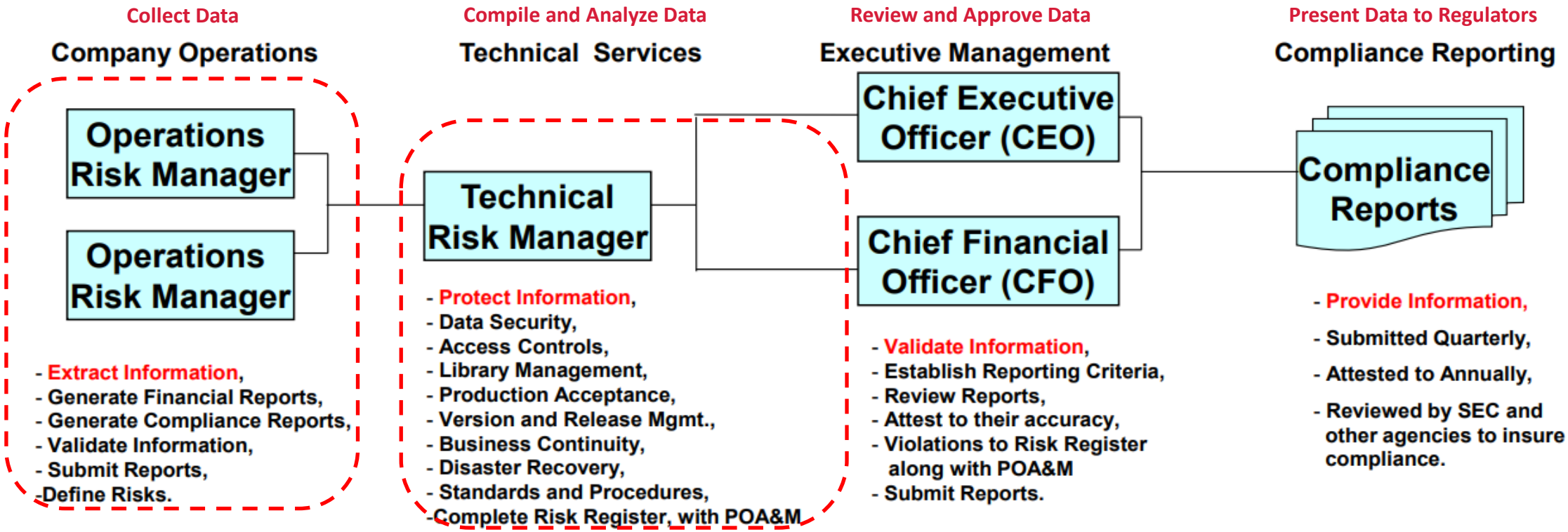
Migrating Applications to the Cloud - Functions / Tests

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Continuous Compliance Reporting

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Auditing Process:

- Domestic and International Laws and Regulations are defined,
- Audit Requirements are Defined,
- Audit Scripts are created,
- Auditor performs their Audit,
- Company Operations personnel are employed to verify Line of Business adherence to compliance,
- Technical Services complies Operations Reports,
- Risk Register and POA&Ms generated,
- Executive Management Agrees on Reporting format and data,
- Compliance Reports are created and submitted,
- Letter of Attestation is generated for Regulators

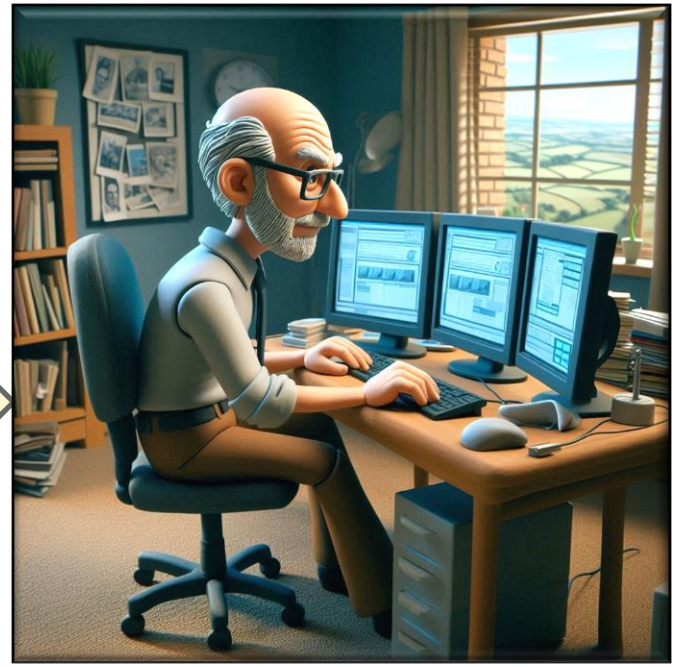
Reaching out to assist our clients

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

- 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