



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

Enterprise Resilience, Business Recovery Management, and Risk Management

Contact Information:

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

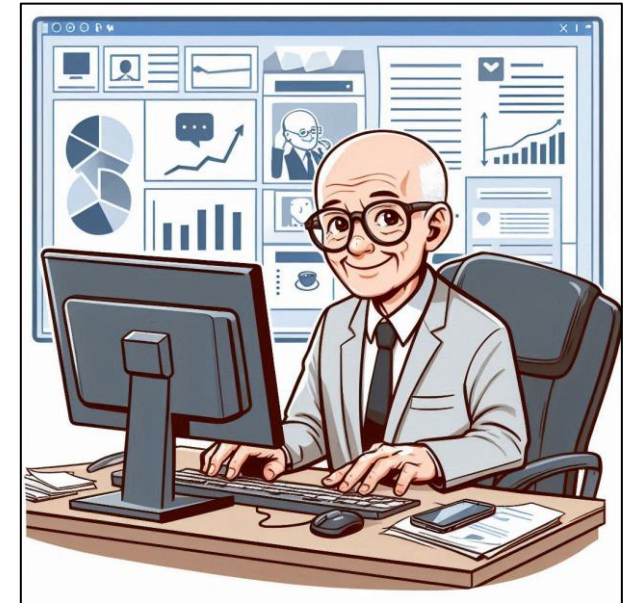
A word from Thomas Bronack

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 have provided enterprise analysis, evaluation, recommendations, Key Performance Indicators (KPIs), Enterprise Risk Management, 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.

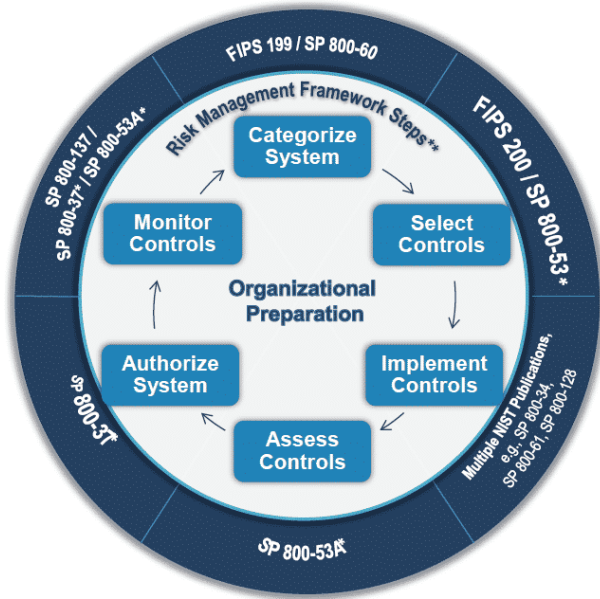
DCAG follows the “**Whole of Nation**” and “**Secure by Design**” guidelines developed by DHS/CISA to produce vulnerability-free components through Software Bill of Materials (SBOM) to identify and correct vulnerabilities prior to production and CTEM error identification while in production. This supports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



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

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

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 Enterprise 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** major 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 than 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.

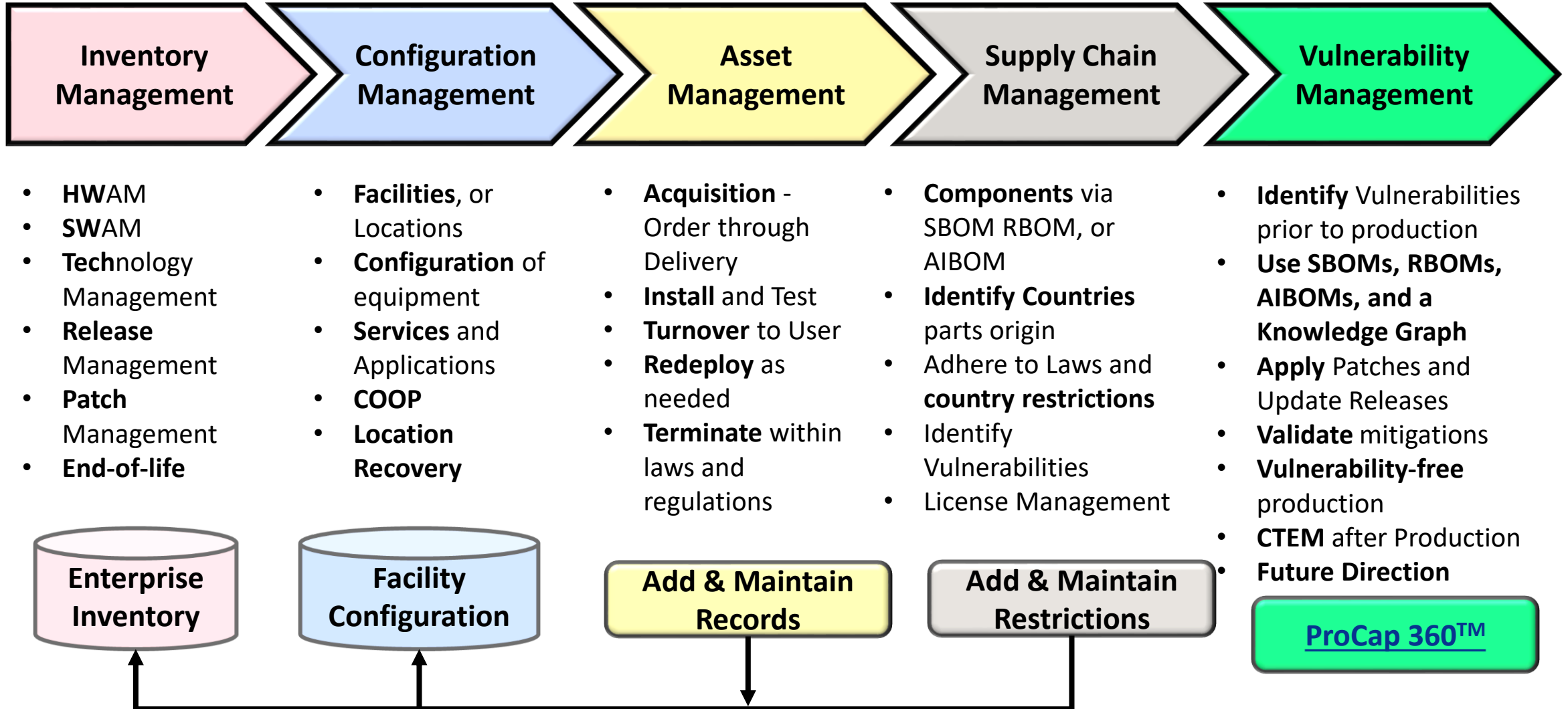
Business Resilience Plan must contain

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**

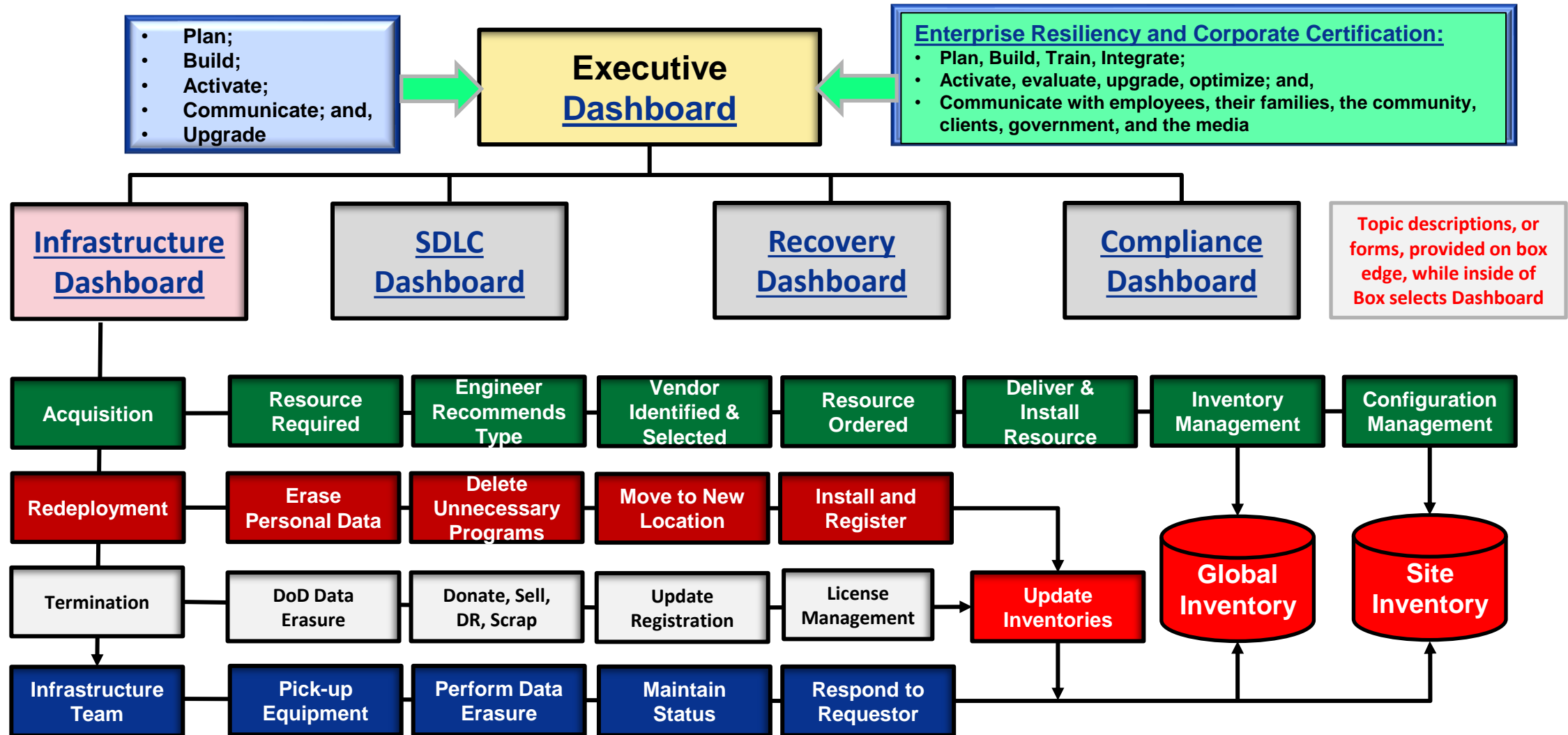
Know and Control your Environment

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



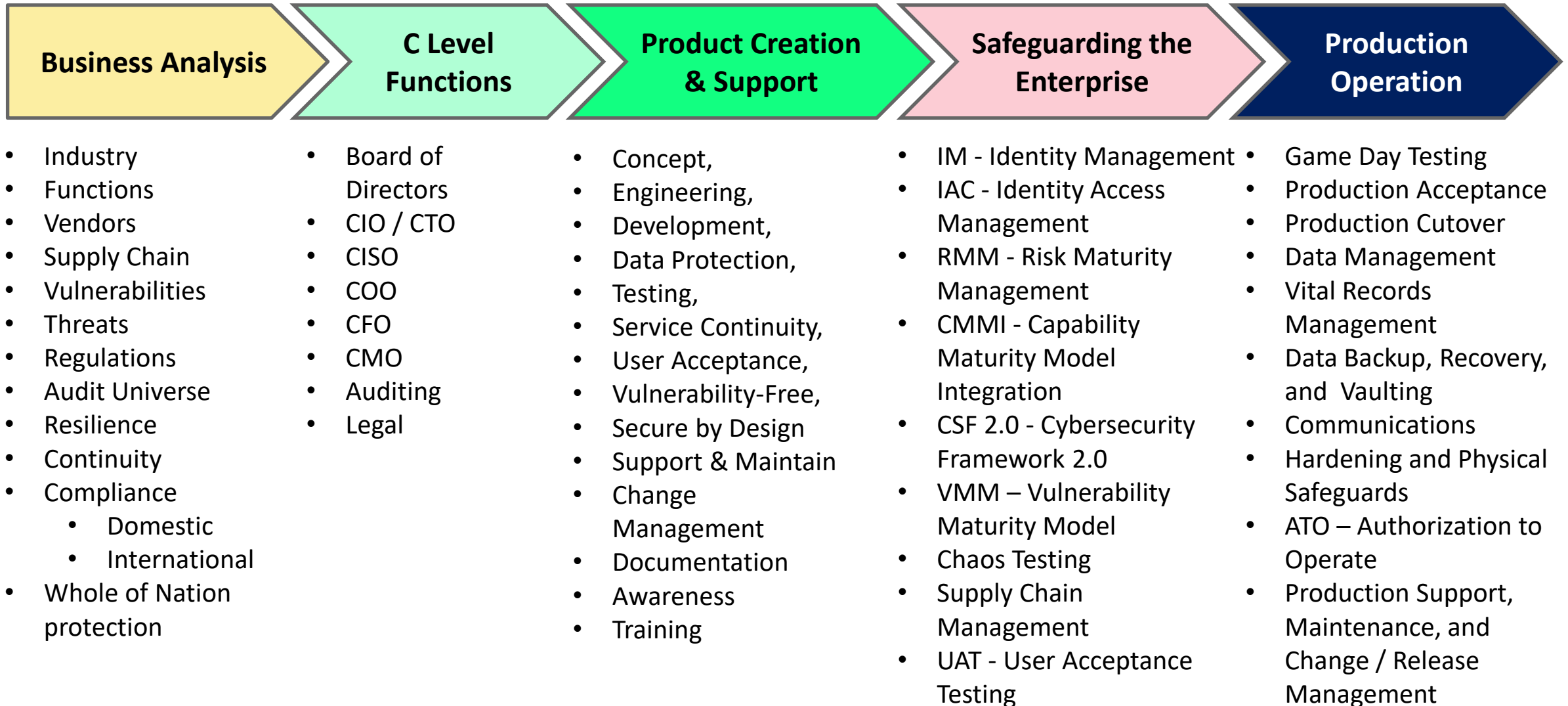
Asset Management Process

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

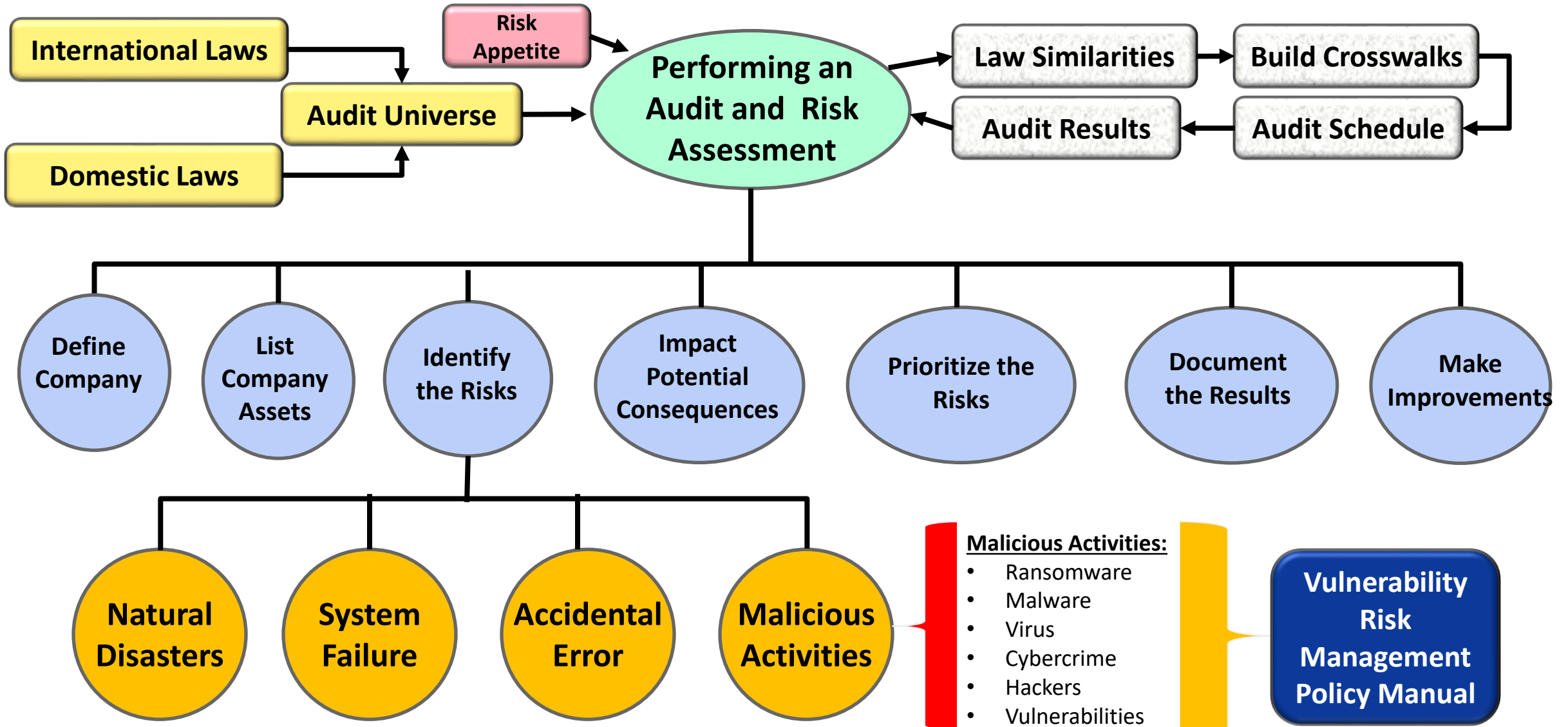


Safeguarding your Enterprise

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



Performing an Audit and Risk Assessment



Vulnerability Management definition and process

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

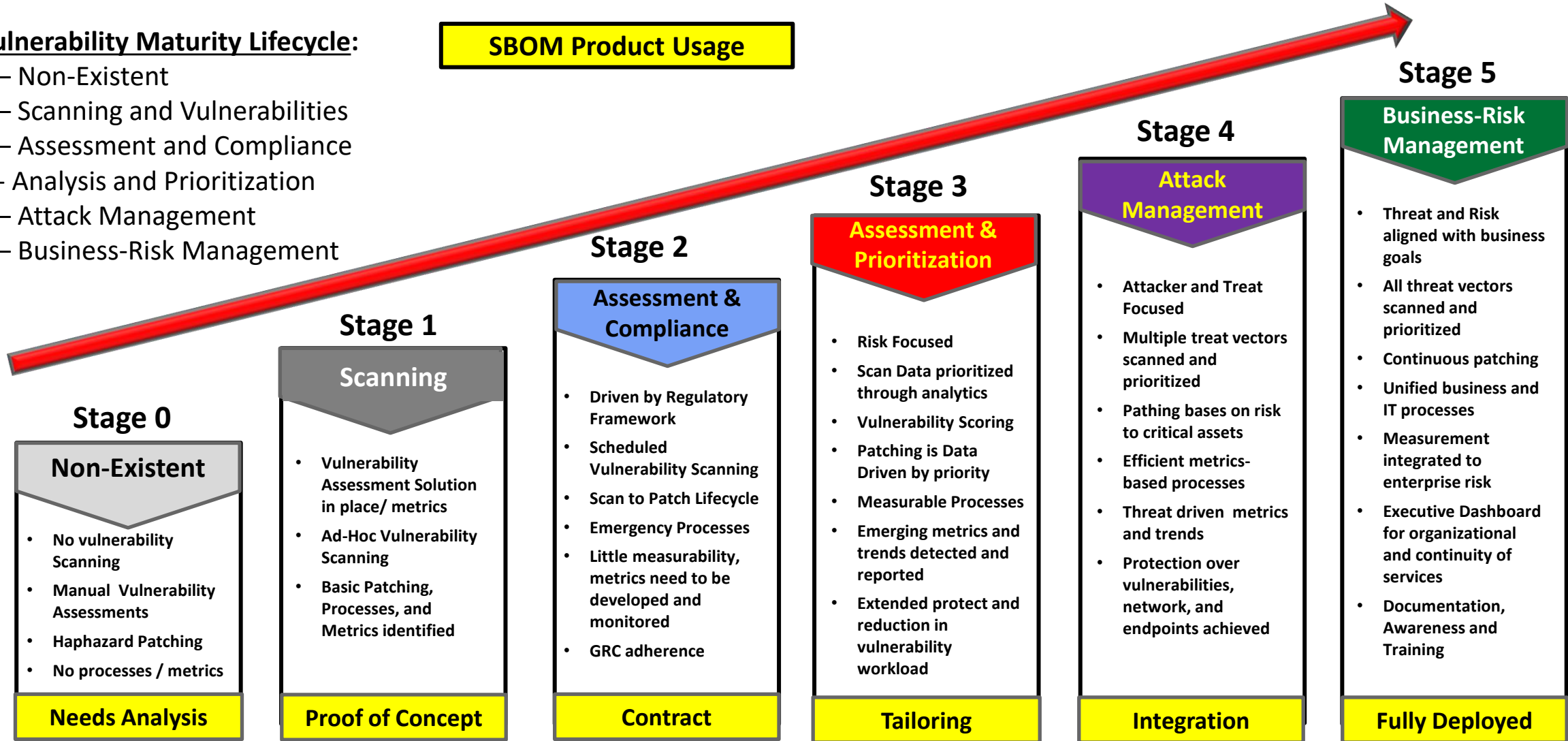


Vulnerability Management Maturity Lifecycle

SBOM Product Usage

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



Global Vulnerability Management Policy generation

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



- Business:**
- Services
 - Applications
 - Topology
 - Regions
 - Countries
 - Operation Centers
 - Workflow
 - Job Responsibilities
 - Vulnerabilities
 - Security
 - Gaps
 - DevSecOps
 - CATO, CTEM
 - Problem/Incident Management
 - Recovery Management
 - ITSM, ITOM

Country:

- Statues
- Laws
- Guidelines
- Domestic
- International
- General Policy
- Auditing & Reporting
- Gap's & Exceptions
- Mitigations

Company:

- Business Services and Applications (Rated 1-7)
- Technical
- Engineering
- Development
- Production
- Tools
- Workflow
- Migrations
- Transitions

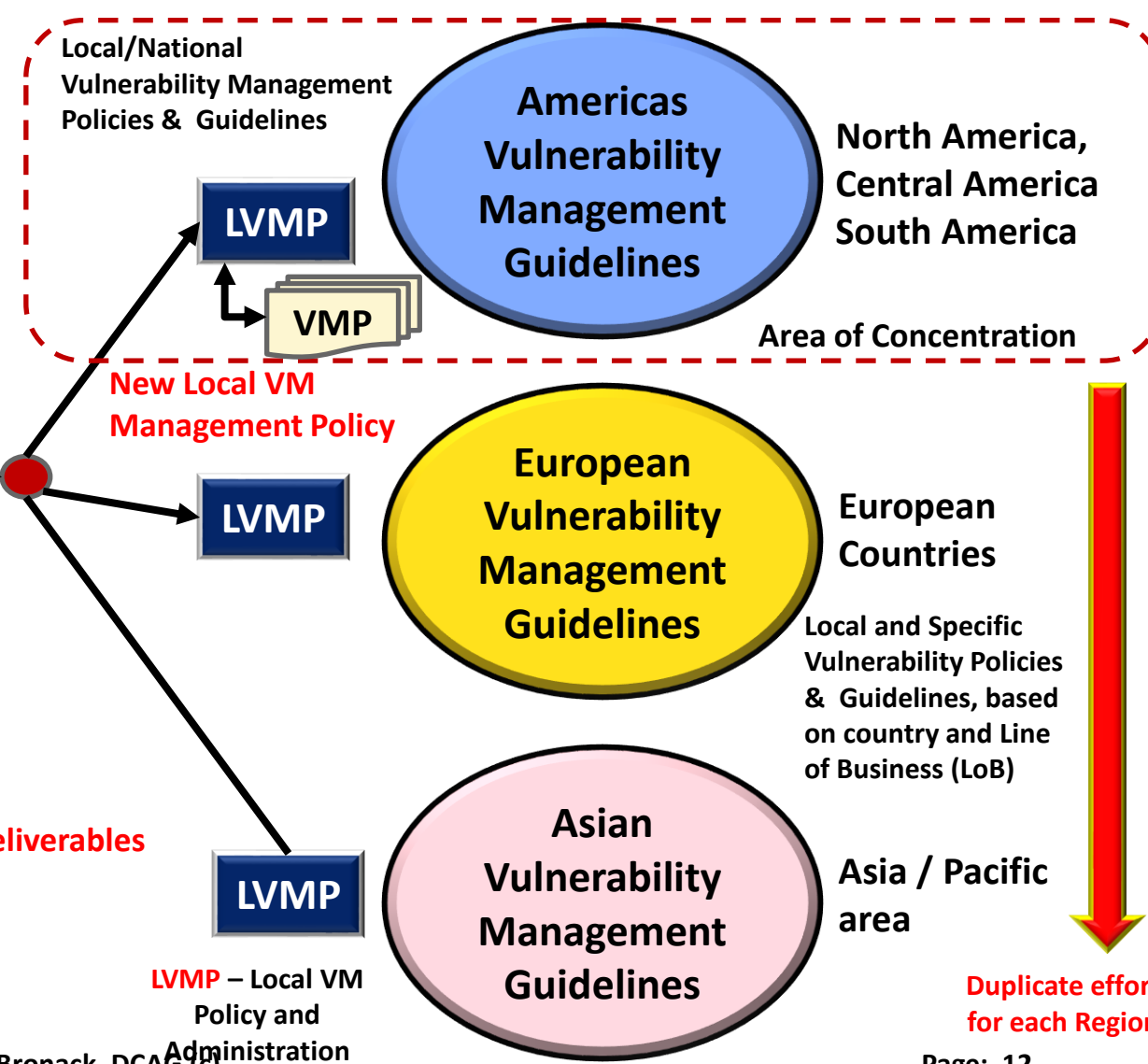
Staff:

- LOBs
- Organization
- Structure & Titles
- Component Owners
- Job Functions & Responsibilities
- Job Descriptions
- Skills Matrix
- Awareness & Training

Review existing VM Policies
 Global VM Policies

11/18/2024 **Could also be Company HQ and Domestic Regions**

Risk Management, ThomasBronack, DCAG (6)



Research

Deliverables

LVMP – Local VM Policy and Administration

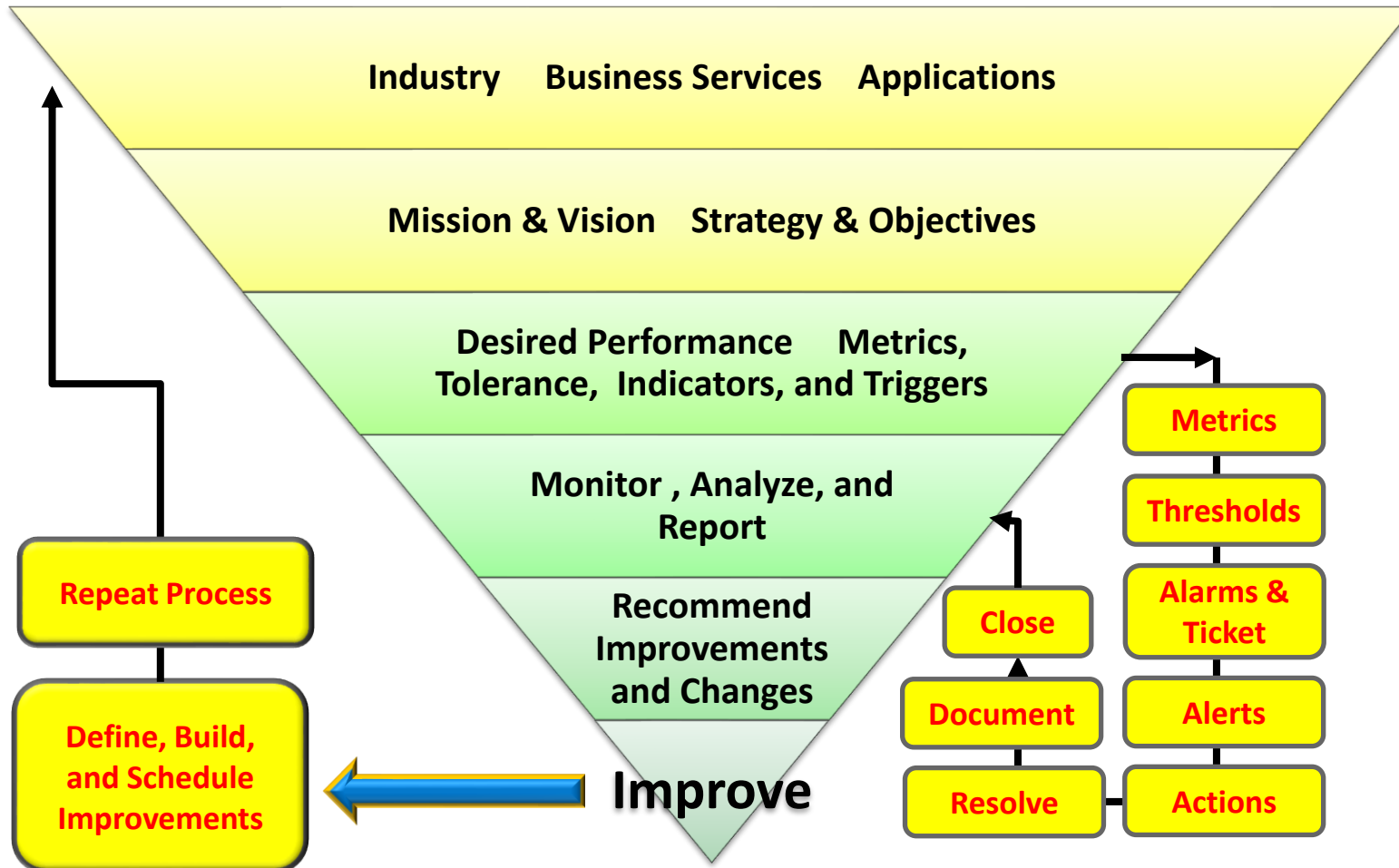
Area of Concentration

Duplicate effort for each Region

The Risk Appetite Process Using COSO

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

Defining the Risk Appetite using COSO

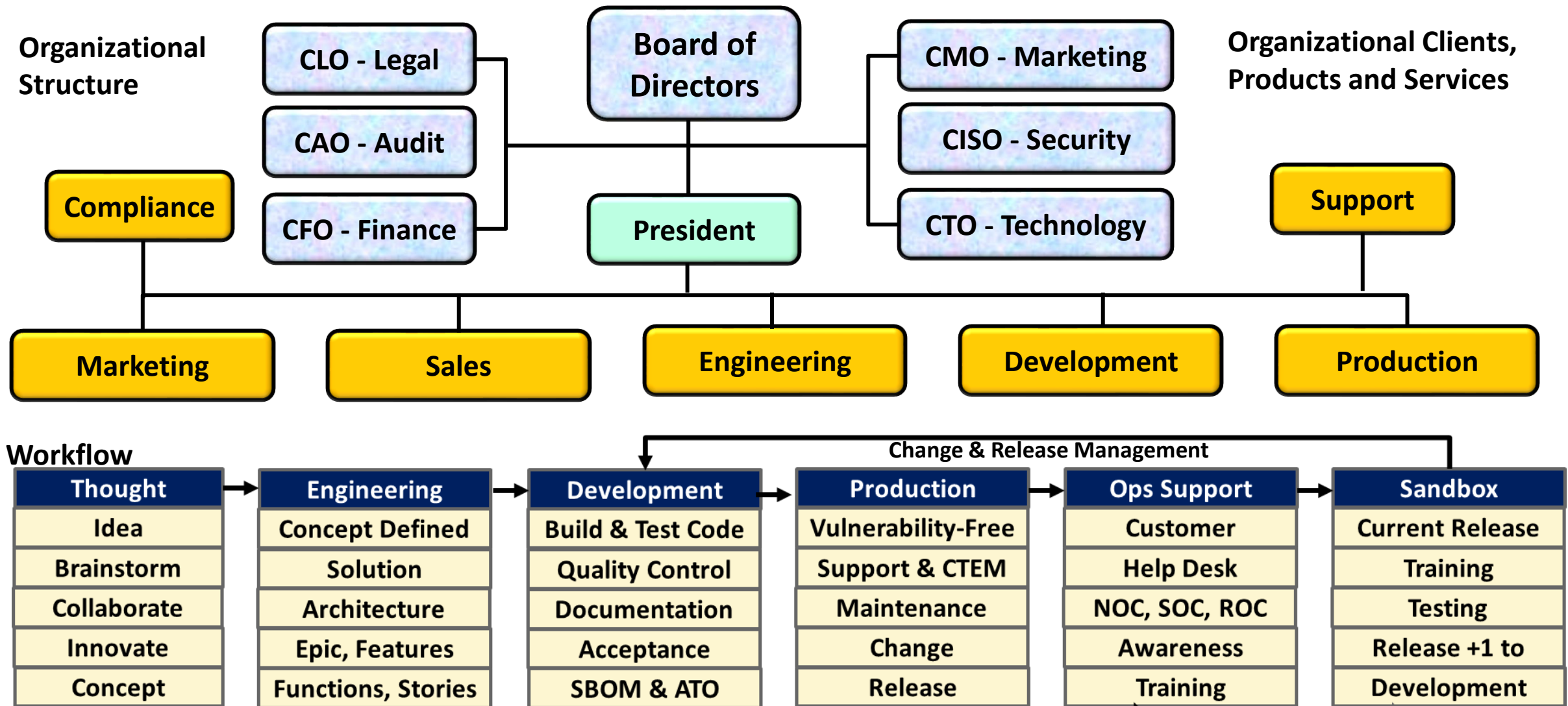


COSO for Risk Appetite & Evaluation:

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.

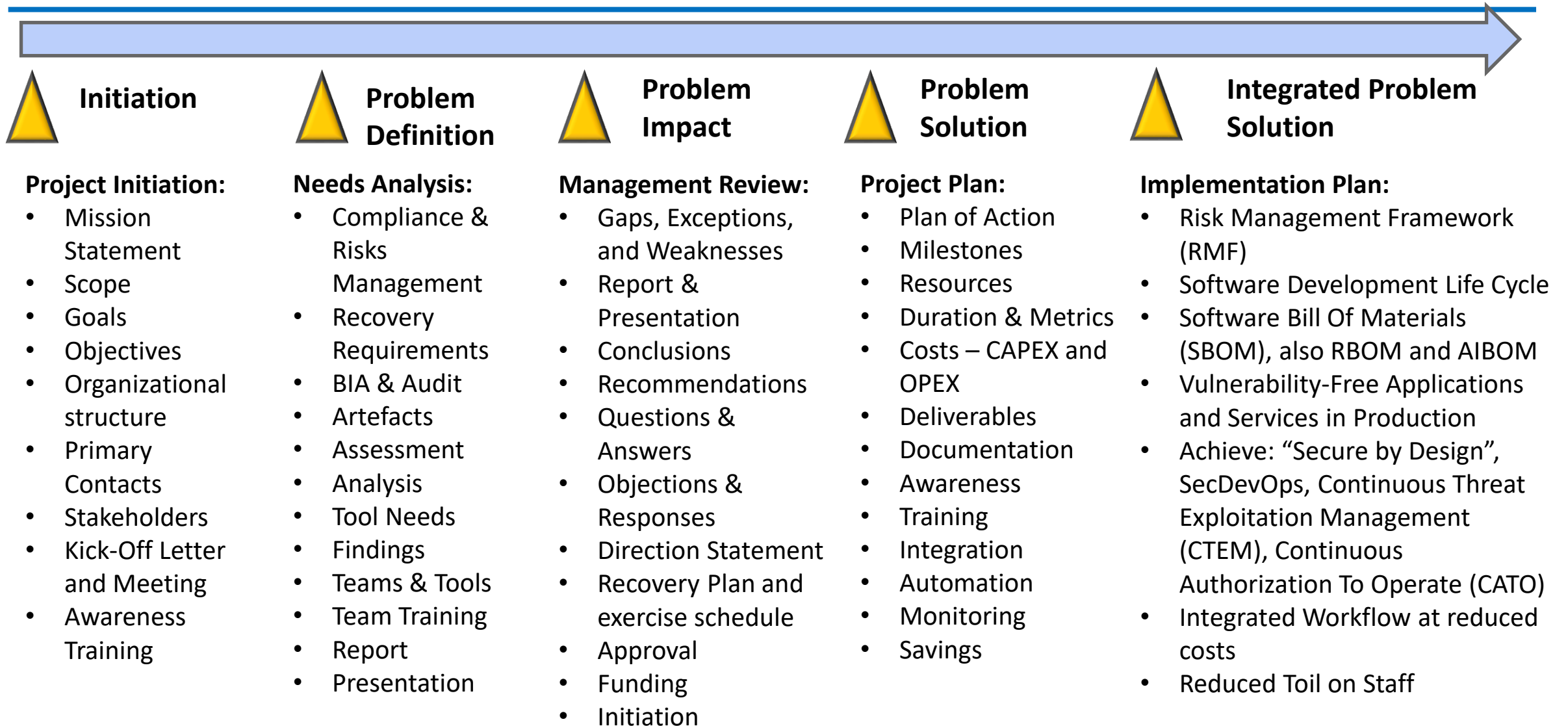
Organization and Functional Responsibilities

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



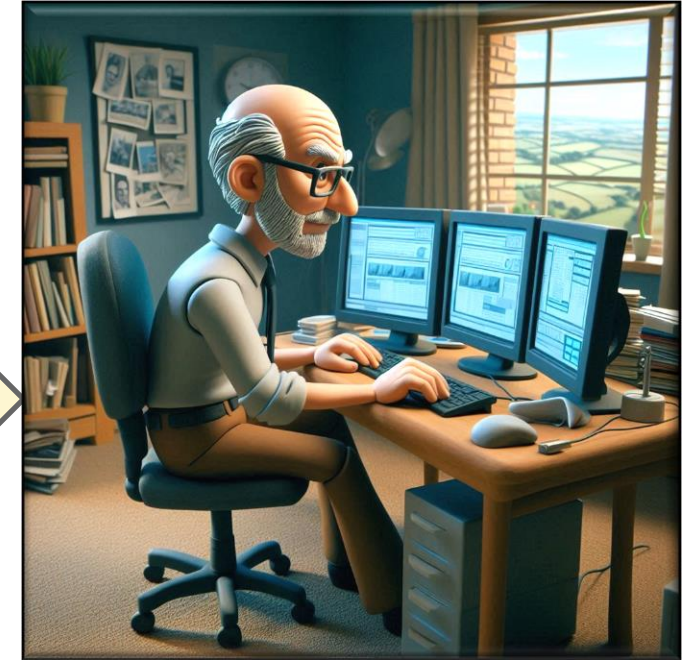
Reaching out to assist our clients

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



- Discuss
- Define
- Propose
- Achieve

Quality Service at
a Reasonable
Price



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