Created by:

Thomas Bronack, CBCP
Bronackt@gmail.com
Cell: (917) 673-6992

Thomas Bronack
Service Offering

Enterprise Resiliency

Including

Site Reliability Engineering and Risk Management

with

Tom Bronack

Business Continuity, IT Disaster Recovery, Business Location Recovery (COOP), Workplace Safety and Violence Prevention, Emergency Management, Crisis Management, Supply Chain Management, Site Security / Salvage / Restoration, and Application Cloud Migration for Efficiency and Failover / Failback Recovery Operations, with Identity Management, Risk / Audit Management, Asset Management, and Infrastructure Management

Risk, Audit, Cyber & Compliance Risk Management, Laws & Regulations, Auditing, Gaps & Exceptions, Obstacles, Risk Register, Security Enforcement, SOC & Help Desk, Contingency Command Center (CCC), and Emergency Operations Center (EOC)

Business Impact Analysis (BIA) Perform a BIA of facilities, to define their staff, criticality, functions, required supplies, vendors, and Recovery Needs.

Cybersecurity Foundation Management to eliminate risks

Business Continuity Management is the combinations of all recovery disciplines under one umbrella.

Personnel Services to ensure proper awareness and training to all levels of staff regarding recovery planning and operations.

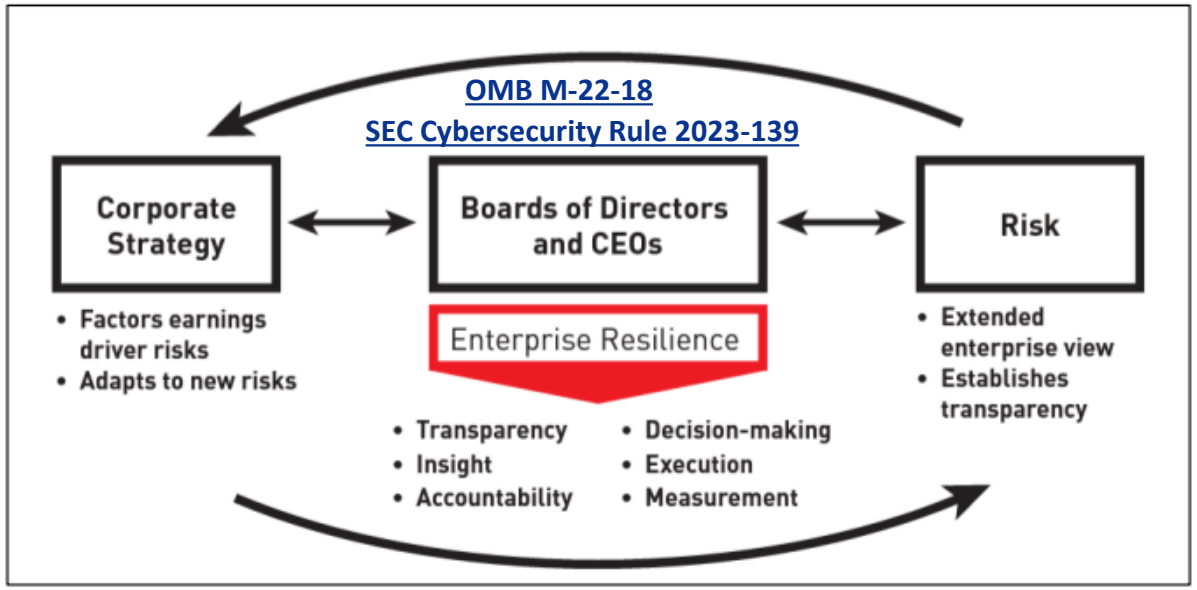
Cloud Migration, Resilience, & DR Planning to reduce costs, optimize service, and provide recovery services.

- **IT Disaster Recovery** – to protect the data center and its infrastructure
- **Business Location Recovery –** to protect business locations and their staff.
- **Workplace Safety and Violence Prevention** – to protect personnel from harm or Active Shooter situations.
- **Emergency Management** – to protect the company from interruptions due to natural and man-made disaster events.
- **Crisis Management** – to protect the company and its staff from Crisis Situations that can cause harm to staff and interrupt the business from delivering services.
- **Supply Chain Management** – to ensure the continuous supply of materials as needed supplies during normal and recovery operations in compliance to government regulations.
- **Site Security, Salvage, and Restoration** during and after a business location has a disaster event.
- **Application Migration and DR Planning** for On-Premises, Cloud, and Hybrid applications to improve efficiency, performance, and Failover / Failback operations

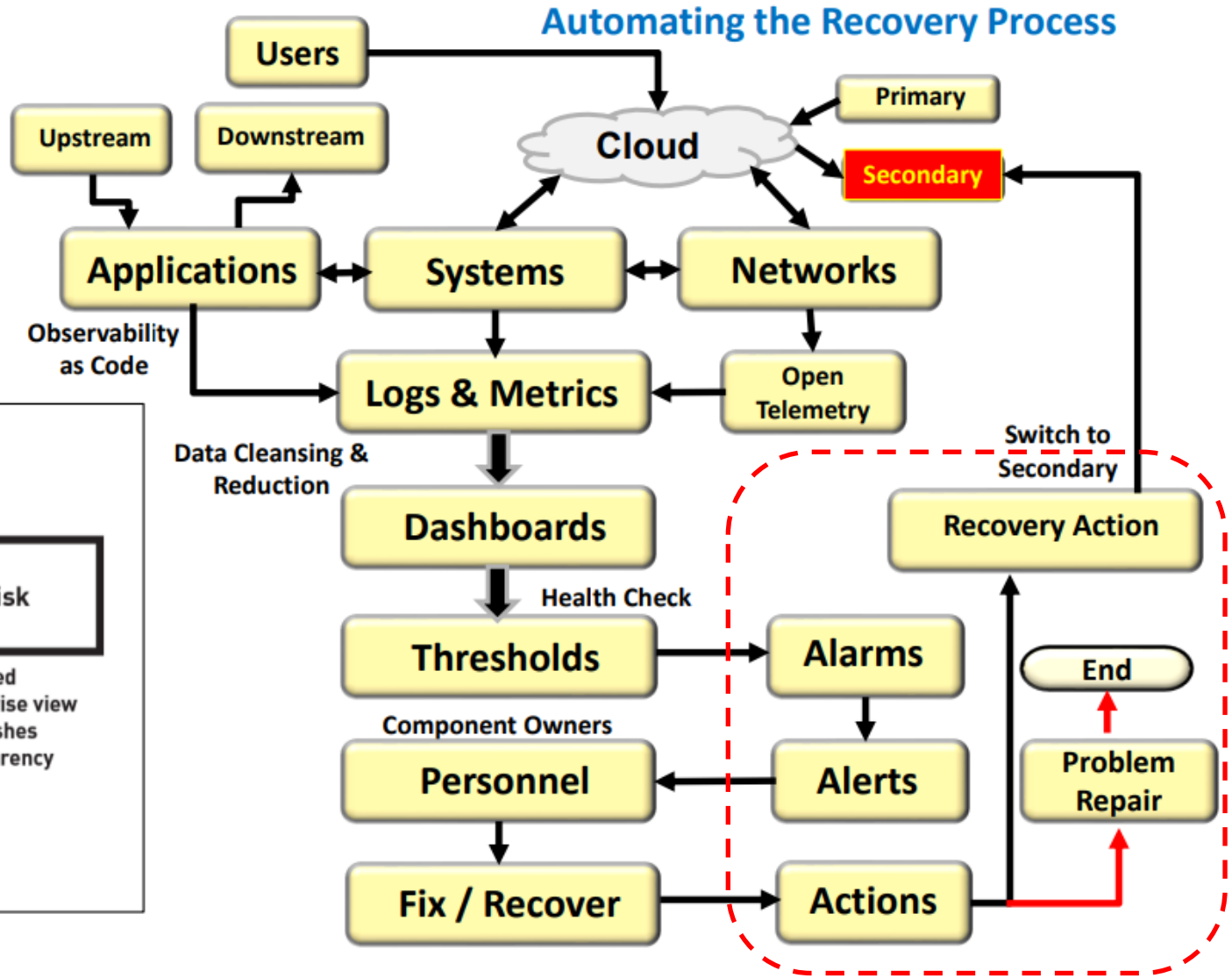
Board of Directors concerns

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

The Board of Directors is responsible for protecting the company and ensuring its reputation and continued growth. Therefore, they must establish Resilience, Compliance and Safeguards to ensure continued operations.



Risk Management Life Cycle



What does Enterprise Resilience consist of?

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

- Enterprise Resilience requires a Company Culture and Awareness
- Metrics, Monitoring & Reporting,
- Support & Improvement

Enterprise Resilience concists of:

- Enterprise Products & Services,
- Critical Economic Services,
- Financial Health & Visibility,
- Brand and Company Reputaton,
- Risk Management & Business Impact Analysis,
- Business Continuity / Continuity of Operations/ Disaster Recovery,
- Crisis Management & Communications
- Critical Environments,
- Information Security,
- Human Resource Management,
- Production Operations and Support,
- Incident & Problem Response,
- Lega, Audits, & Compliance,
- Organizational Behavior,
- Supply Chain Resilience,
- Personnel Safety and Violence Prevention.

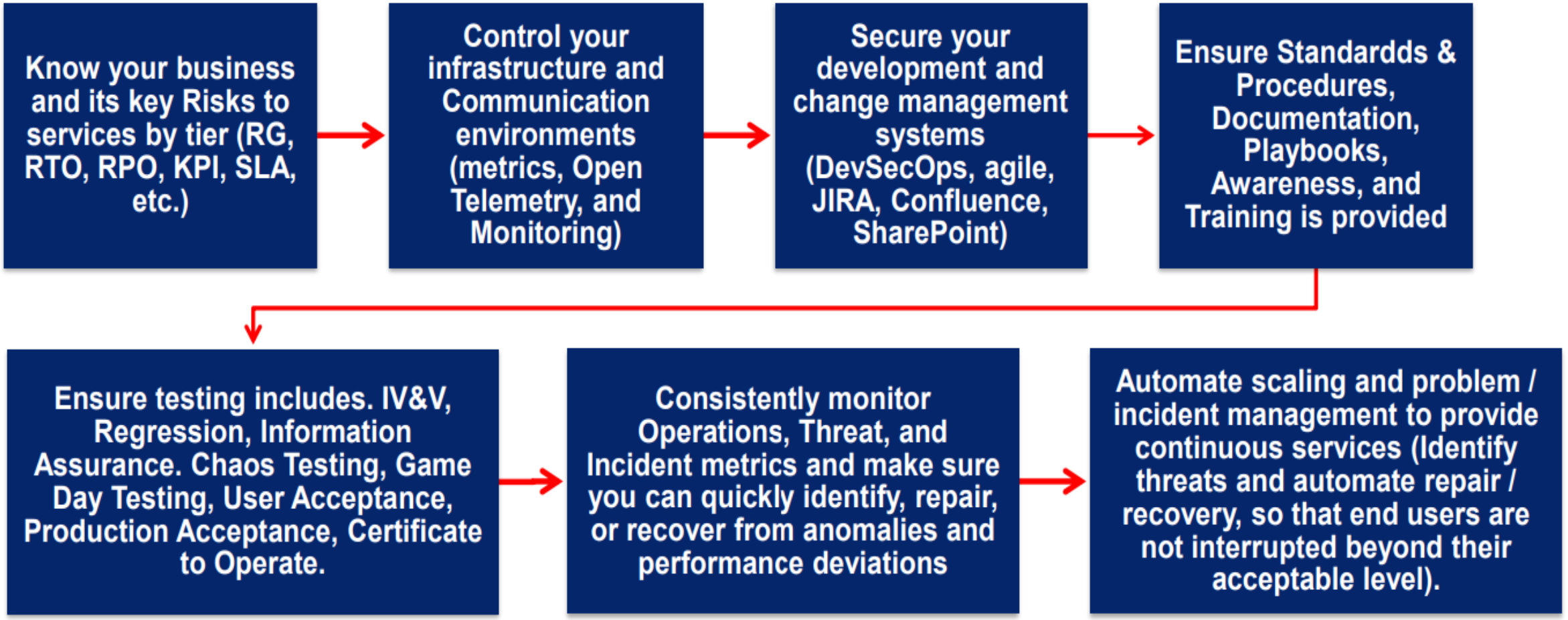
Process followed in performing Enterprise Resilience

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

1. **Rating the sensitivity of your company's applications – Know your company**
   a. **Revenue Generators** – Protecting Revenue Stream and Profits
   b. **Client Facing** (Dashboards, Websites, application extensions, etc.) – protecting Reputation & Brand
   c. **Supporting** company operations
   d. **Recovery** Time Objective ((RTO), Recovery Point Objective (RTO), Recovery Time Capability (RTC), Recovery Group (service continuity, time to recover, time sensitive applications and services) and Recovery Certification & Testing
2. **Locate weaknesses to be overcome – Know your environment**
   a. **Analyze** exposures and how you can best protect the business going forward (Risk Assessment, BIA, Security (Physical / Data / CSF / CIA), Compliance (Laws, Regulations, Attestation, Auditing), Development (Systems Engineering Life Cycle – SELC), Operations (Systems Development Life Cycle – SDLC), Dev/Sec/Ops – Agile, Jira, Confluence, SharePoint), IT Operations (ServiceNow, ITIL), Standards & Procedures, Documentation, Awareness, Training, Career Pathing, Identity Management (IM, IAM, CIAM, RBAC, ABAC, MFA, ZTA).
   b. **Identify Gaps,** Exceptions, Obstacles and either Mitigate, or Mediate weaknesses. Implement required Controls over identified Risks (Place Risks in Risk Register and develop a POA&M to correct Risk)
3. **Optimize Development, Test, Production, and Change Management Environments – Optimize and Comply**
   a. **Optimize auditing and** providing a Letter of Attestation to Regulators (Audit Universe).
   b. **Ensure security** is optimized and in place with awareness and staff training provided as required (use SBOM for Supply Chain).
   c. **Utilize Chaos Testing** to develop responses to encountered problems, prior to production acceptance. Ensure problem Runbooks and Recovery Runbooks are exercised correctly.
   d. **Implement** optimized Application Program Monitoring and Environment Observability System.
   e. **Monitor metrics (**PKIs, SLAs) to identify problems via thresholds that generate Alarms, Alerts, and Actions to be Taken.

How to protect your company

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

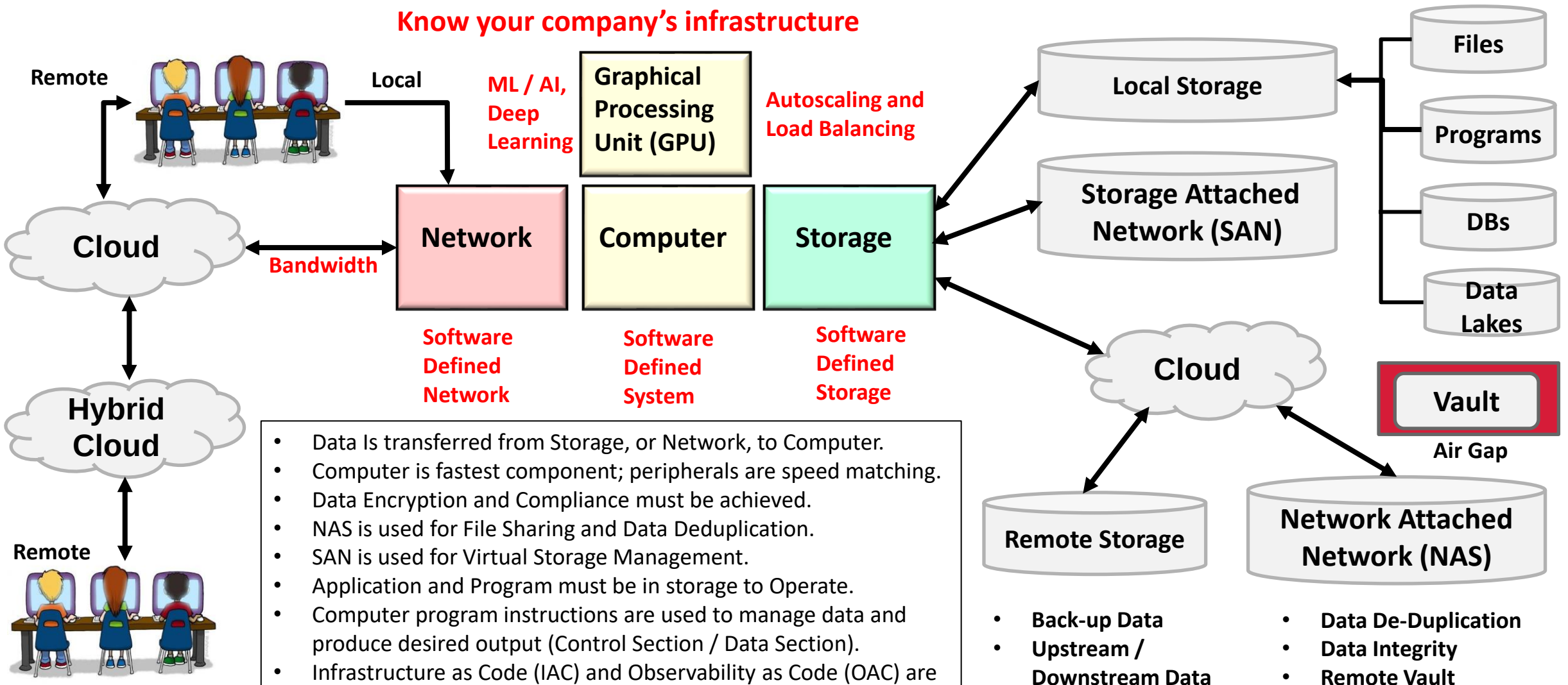


Integrate standards & procedures within everyday functions performed by personnel and ensure the implementation of Awareness and Training programs to keep staff and management informed

Monitoring Operations and Controlling Resources

Thomas Bronack
Email: bronackt@gmail.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.
- NAS is used for File Sharing and Data Deduplication.
- SAN is used for Virtual Storage Management.
- Application and Program must be in storage to Operate.
- Computer program instructions are used to manage data and produce desired output (Control Section / Data Section).
- 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**

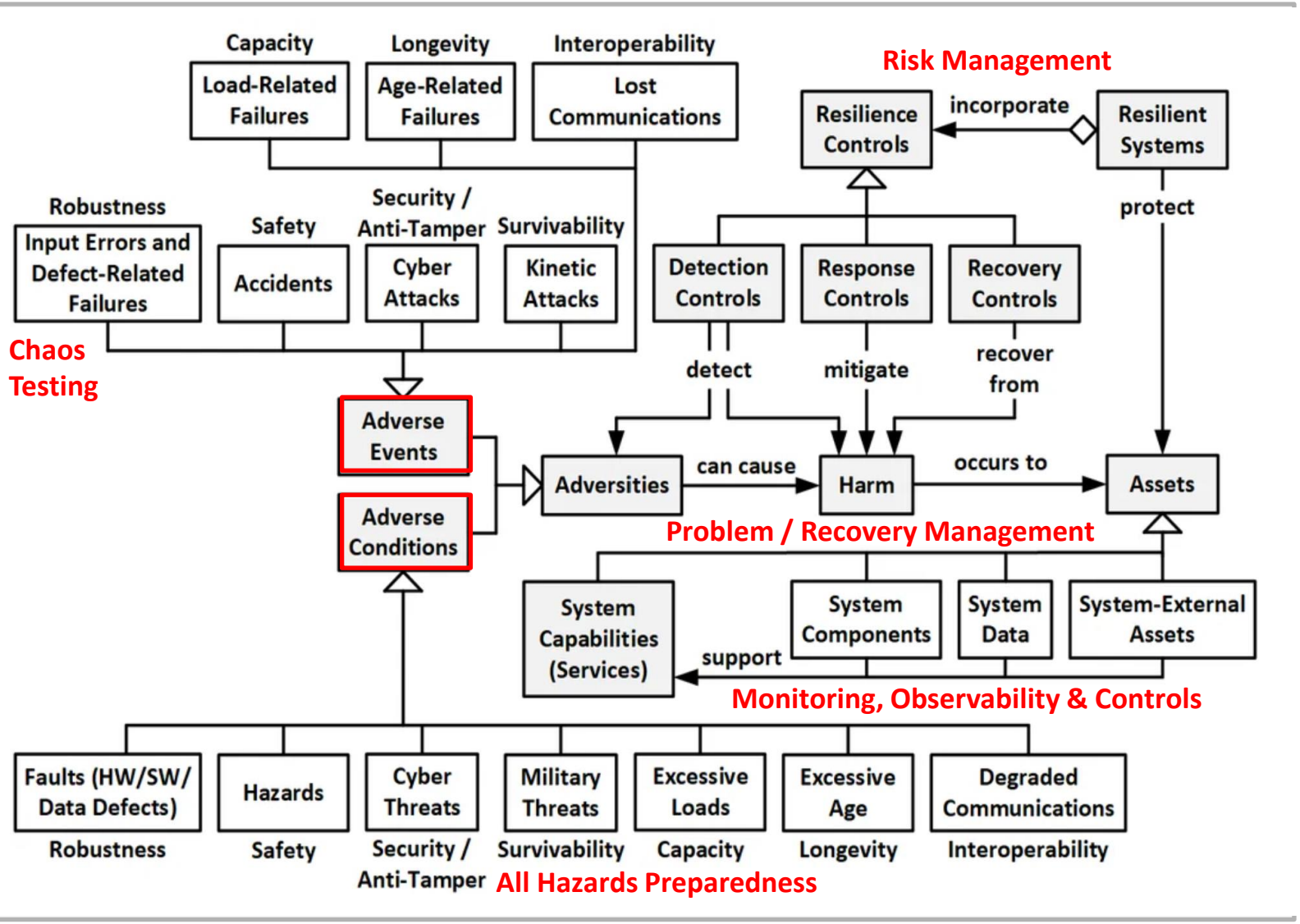
What is Resilience and why is it important

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

Definition:

Basically, a system is resilient if it continues to carry out its mission in the face of adversity (i.e., if it provides required capabilities despite excessive stresses that can cause disruptions). Being resilient is important because no matter how well a system is engineered, reality will sooner or later conspire to disrupt the system.

Achieving resilience when so many components can cause a disruption if a difficult taks indeed. It requires the full understanding and cooperation of the entire organization, its vendors, and suppliers.



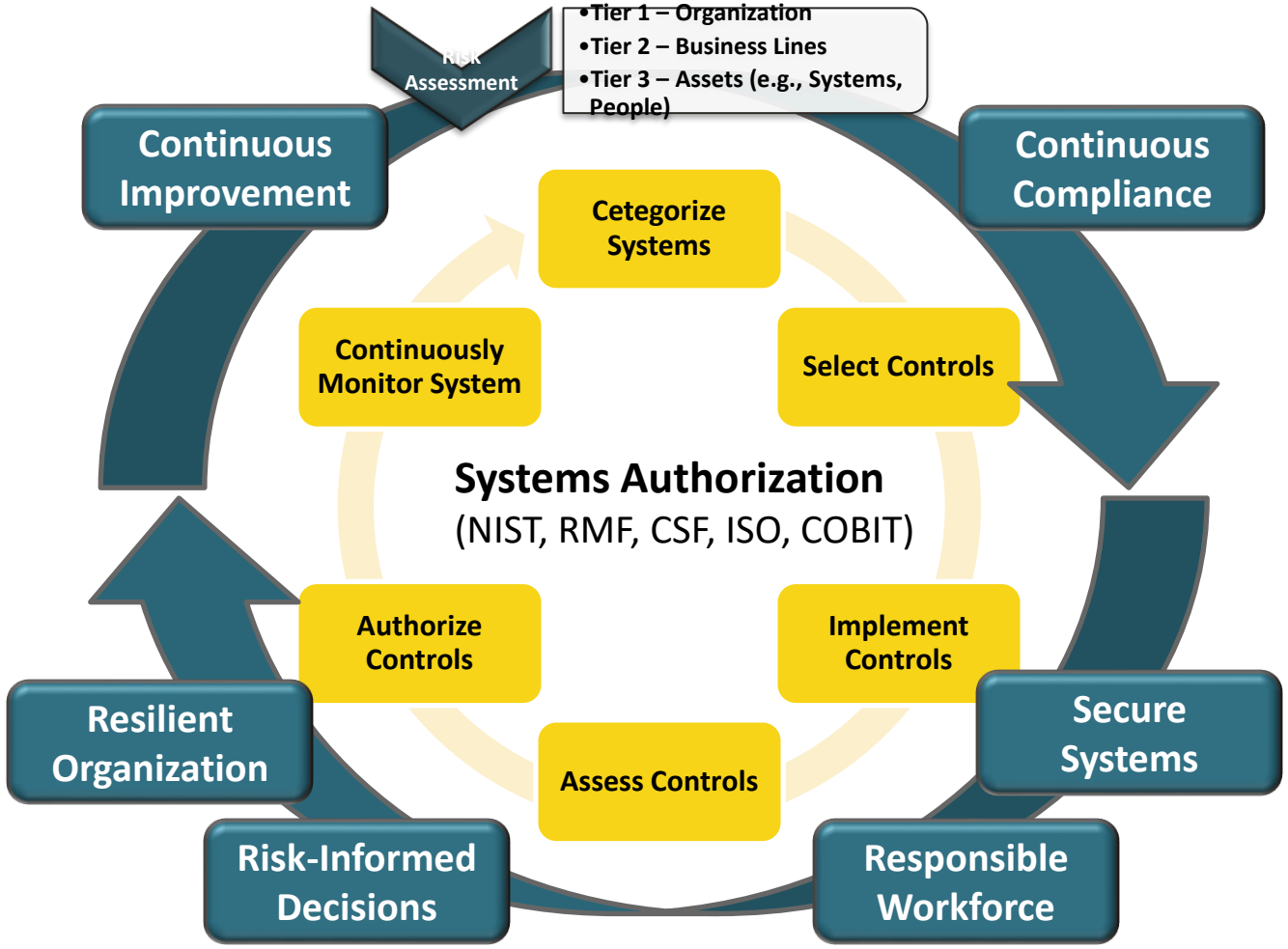
Ensuring Compliance via GRC and Risk Assessment

Thomas Bronack
Email: bronackt@gmail.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@gmail.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 businesss 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:

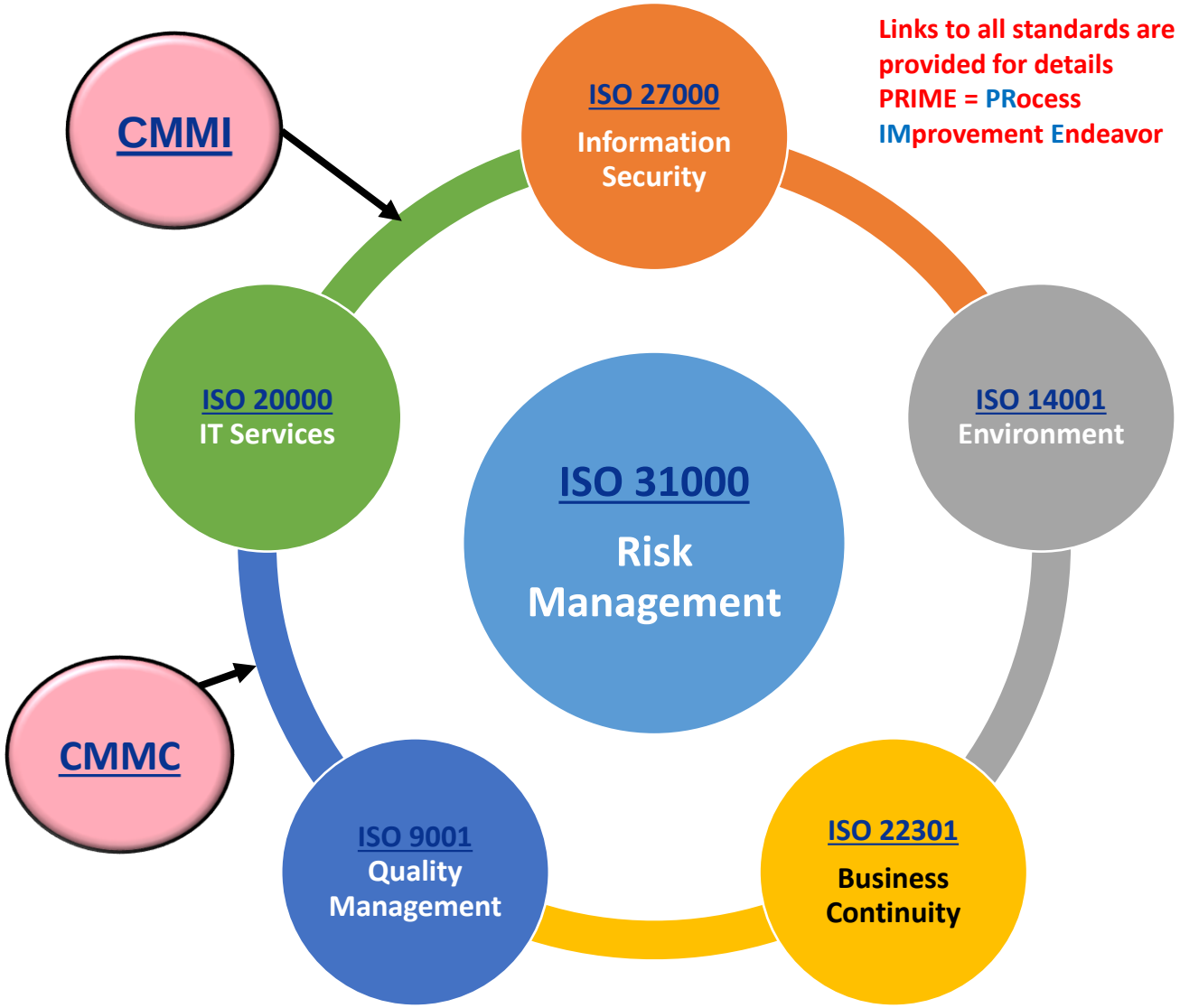
- Regulatory Audits and Attestations
- Risk Register with POA&M
- Standards Audits (e.g., ISO)
- Contractual Audits (e.g., PCI)

Reporting:

- Internal
- Regulatory Bodies
- Customers

The newest Integration Model – PRIME Approach

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



Links to all standards are provided for details
PRIME = PRocess IMprovement Endeavor

Developing a business optimization approach that combines these ISO Standards will help your company 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 Recovery Management.

Integrate Quality Management (ISO 9001) within all of 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.

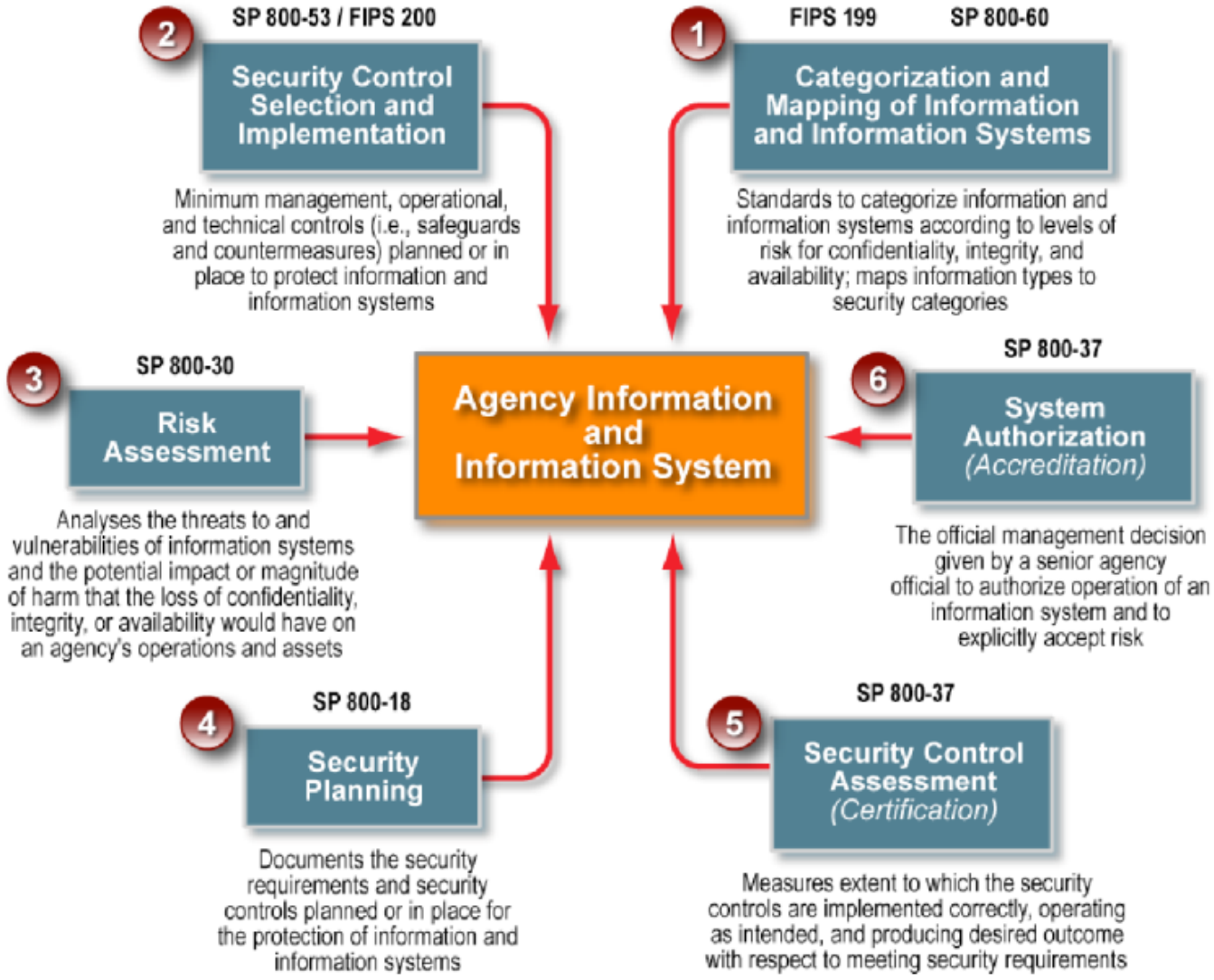
Finally ensure your **IT Services** (ISO 20000) are of the highest quality possible and that all ISO standards are adhered to in compliance with existing laws and regulations, so that you never have to fear failing an audited.

NIST SP 800 Technical Guidelines

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

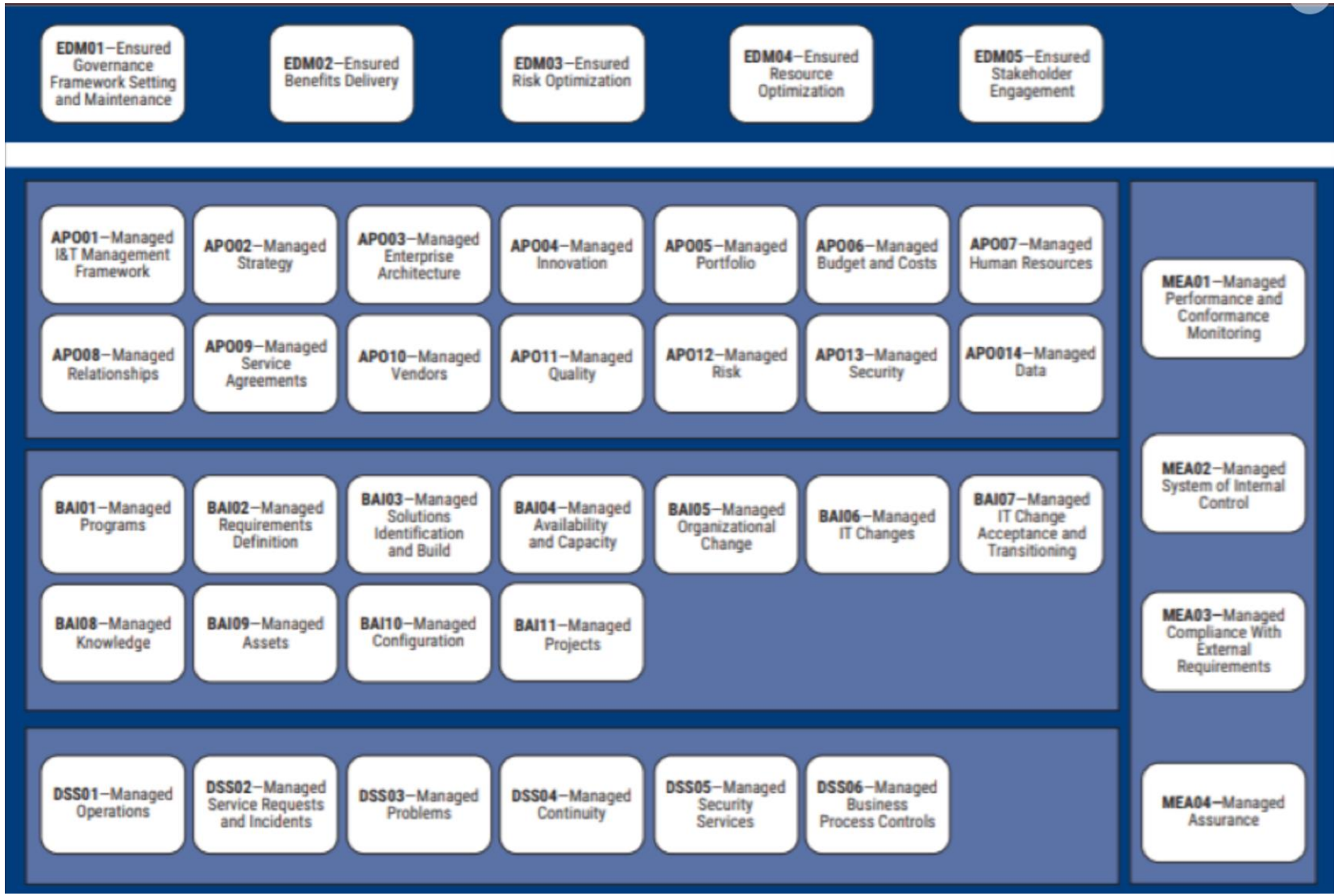
NIST SP 80- Guidelines:

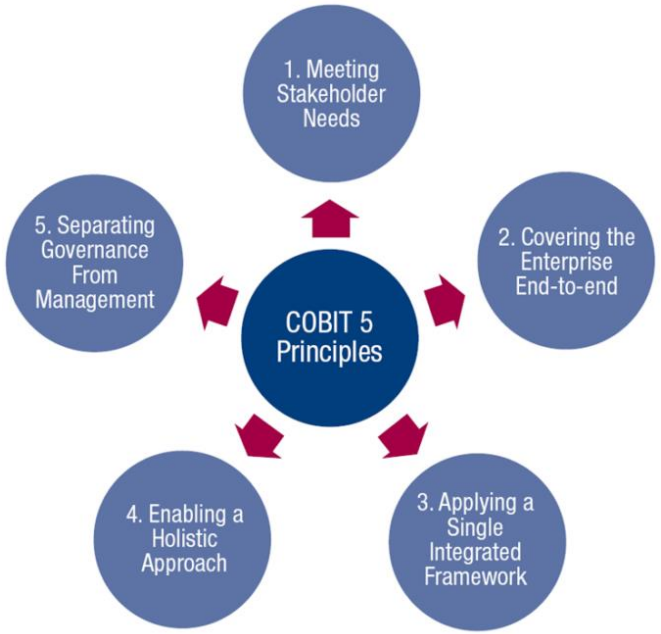
1. SP 800-60 – Categorization and Mapping of Information and Information Systems.
2. SP 800-53 – Security Control Selection and Implementation.
3. SP 800-30 – Risk Management.
4. SP 800-18 – Security Planning.
5. SP 800-37 – Security Control Assessment (Certification).
6. SP 800-37 – System Authorization (Accreditation).
7. SP 800-36 – Guide to Selecting IT Security Products.
8. SP 800-66 – HIPAA Implementation and Information Security.



COBIT 5 Framework (Integrating Business with IT)

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

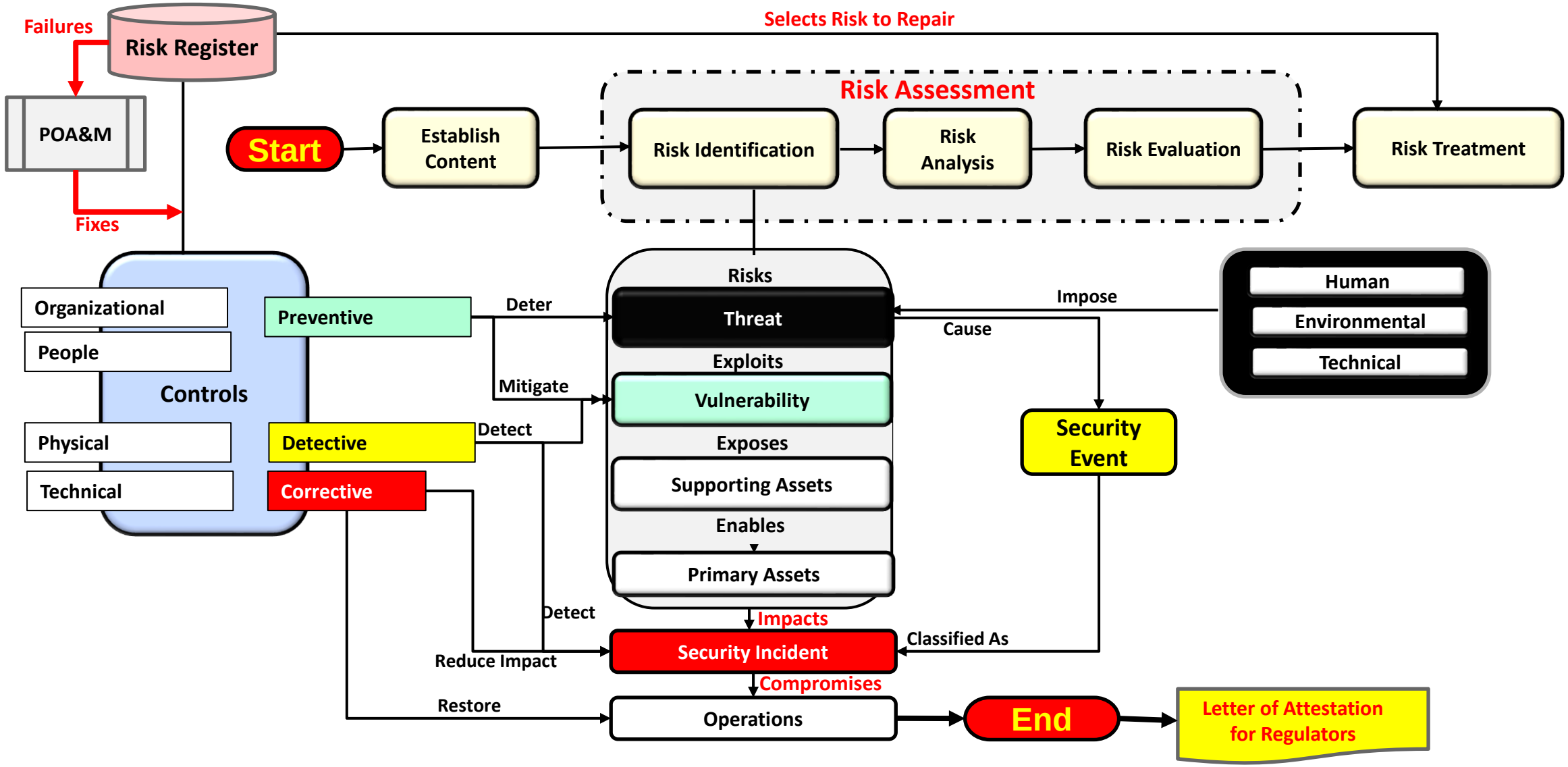




1. Metering Stakeholder needs.
2. Covering the Enterprise, end-to-end.
3. Applying a single integrated framework
4. Enabling a Holistic Approach
5. Separating Governance from Management

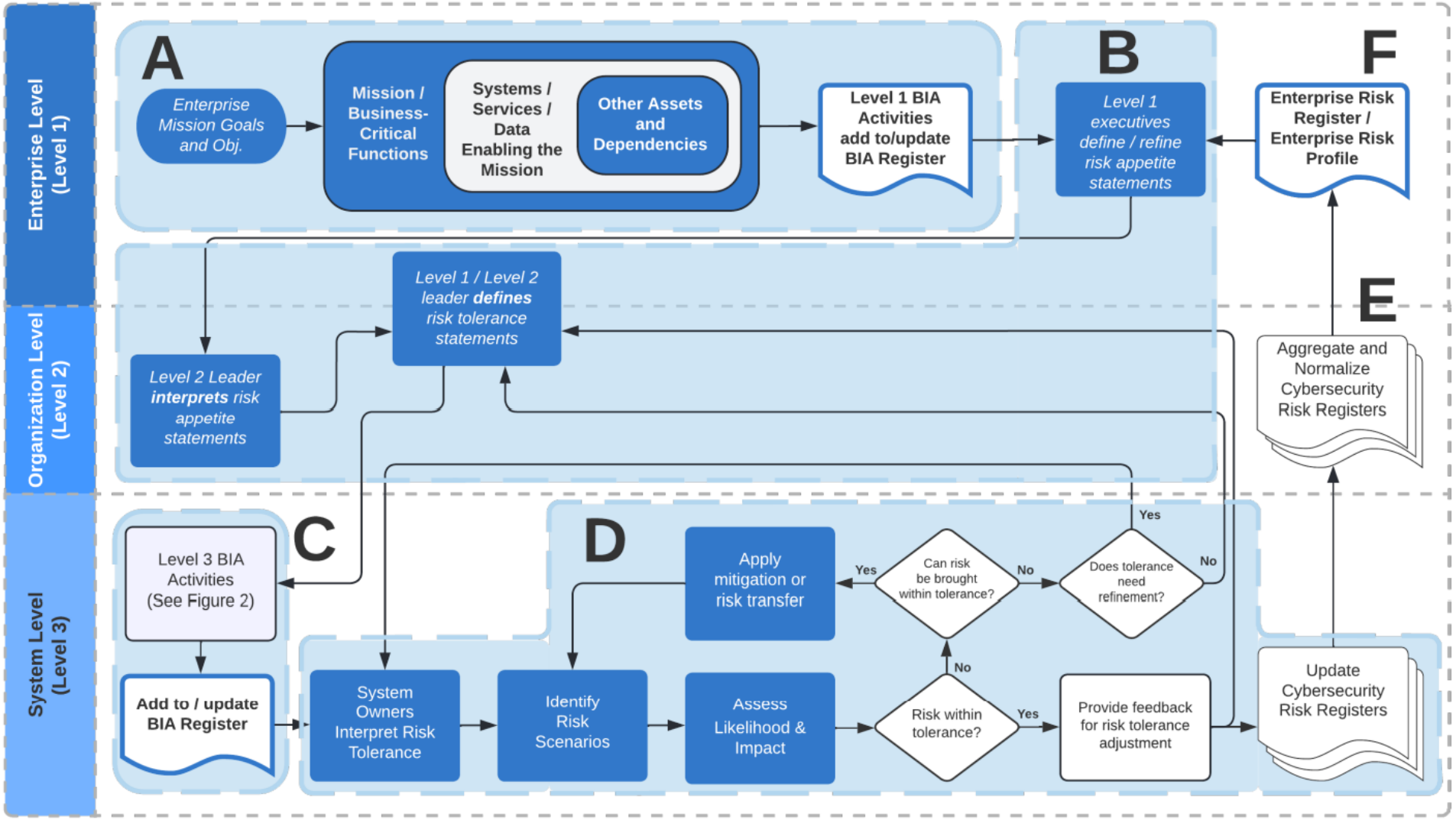
Risk Management with ISO 27000: 2022

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



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

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



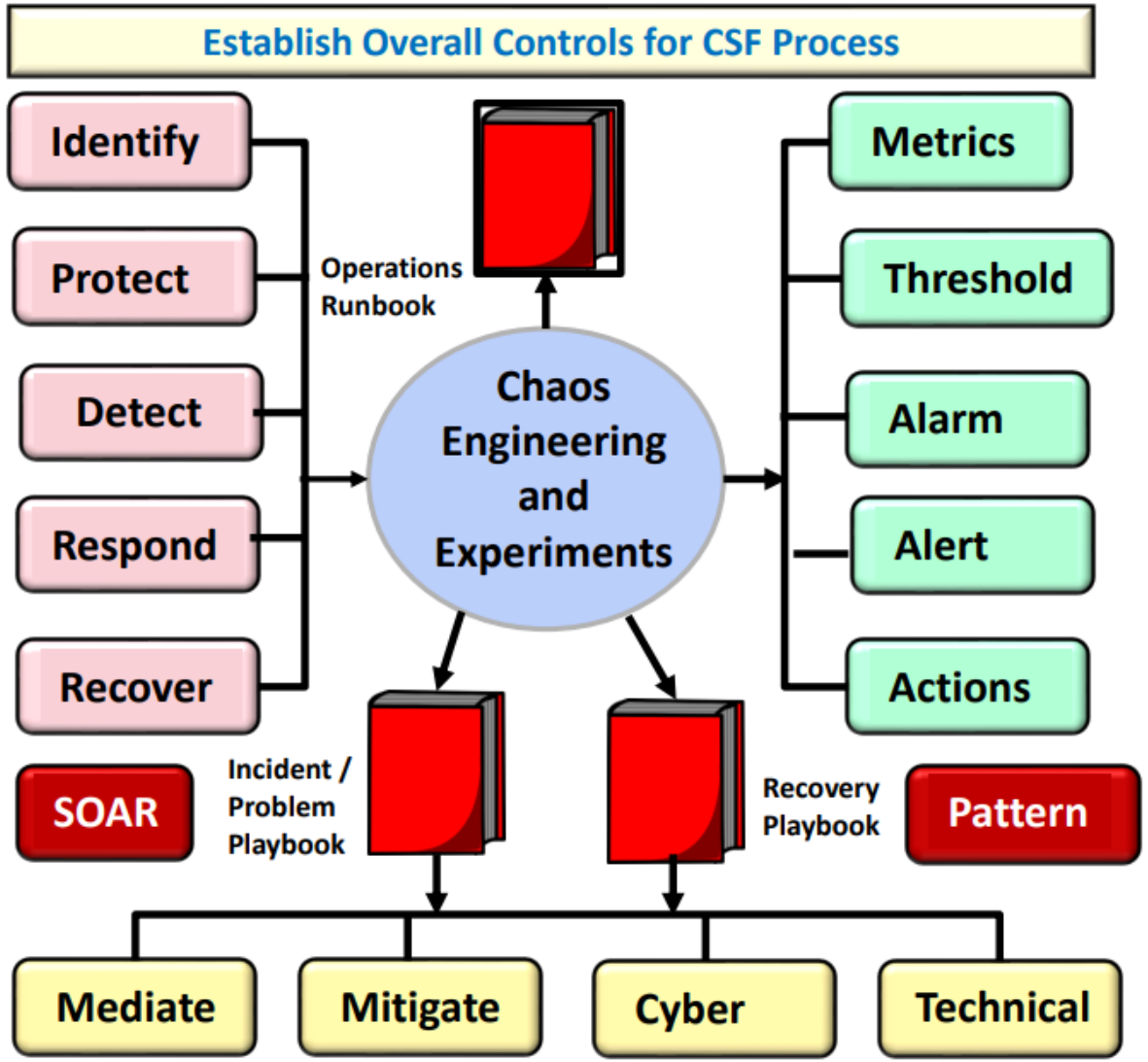
Link to Document

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

Detecting and Responding to Cyber Problems - CSF

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

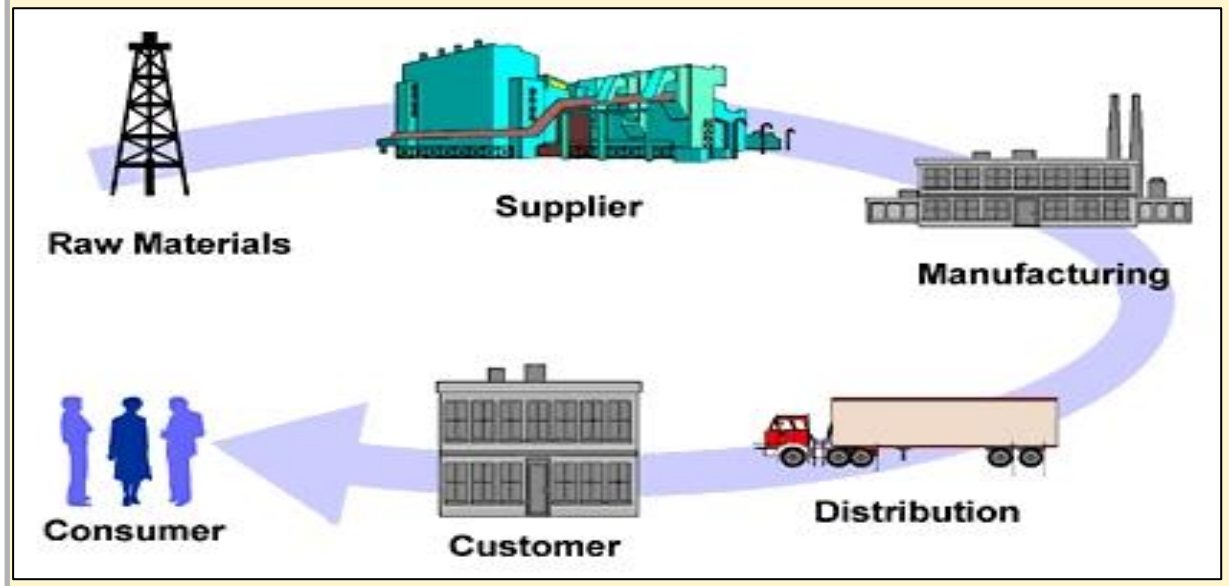
Function		Code	Category	Cybersecurity Framework (CSF)
Identify	ID	ID.AM	Asset Management	
		ID.BE	Business Environment	
		ID.GV	Governance	
		ID.RA	Risk Assessment	
		ID.RM	Risk Management Strategy	
		ID.SC	Supply Chain Risk Management	
Protect	PR	PR.AC	Identity Management and Access Control	
		PR.AT	Awareness and Training	
		PR.DS	Data Security	
		PR.IP	Information Protection Processes and Procedures	
		PR.MA	Maintenance	
		PR.PT	Protective Technology	
Detect	DE	DE.AE	Anomalies and Events	
		DE.CM	Security Continuous Monitoring	
		DE.DP	Detection Processes	
Respond	RS	RS.RP	Response Planning	
		RS.CO	Communications	
		RS.AN	Analysis	
		RS.MI	Mitigation	
		RS.IM	Improvements	
Recover	RC	RC.RP	Recovery Planning	
		RC.IM	Improvements	
		RC.CO	Communications	



Supply Chain Management - Physical Environment

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

- Supply Chain has international connections where raw materials are collected, and manufacturing achieved.
- Materials are transported to domestic market via ships, planes, and other means.
- Materials are delivered to suppliers and distributors who then deliver products to end clients.
- End client must be informed of supply chain interruptions so that alternative suppliers can be obtained.



- Customer must have contingency plans to address the loss of raw materials, suppliers, manufacturing, distribution, and delivery to customer locations.
- If disaster event require customer to move to secondary site, then supplier must be able to continue to supply materials to the secondary at the same desired rate.
- All “Single-Points-Of-Failures” in Supply Chain must be identified and alternatives created to protect business.
- National and International laws and regulations help achieve supply chain protection.

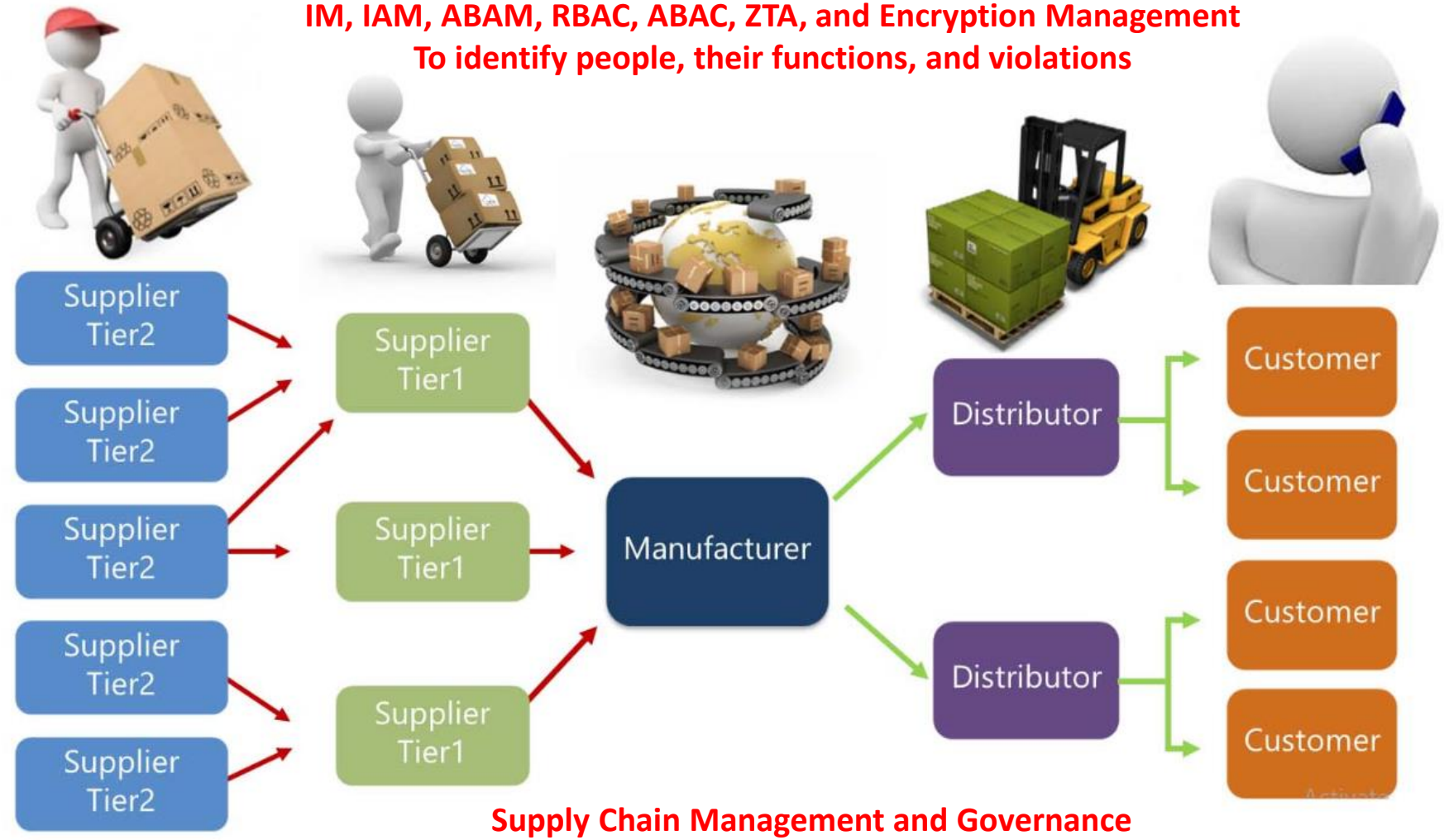
Supply Chain Verification and Certification

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

Supply Chain certification does not end at the primary vendor but includes subsequent vendors in the primary vendor's supply chain. Any of these vendors could suffer a catastrophic disaster or use banned providers or locations in violation of acceptable laws.

This is evident in the SolarWinds Orion catastrophe, where many companies were affected by a single breach event.

Consider using AI, ML, RPAs, or automated tools to assist in Supply Chain Management.



SBOM – Software Supply Chain

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

Process & Usage:

1. Generate SBOM.
2. Validate all vendors and Components for vulnerabilities.
3. Review Vulnerabilities.
4. Either update release or install Patch to repair vulnerability, prior to entering the production environment.
5. Pass UAT and PAT to enter Production with an Authorization To Operate (ATO).
6. Add SBOM to SBOM Repository so searches can identify all applications where component is used.

Critical Insights for SBOM Management

Critical Insights

- SBOMs are a critical element of software supply chain management.
- SBOMs are here to stay.
- SBOM technologies are evolving rapidly.

Impacts on Product Leaders

- Protect the integrity of the software supply chain by combining SBOM data with a robust software vulnerability management strategy.
- Identify the demands and dynamics of SBOM disclosures that may differ from one industry to another.
- Focus on ways to integrate and leverage SBOM technologies and techniques into broader digital business strategies.

Software Suppliers and component information to create a Software Bill of Materials and check for vulnerabilities (CVEs*).

*CVE is Common Vulnerability Enumeration
SBOM – Software Bill Of Materials.

See EO 14028 for Details

Repair Vulnerabilities prior to Production and maintain an inventory of all application software components. Use cross application index to identify component usage across applications.

Levels of Security Protection

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

New User
- Identity Papers
- Biometrics

Levels of Authorization

Identity Management (IM)
- Identity Papers
- Biometric Information
- Profile
- ID Card
- Learning Skills Matrix (LSM)

Identity Access Management (IAM)
- Job Title
- Functional Responsibilities
- Physical Location Restrictions
- ID Card Restrictions

Role Based Access Control (RBAC)
- Based on Title
- Group Association
- CRUD Identification
- Job Title Access Profile

Multi-Factor Authentication (MFA)
- Userid
- Password
- Call-Back, PIN
- Secondary Validation

Attribute Basses Access Control (ABAC)
- Machine Identification
- Machine Authorization
- Knowledge of User Location for verification

Zero Trust Authentication (ZTA)
- Combines RBAC, ABAC, & MFA
- Uses Certificates with IAM
- User Session only, then reapply

IM User Profile
- Data Base Profile
- ID Card

IAM User
- Job Title
- Functional Responsibilities
- Authorized Locations
- Restrictions

RBAC Profile
- Job Title
- Group
- CRUD
- Access Profile

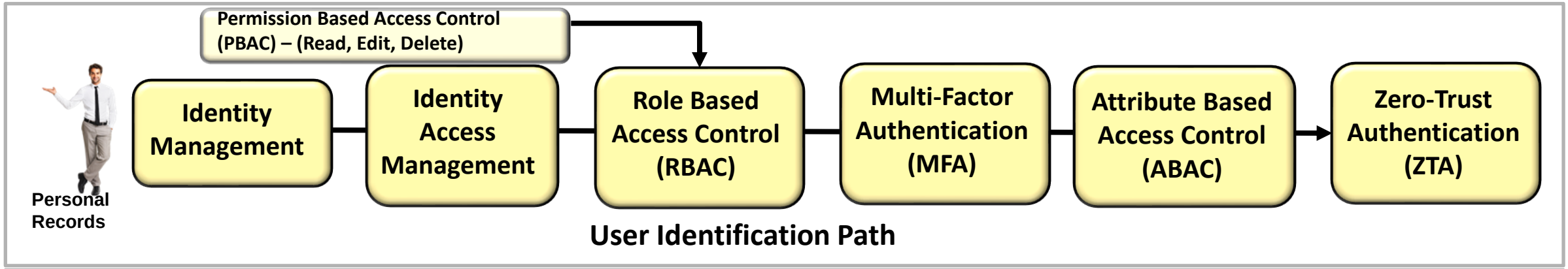
MFA Profile
- Userid / Pswd
- Secondary Validation
- PIN, Call Back

ABAC Profile
- Machine
- Location
- Authorization

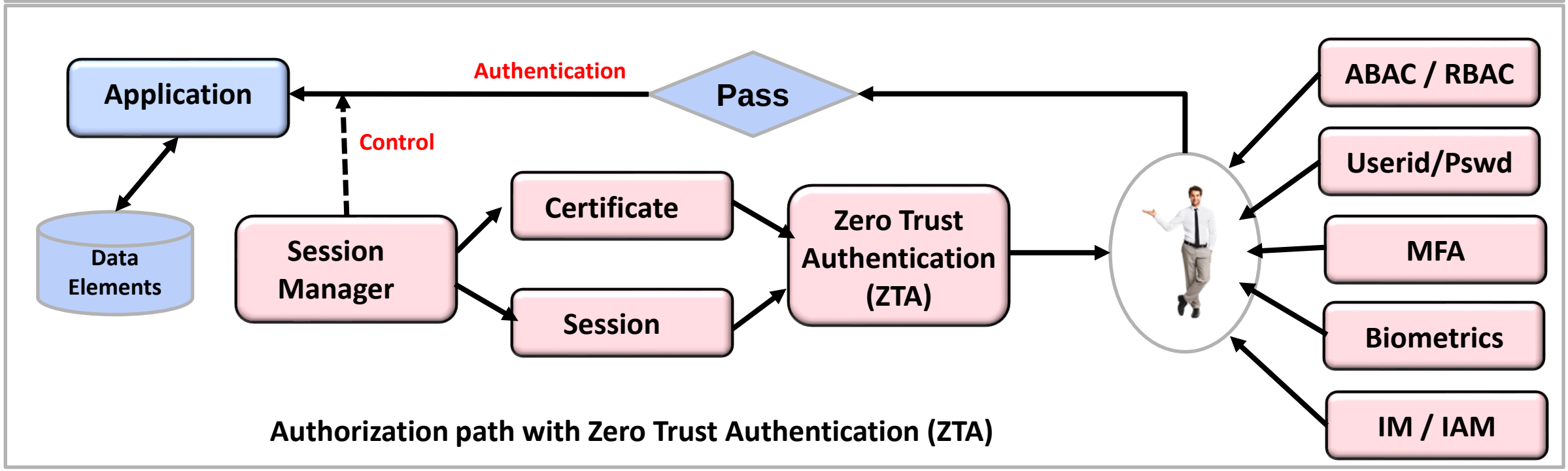
ZTA Profile
- RBAC, ABAC, & MFA
- Certificates
- Session Manager
- Single Usage

Identity and Access Management technologies

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



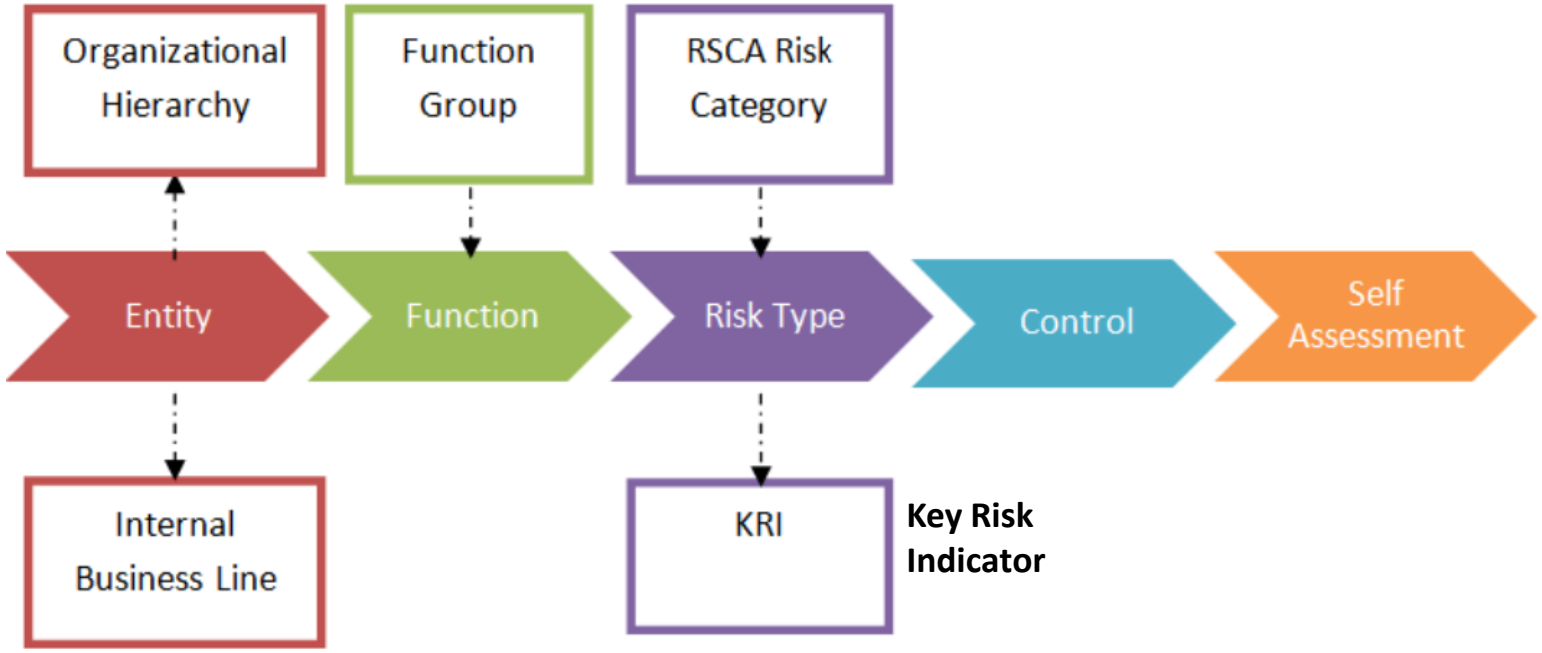
User Identification Path



Authorization path with Zero Trust Authentication (ZTA)

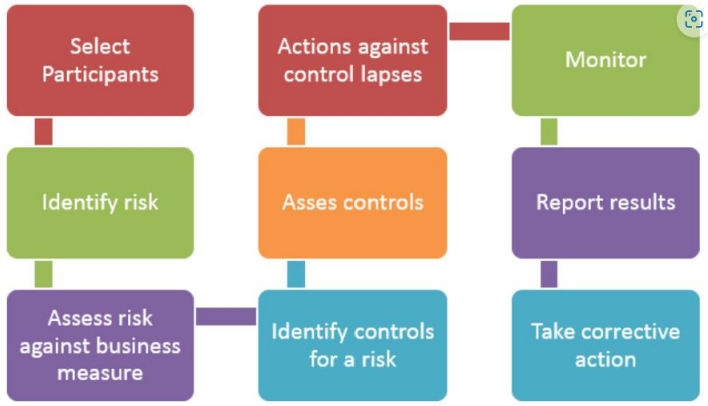
Risk Control Self Assessment (RCSA)

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



Steps within a RCSA are:

1. Select Participants
2. Identify Risks
3. Assess Risk aginst business measure
4. Actions against control lapses
5. Access Controls
6. Identify controls for a risk (KRI)
7. Monitor
8. Report results
9. Take corrective actions to continuously improve process



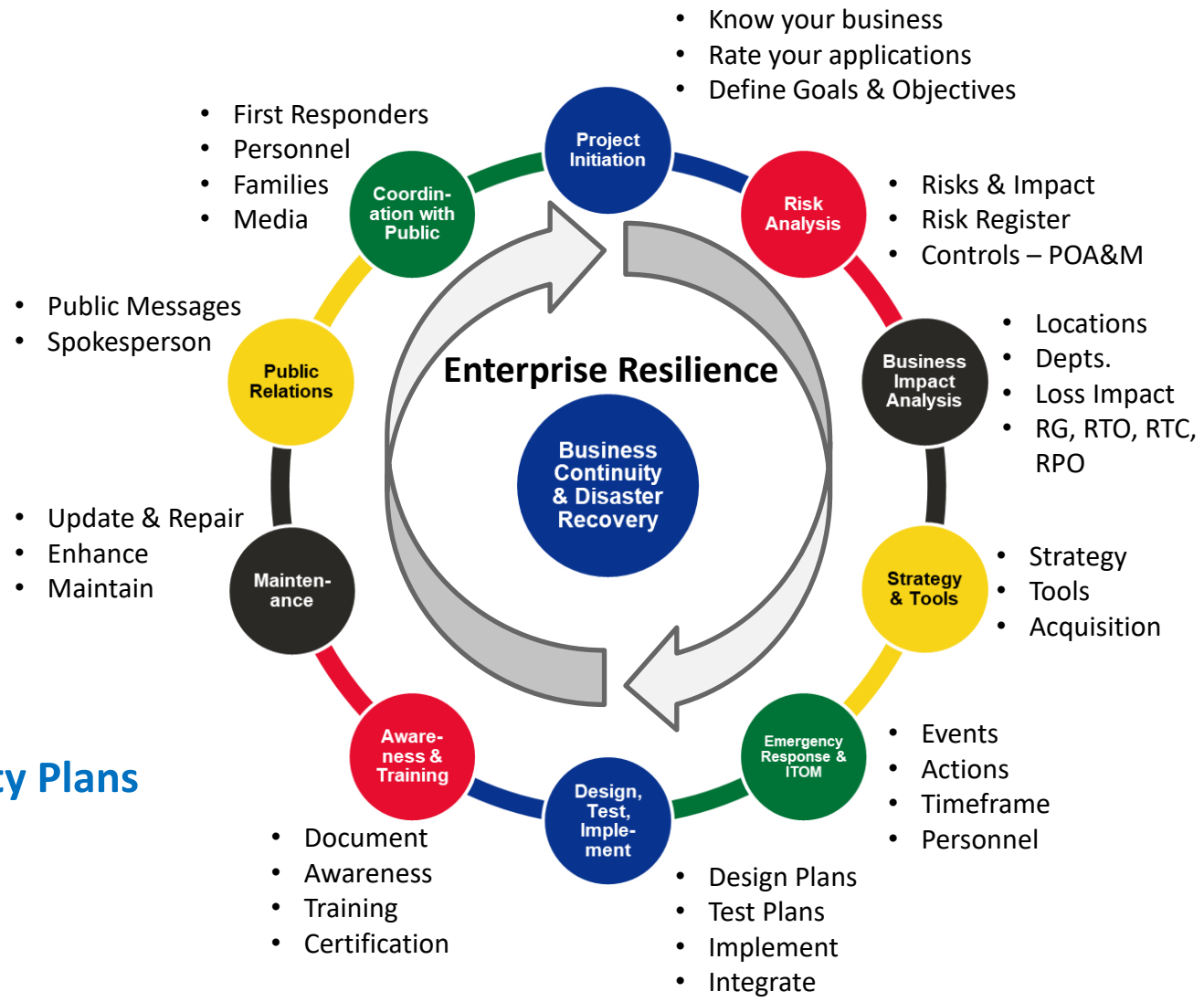
RCSA (Risk Control Self Assessment) is an empowering method/process by which management and staff of all levels collectively identify and evaluate risks and associated controls. It adds value by increasing an operating unit's involvement in designing and maintaining control and risk systems, identifying risk exposures and determining corrective action. The aim of RCSA is to integrate risk management practices and culture into the way staff undertake their jobs, and business units achieve their objectives. It provides a framework and tools for management and employees to:

- Identify and prioritize their business objectives
- Assess and manage high risk areas of business processes
- Self-evaluate the adequacy of controls
- Develop risk treatment action plans
- Ensure that the identification, recognition and evaluation of business objectives and risks are consistent across all levels of the organization

Ten Step Process to establish BCM/DR Practice

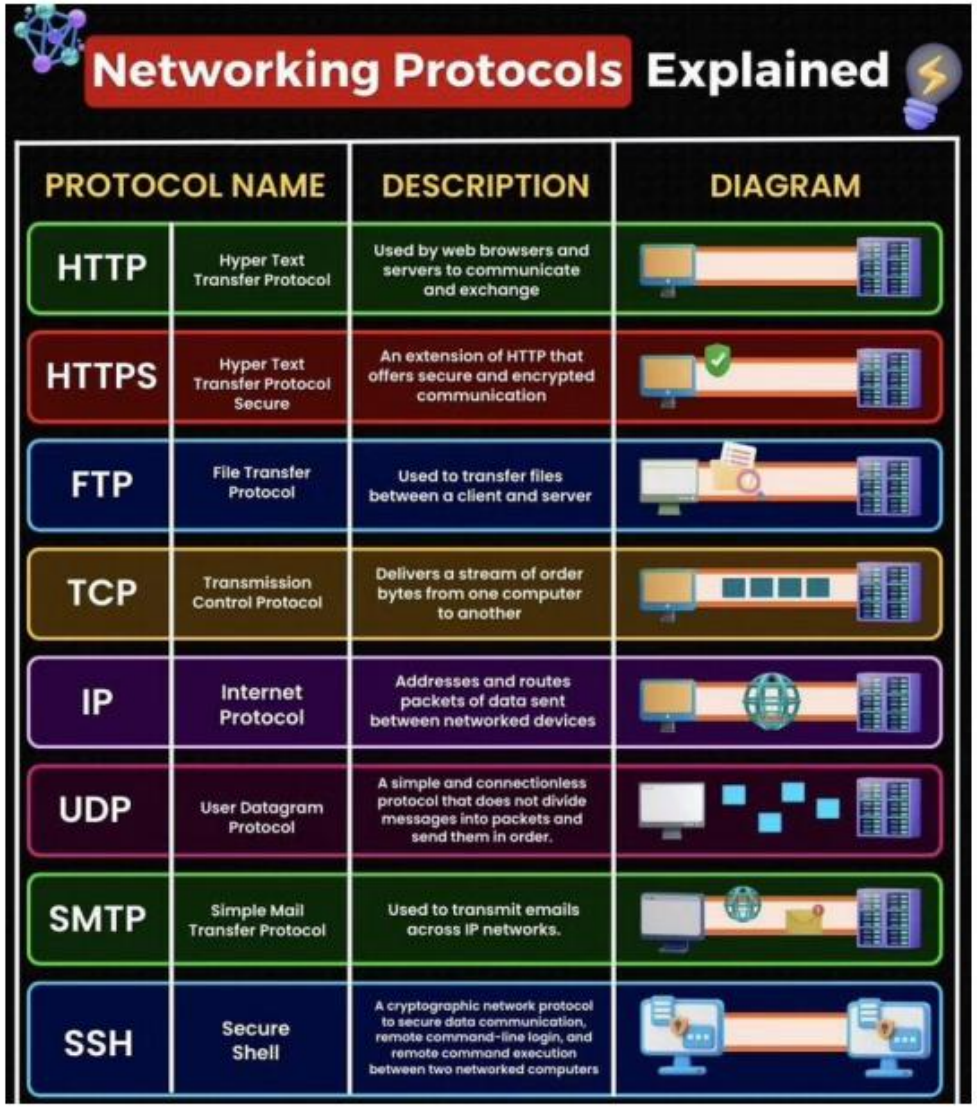
Thomas Bronack
Email: bronackt@gmail.com
Phone: (917) 673-6992

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
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



Communications Protocols & Seven Layer Model

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

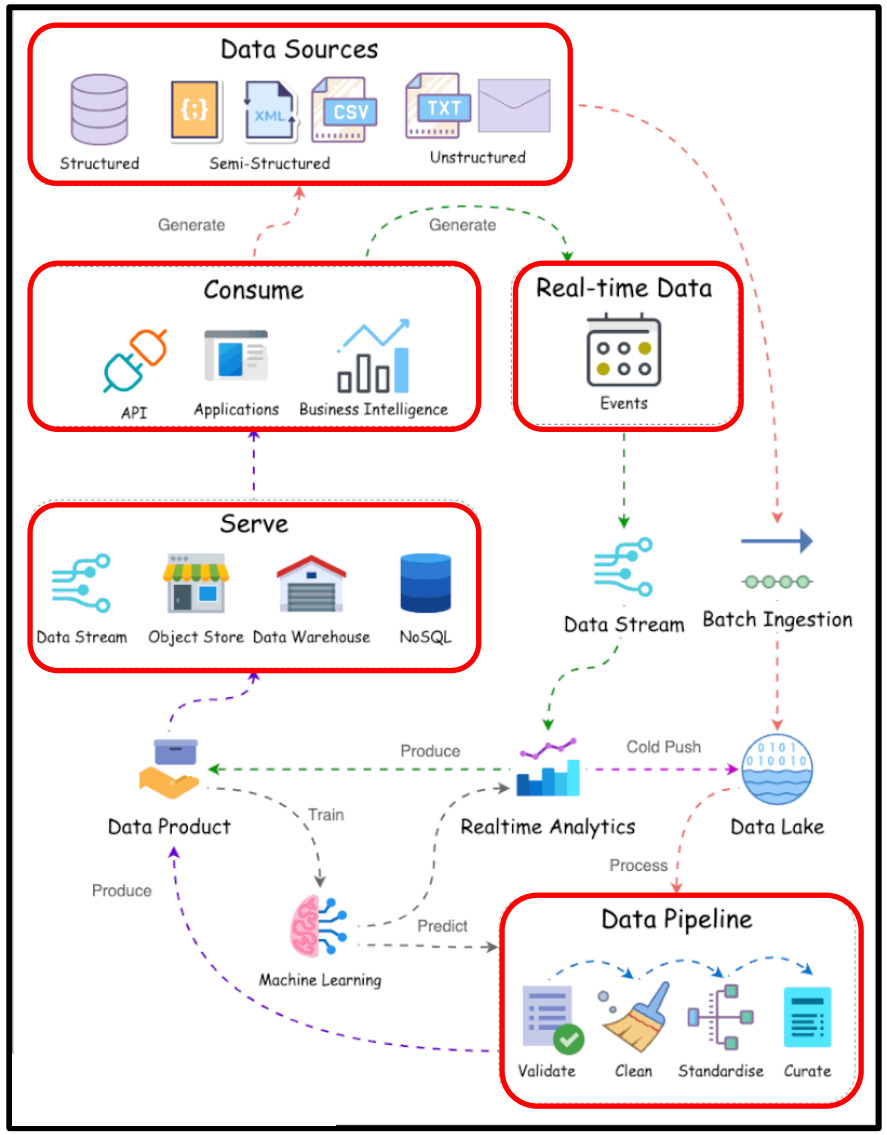


Layer	Application / Example	Central Device / Protocols		DOD4 Model
Application (7) Serves as the window for the user and application processes to access the network services.	**End User Layer** – Program that opens what was sent ot creates what is to be sent • Resources sharing, Remote File Access, Remote Printer Access, Directory Services, Network Management	User Applications SMTP	Gateway (Can be used on all layers)	Process
Presentation (6) Formats the data to be presnted to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax Layer** – Encrypt & Decrypt (if needed) • Character Code translation, data conversion, data compression, data encryption, data set translation	JPEG / ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** – (Logical Ports) • Session establishment, maintenance and termination, Session support – perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS Names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** – Host to Host, Flow Control • Message segmentation, Message acknowledgement, Message traffic control, Session multiplexing	Packet Filtering	TCP/SPX/UDP	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** – ("letter", Contains IP Address) • Routing, Subnet traffic control, Frames fragmentation, Logical – physical address mapping, Subnet usage accounting		Routers IP/IPX/ICMP	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("Envelope", contains MAC address) (NIC Card – Switch – NIC Card), (end-to-end) • Establishes & terminates the logical link bewtween nodes, Frame trffic control, Frame sequencing, Frame acknowledgement, Frame delimiting, Frame error checking, Media access control		Switch Bridge WAP PPP/SLIP (Land Based Layers)	Network
Physical (1) Concerned with the transmission and reception of the unstructures raw bit strean over the physical medium.	**Physical Structure** (Cables, hubs, etc.) • Data encoding, Physical medium attachment, Transmission Technique, Baseband or Broadband, Physical medium transmission Bits & Volts		Hub	

End User
Application
Data Format
Presentation
Data Sync to Ports
Session
Host to Host - Flow
Transport
Packets over Network
Network
Link Control - Tunnel
Data Link
Network Connections
Physical

Data Flow and Internet Routing Policies

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

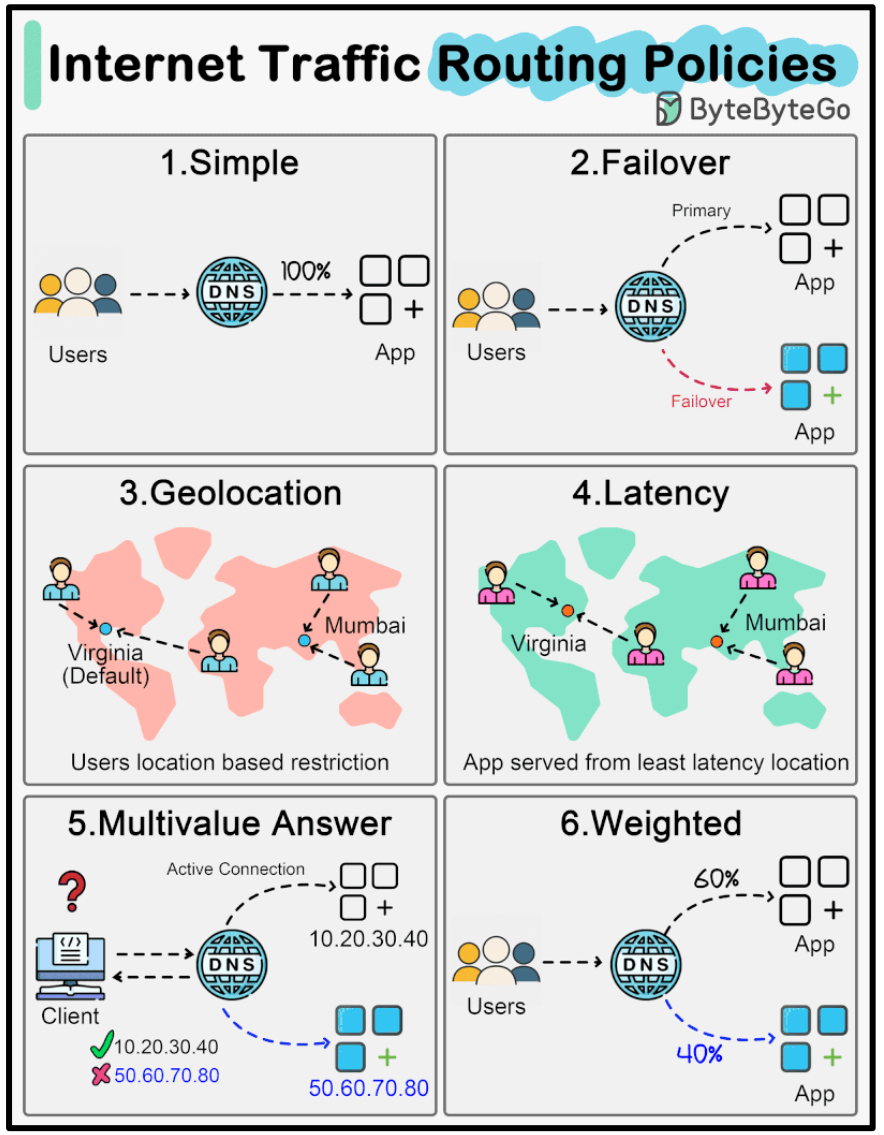


Data Flow:

1. Data starts and ends at the consumer in real-tie or batch mode.
2. Data lakes can store all types of data for analysis and can archive data (Freeze), recall data (Thaw), or use current data.
3. Data pipeline consists of receiving data, validate data, clean data, standardize data, and create data
4. After Pipeline data is used for products, machine learning for AI, real-time analysis, predictions, and data lake storage. Data is provided to consumers via servers.

Internet Traffic Routing Policies:

Use to control the flow of data to remote locations through the internet.



Building and Implementing an Application

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

Programmers:
- Development
- Test
- Maintenance

Develop once, maintain many

Development

User Request

- User Requests Application by providing a "Requirements Definition"
- Business Reason Defined
- Asset Definition Management (ADM)
- Data Sensitivity performed
- Data Handling & Retention
- Identity Management (IM)
- Identity Access Management (IAM)
- Business Needs Analysis
- Technical Needs Analysis
- Requirements Analysis
- Configuration Management
- Decision for Buy / Build
- Risk Management
- Interface Management
- Data Management
- Vital Recrds
- Recovery Management

TECHNICAL MANAGEMENT PROCESSES

- Technical Planning
- Requirements Management
- Configuration Management
- Technical Assessment
- Decision Analysis
- Risk Management
- Interface Management
- Data Management

TECHNICAL PROCESSES

- Requirements Development
- Logical Analysis
- Design Solution
- Design Processes
- Realization Processes
- Transition
- Validation
- Verification
- Integration
- Implementation
- Test

SELC **SDLC**

Maintenance

Enhance, Or Fix Problems

Change

Maintenance

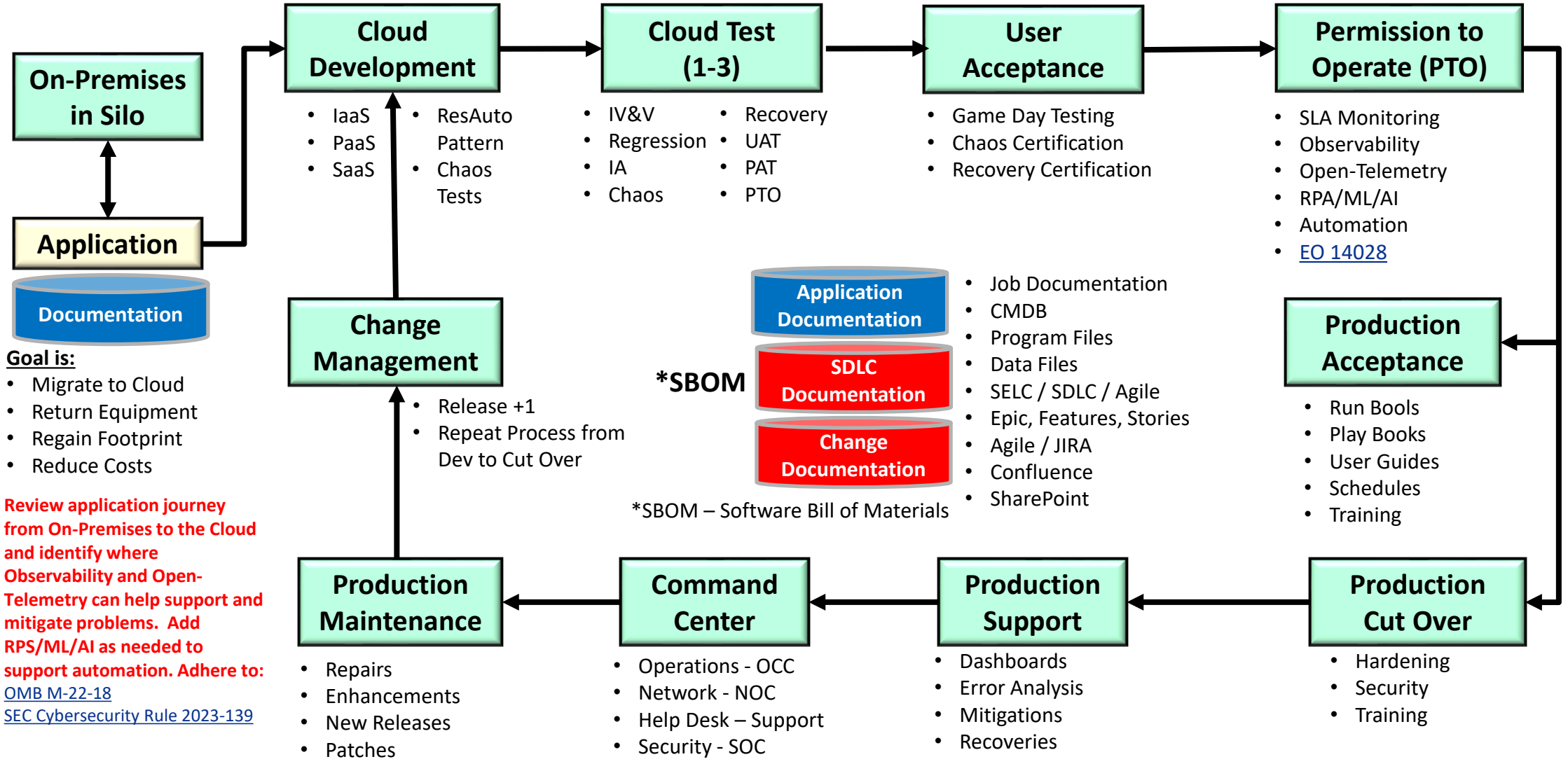
Fix Problems, Update Releases, Enhancements

Domains

- **Sandbox** — *Learn on current release*
- **Development** — *Build*
- **Testing** — *Test Requirements*
- **Recovery** — *Validate Recovery*
- **Acceptance** — *User Accepts*
  EO 14028
- **Production** — *Production Accept*
- **Integration** — *ATO - Staff Operations*
- **Support** — *Tech Problems Cyber Incidents*

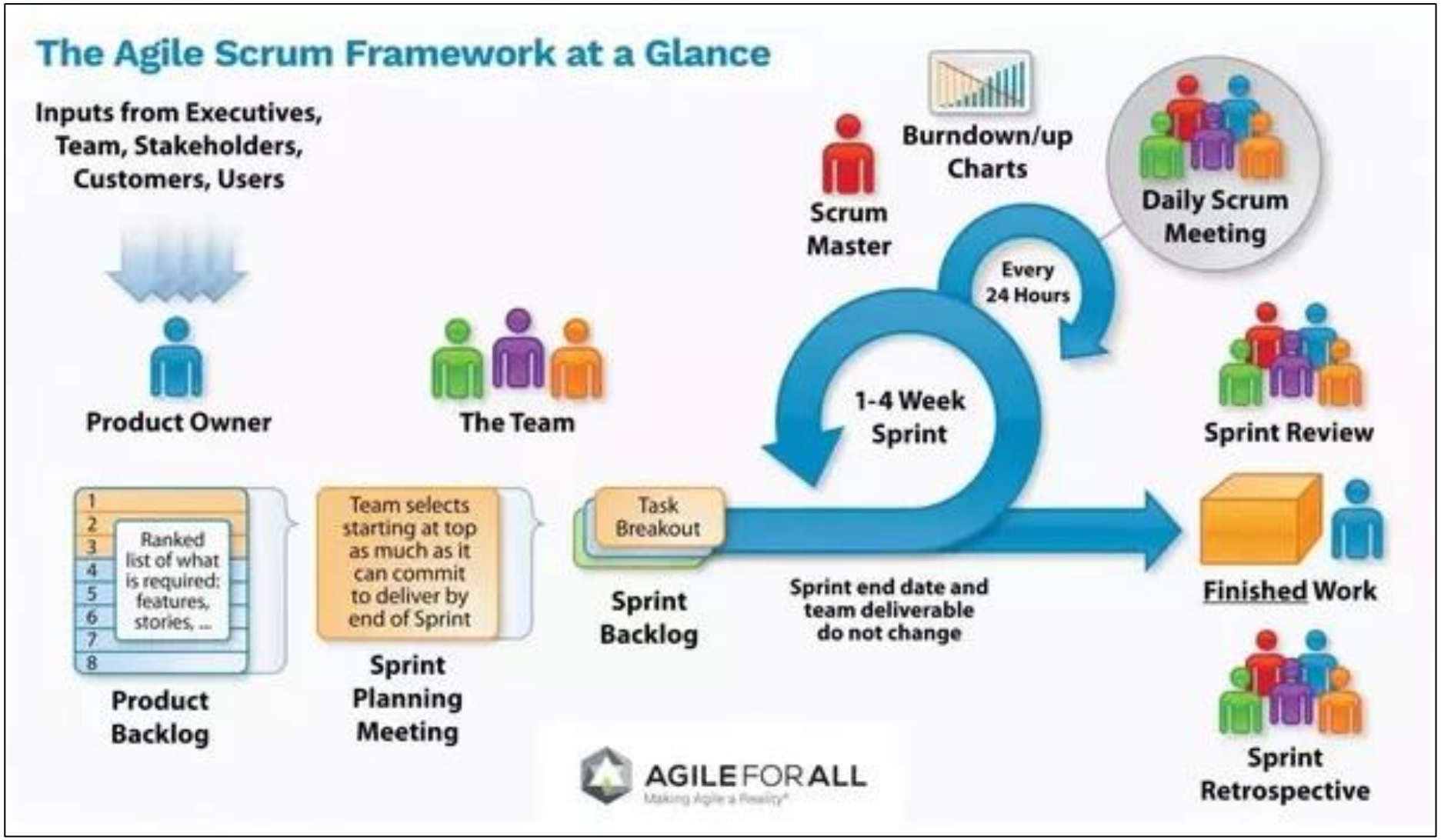
Migrating Applications to the Cloud

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



Agile vs Waterfall Systems Development

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

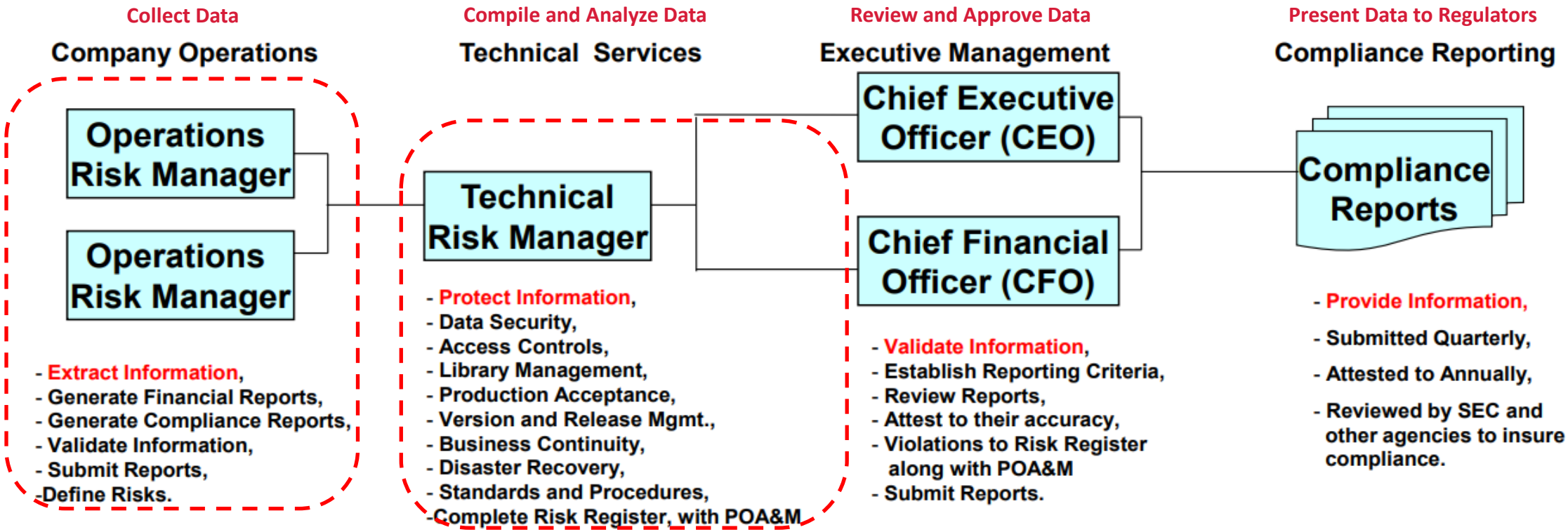


- Conception
- Initiation
- Analysis
- Design
- Construction
- Testing
- Deployment

Waterfall Model

Continuous Compliance Reporting

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

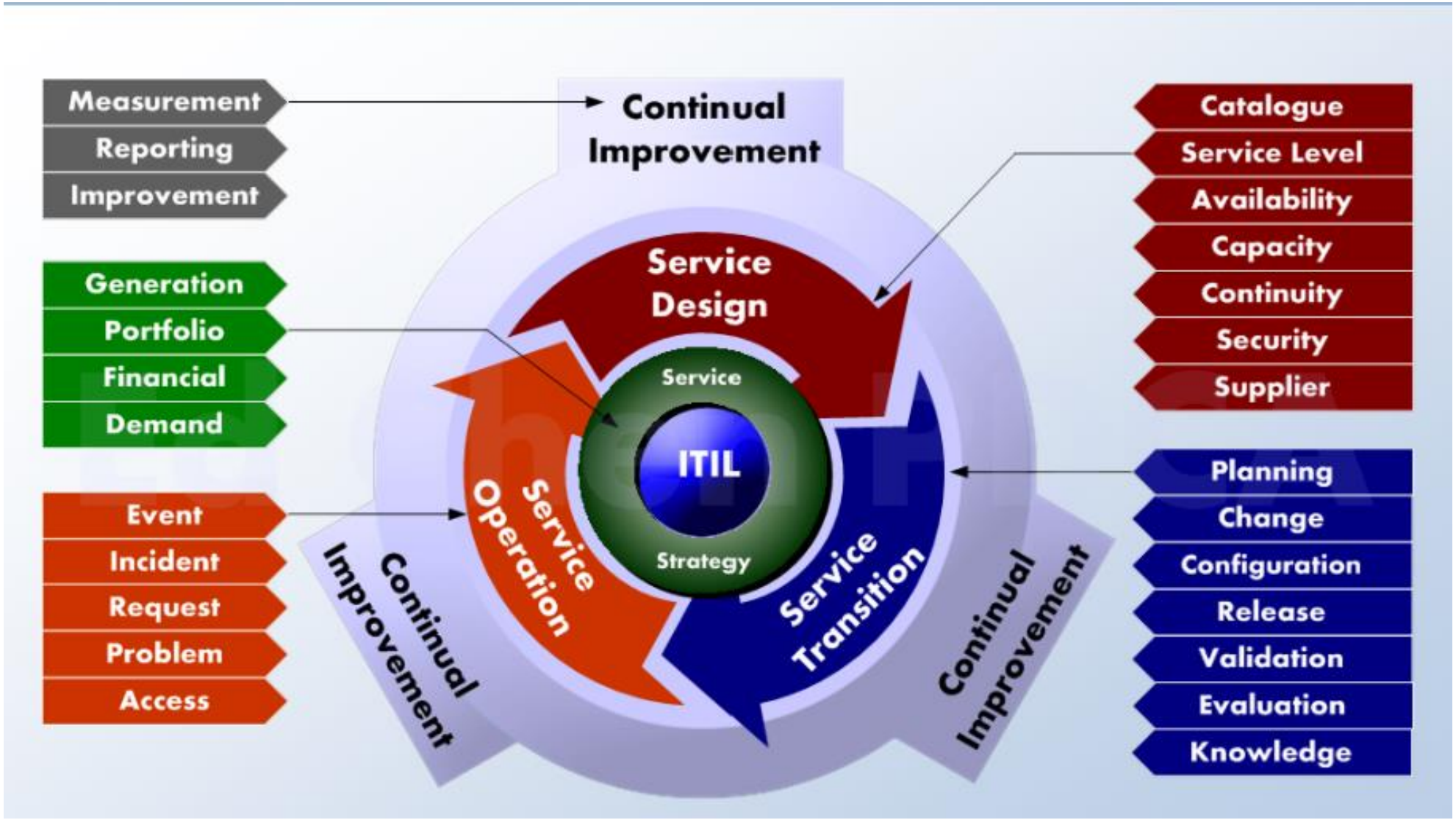


Auditing Process:

- 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

Information Technology Infrastructure Library (ITIL)

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



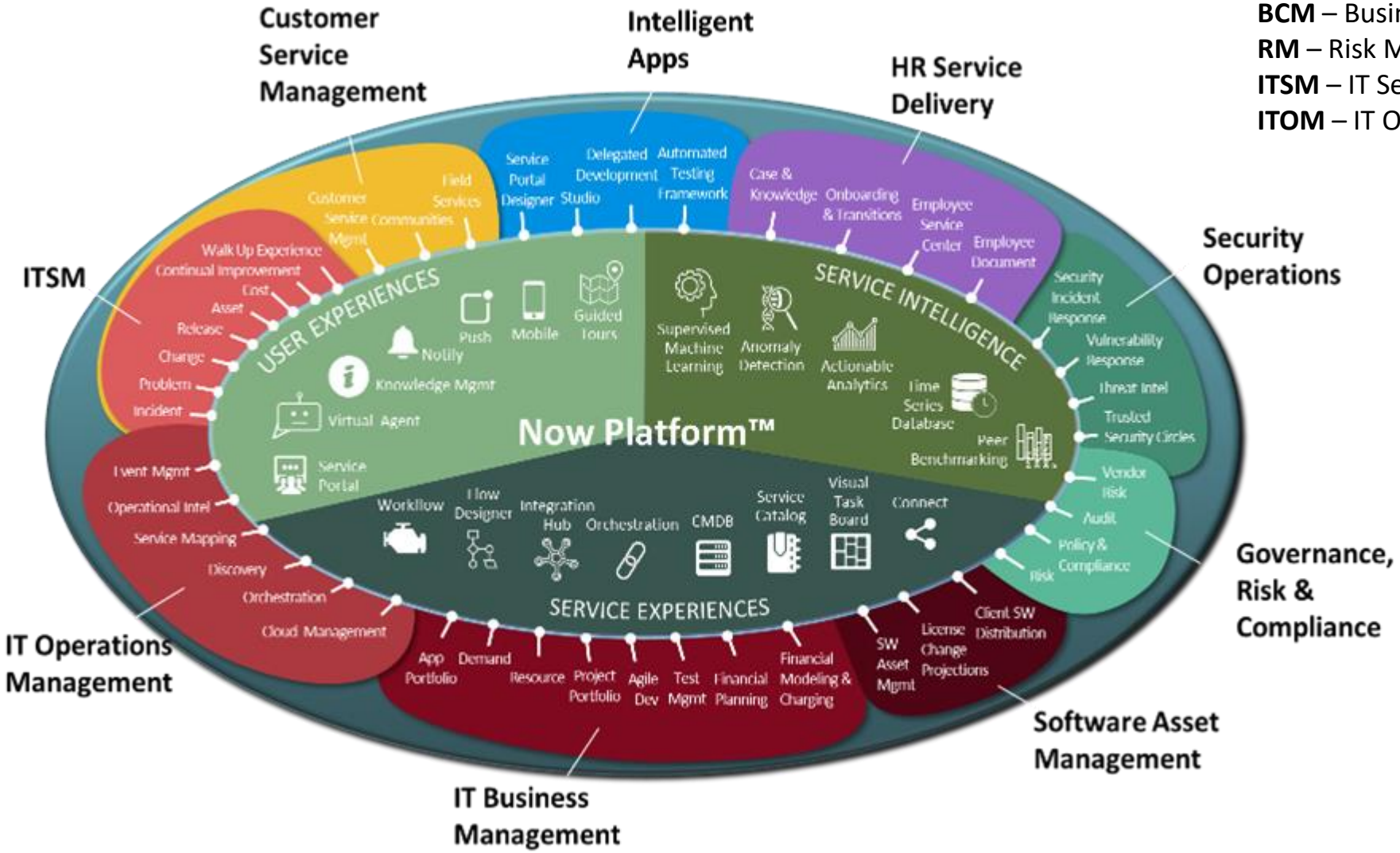
ITIL assists in:

- 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

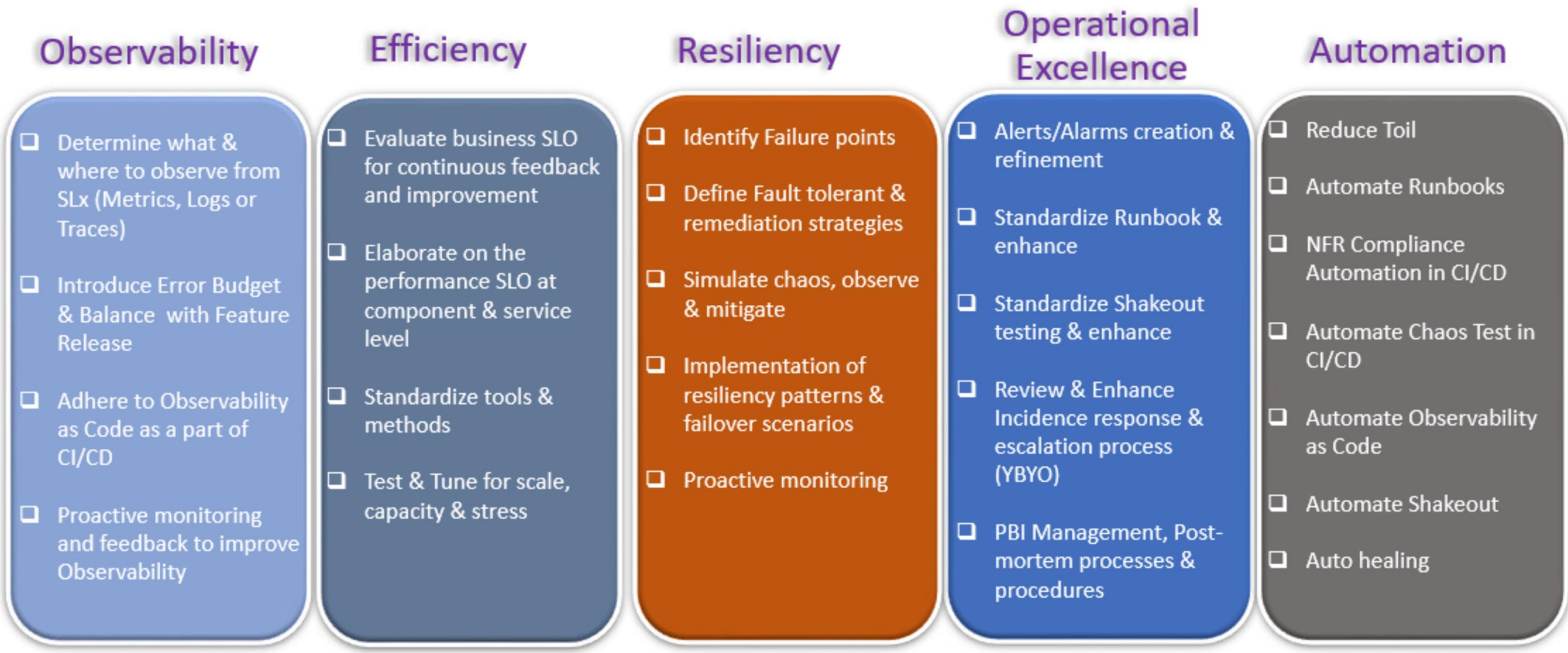
Thomas Bronack
Email: bronackt@gmail.com
Phone: (917) 673-6992

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



Five Pillars of Site Reliability Engineering (SRE)

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



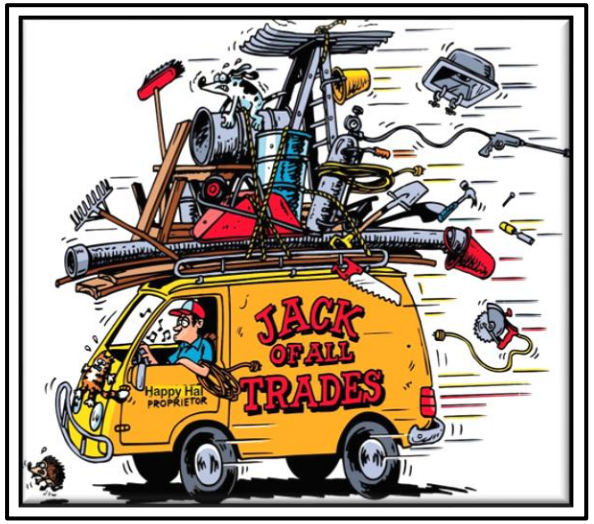
[Google – Site Reliability Engineer Handbook]

NFR – Non-Financial Reporting

Tom Bronack– A strong Generalist

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

My background is comprised of technical, managerial, sales, and consulting with experience implementing safeguarded environments that comply with business/regulatory requirements. Skilled in Enterprise Resiliency and Corporate Compliance Certification, Risk Management, Operations Analysis, creating Disaster Recovery and Business Continuity plans, integrating process improvements within standards and procedures governing business operations and personnel accountability, adept in planning and improving the efficiency of data processing systems/services; optimizing information technology productivity through system implementation, quality improvements, technical documentation, and Dashboards. Excellent communications and personnel interfacing skills as Team Member or Lead.



Selected Accomplishments

- Provided data center builds, migrations, consolidations, and termination services.
- Defined and conducted Asset Management services for equipment acquisitions, redeployment, and termination.
- Led, conducted, and performed IT Technology and Security Risk Assessments / Audits for regulator attestation and Risk Eliminations (Risk Register with POA&M that mitigates. or mediates, problems associated with Risks).
- Implemented Business Continuity Plans for major organizations in the Banking, Brokerage, Insurance, Service and Product Vendors, Pharmaceutical, Manufacturing, and international industries utilizing best practices and virtualization techniques.
- Designed and implemented High Availability and Continuously Available environments for a major bank to meet recovery RTO and RPO discovered via BIA assessments and Recovery Group definitions. Categorized Applications and Services as Critical t Revenue, Operations, or Brand with Risk Group.
- Sales Agent for IBM Business Recovery Services, bringing Chase, Citibank, and Salomon Brothers in as potential clients.
- Sales Agent for Diversified Software Systems, Inc. (DSSI) selling Docu/Text and Job/Scan products and provided professional services to clients.
- Provided consulting services to established offsite vaulting and recovery facilities for clients (both business and IT) and assisted in implementing an automated file vaulting and recovery management system (automated vaulting system).
- Created first Computer Risk Management Department for a bank, then created first data center recovery center with Comdisco at a joint site in NJ.
- Created Security Pacific Risk Asset Management (SPRAM) and Total Risk Management (TRM) company as a subsidiary to Security Pacific Bank.
- Conducted a one-year audit of Midland Bank in England for Computer Science Corporation and reported to bank president.
- Created Five-Year Business Plan for Information Technology Division of European America Bank.
- Merged ADP Proxy and IECA into new $9.3 million facility, while consulting directly to Brokerage Division President.
- Sr. Systems Developer on team creating DHS CDM Dashboard for detecting cyber-crimes and technology threats in near real-time for entire US Government.
- Created Management Dashboard system for Infrastructure, SDLC, BCM, and Compliance and used system to finalize project for manufacturing company.
- Designed Electronic Voting System based on “One Person – One Vote:” using biometrics to eliminate fraud and corruptions, and blockchain to eliminate data tampering and ensure system guaranteed data integrity, security, accessibility, and audit ability.
- Implemented problem/incident management systems based on metric thresholds, alarms to capture anomalies, alerts to notify component owners, and actions performed by component owners to fix problem and update documentation as needed.
- Developed and presented educational classes on Business Continuity, IT/DR, and general Information Technology topics including developing and instructing the BCP – IT/DR course for the Disaster Recovery Institute International (DRII).

- Enterprise Resilience,
- Corporate Certification,
- Risk Assessment,
- Business Impact Analysis,
- Business and Disaster Recovery,
- Project Management,
- Team Leadership,
- Training & Awareness,
- Optimization & Compliance