Created by:

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

Thomas Bronack
Service Offering

Enterprise Resiliency

Including

Site Reliability Engineering

with

Tom Bronack

Business Continuity, IT Disaster Recovery, Business Location Recovery, 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, and Risk / Audit 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.

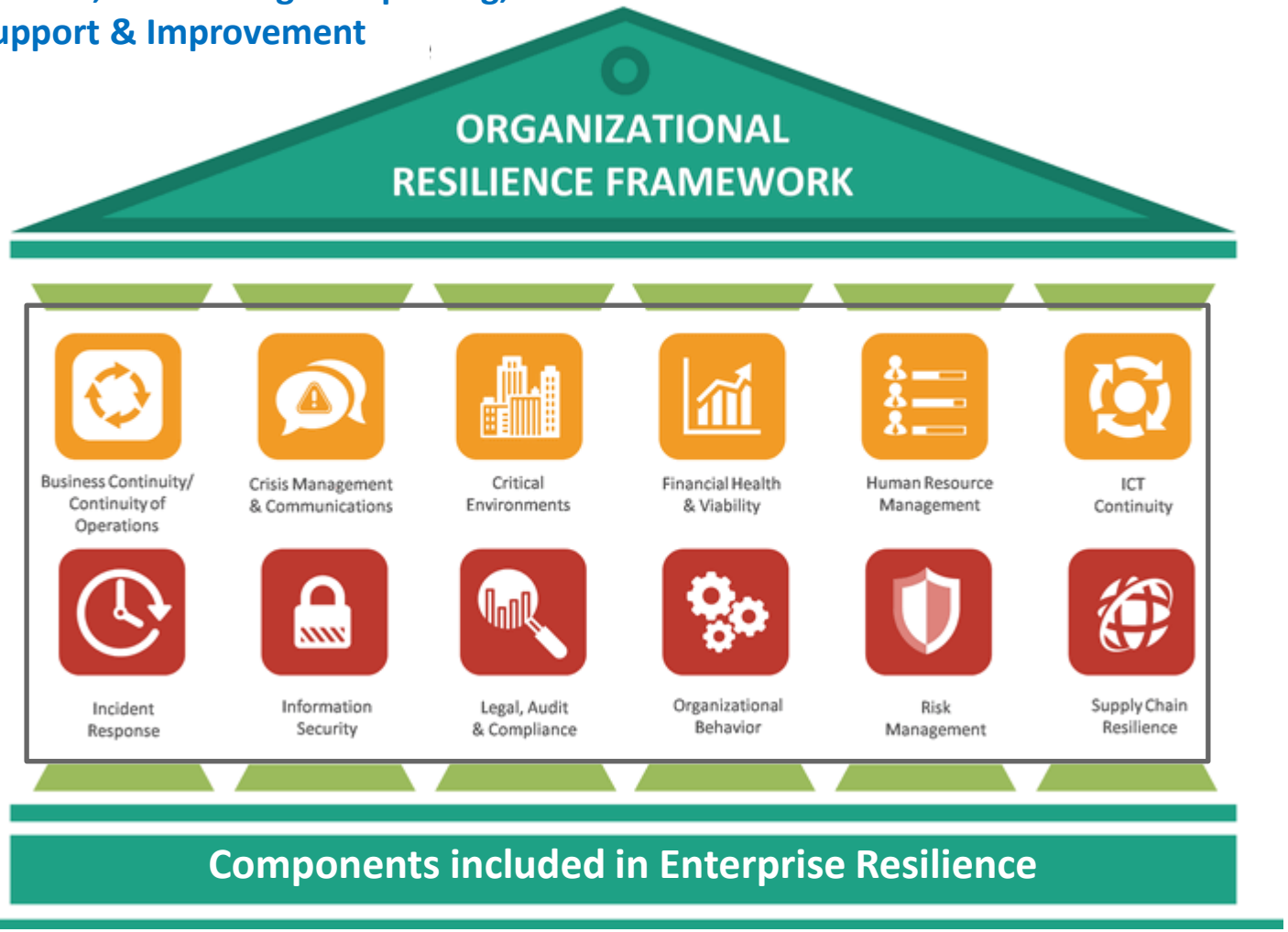
Cloud Migration, Resilience, & DR Planning to reduce costs, optimize service, and provide recovery services.

- **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

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.

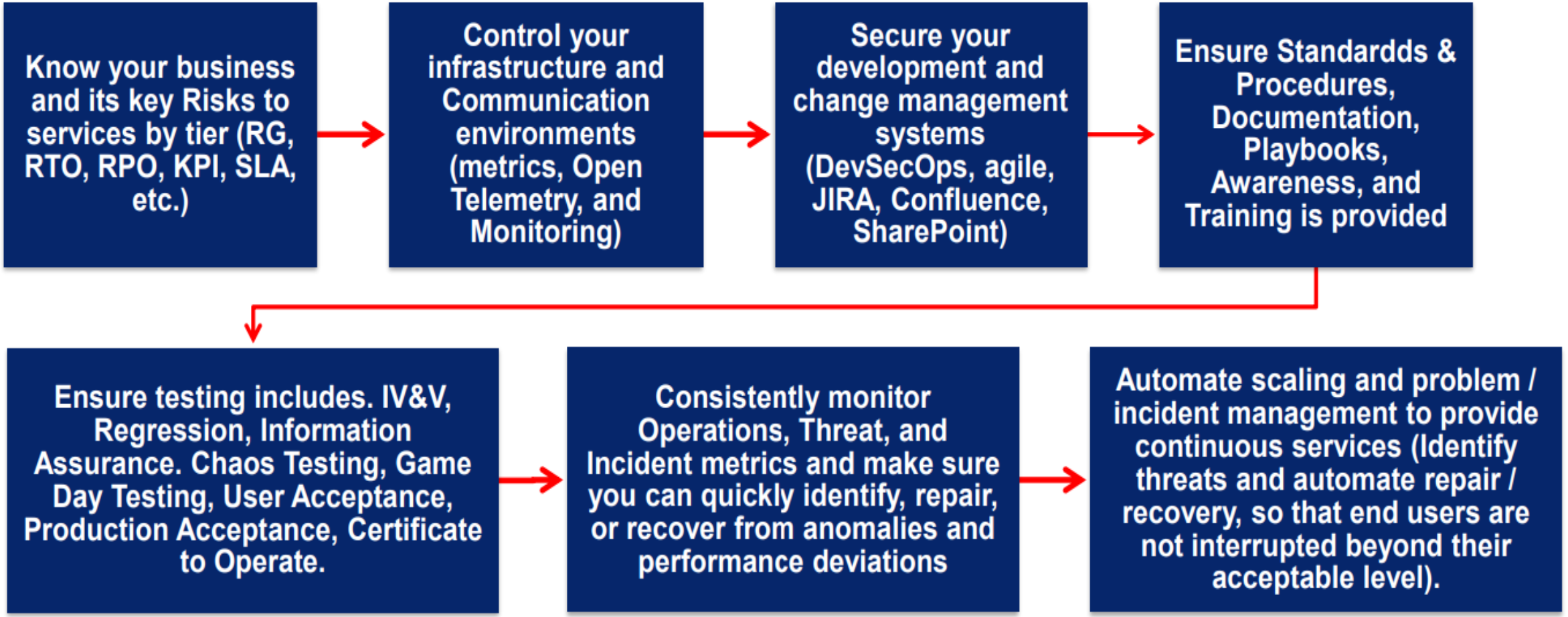
Process followed in performing Enterprise Resilience

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

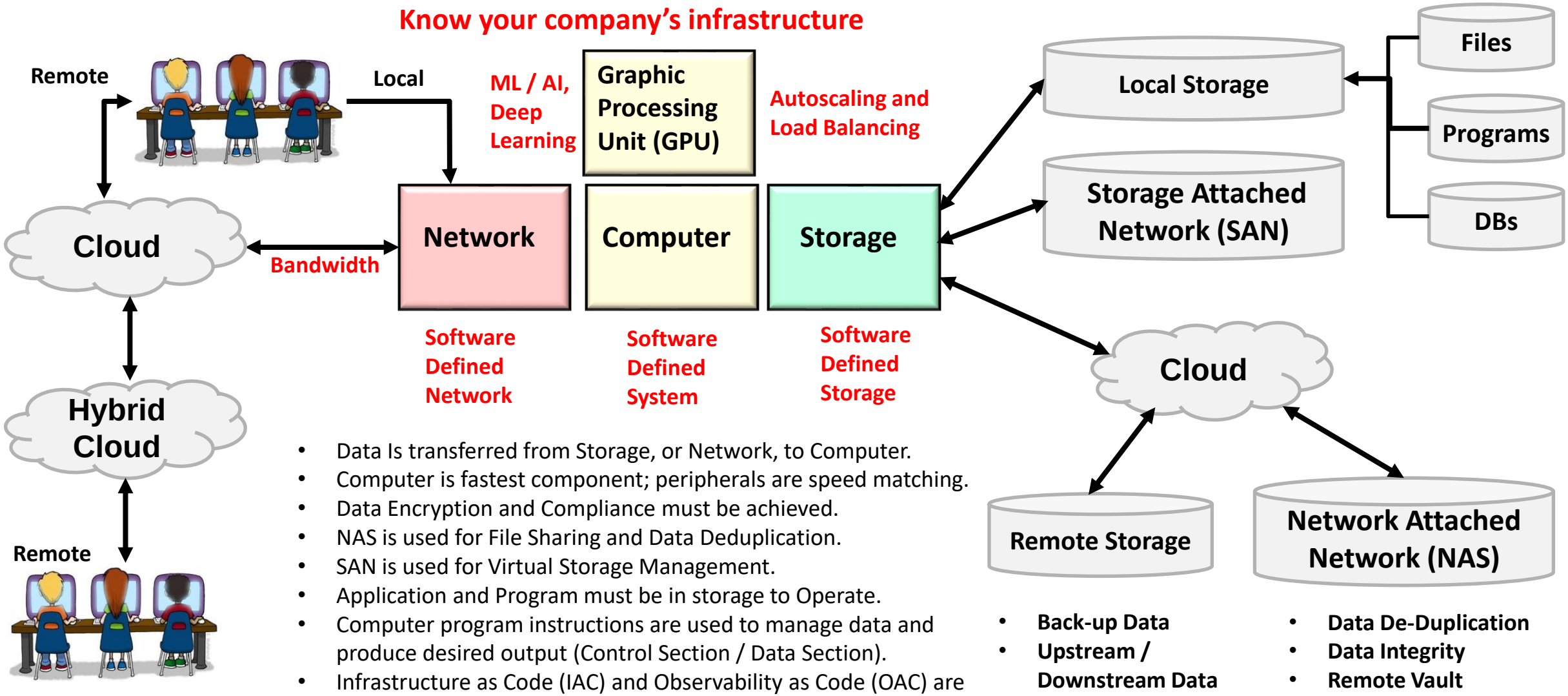


Integrate standards & procedures within everyday functions performed by personnel and ensure the implementation of Awareness and Training programs to keep staff and management informed

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**

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

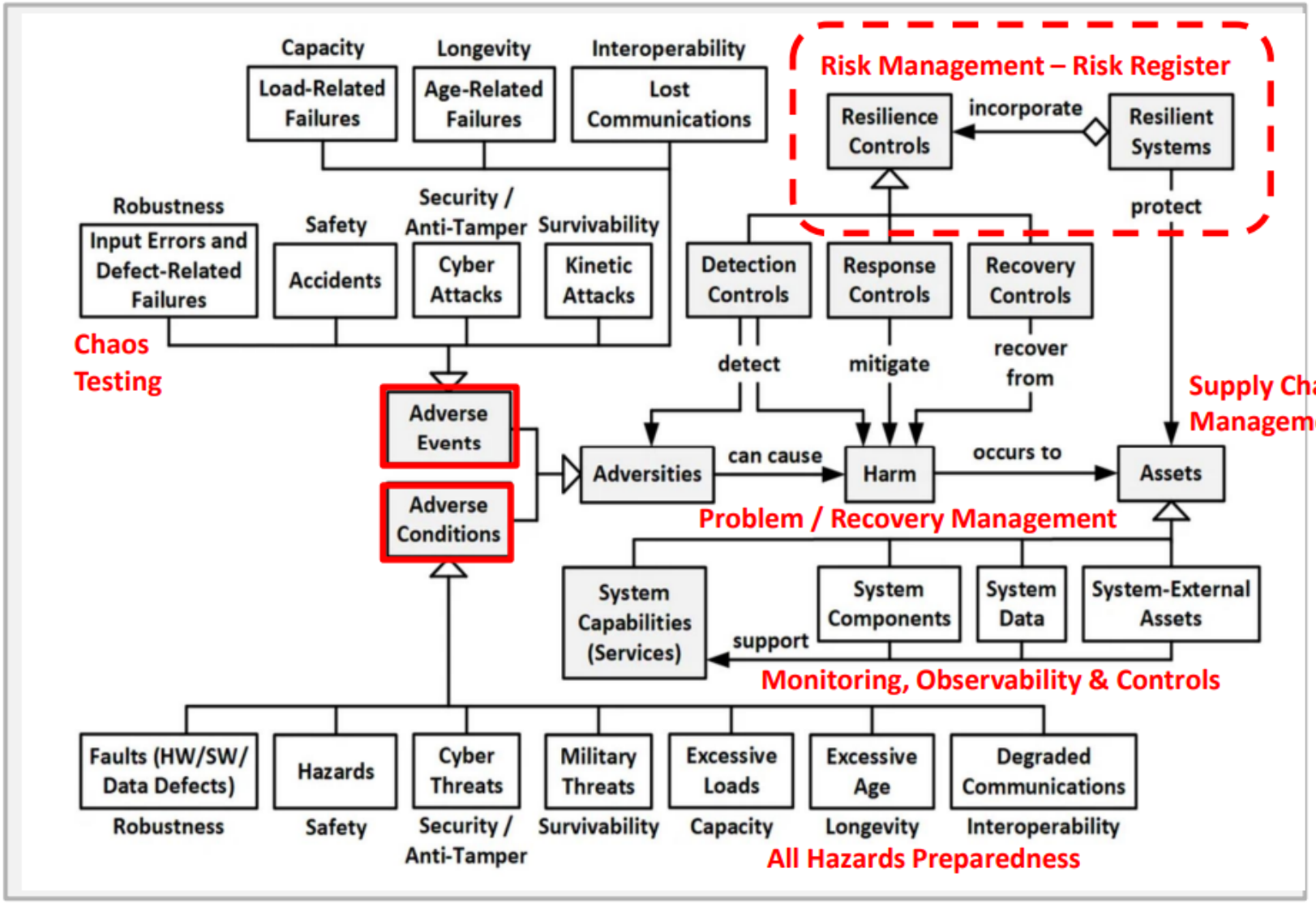
What is Resilience and why is it important

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

Definition:

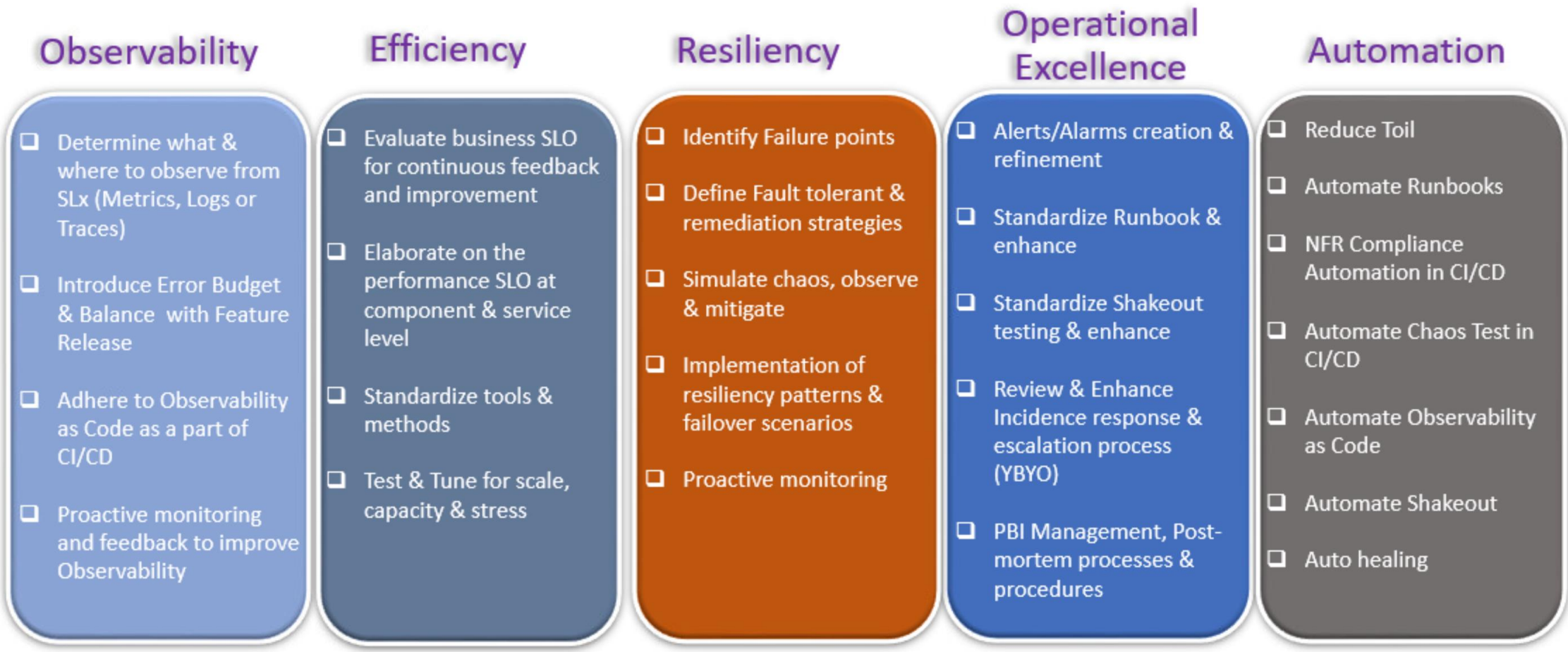
Basically, a system is resilient if it continues to carry out its mission in the face of adversity (i.e., if it provides required capabilities despite excessive stresses that can cause disruptions). Being resilient is important because no matter how well a system is engineered, reality will sooner or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

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



Five Pillars of Site Reliability Engineering (SRE)

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



Google – Site Reliability Engineer Handbook

Adding New Technologies

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

Inventory Management System

CMDB

Resource Status and Location

Product Support L1 – L3

Help Desk Teams

Management and Control

Director – Infrastructure & Operations

IT Operations and Systems Management

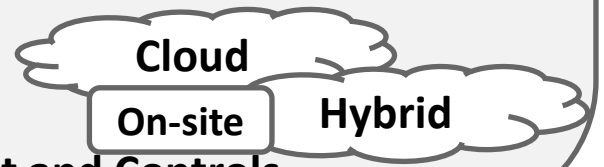
New Device, Software, or Both

- New Resource Order received,
- Resource Requirements & Specifications defined,
- Potential Vendors Identified and selected,
- Analysis of Alternatives (AoA) performed,
- Bids received and offer accepted,
- Delivery Schedule approved,
- Product Installed & Tested,
- Product Accepted.

Asset Management System

- Acquisition,
- Redeployment,
- Termination,
- Coordination,
- Compliance,
- Documentation & Training.

On-Premises or Cloud Environments



Product Management and Controls

Infrastructure Management

Project Management Team

Cybersecurity & Risk Management Team

- Compliance Requirements defined,
- Access Control & Certifications defined,
- Access Controls Defined,
- Protocols & Procedures defined and documented,

Project Management

- Stakeholders & Users
- Subject Matter Experts
- Product & Vendor Selection
- Supply Chain Management
- Resource Requirements,
- Order, Ship, Deliver Tracking
- Install, Test, Implement Coordination,
- Scripting & Integration Management,
- Documentation & Procedures
- Implementation & Testing
- Training & Awareness
- Production Acceptance

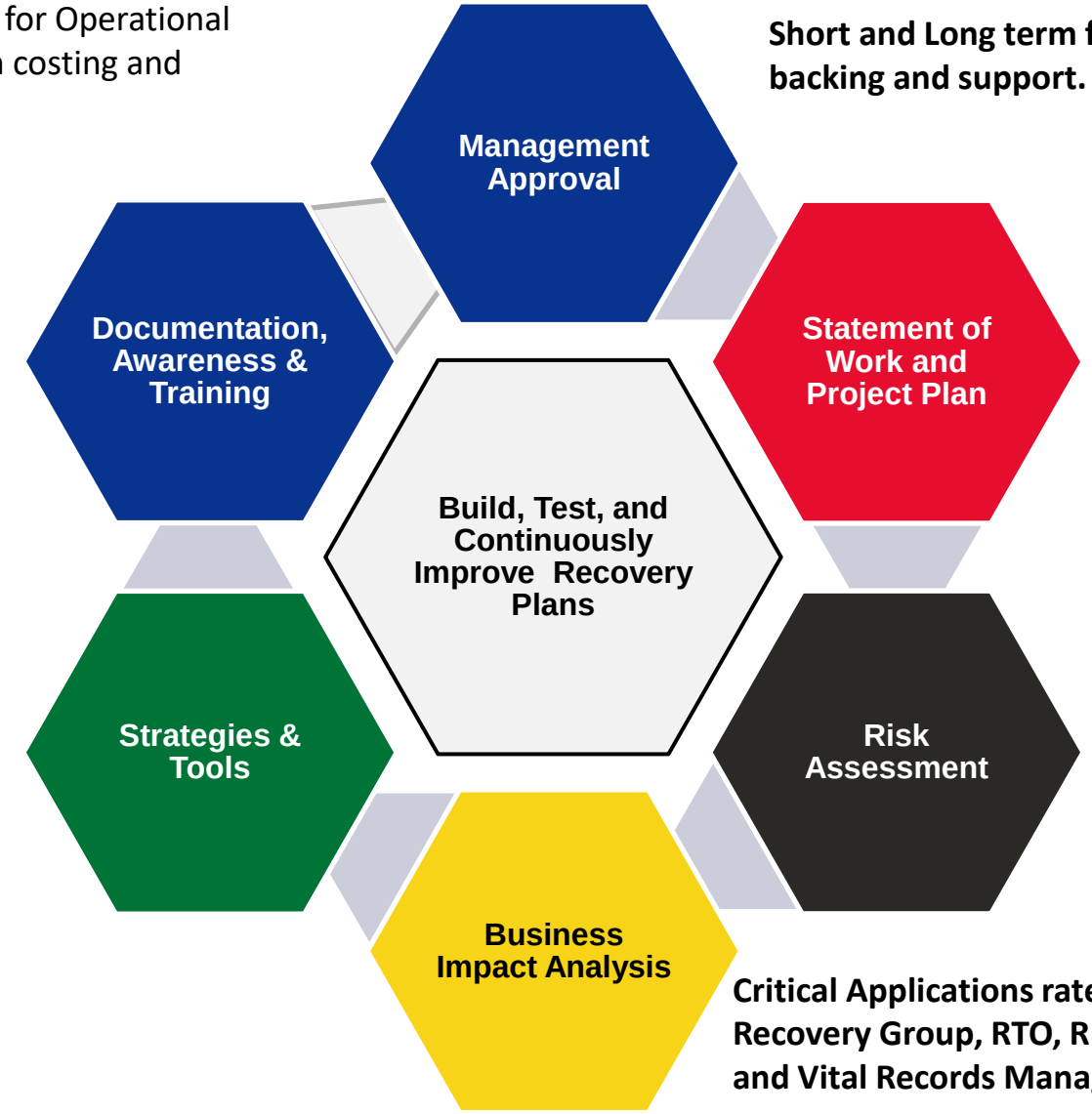
Safeguarding your Business via DR/BC Plans

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

CAPEX for Capital Expenditures and **OPEX** for Operational Expenditures. Both must be considered in costing and ROI planning.

Short and Long term funding, backing and support.

Documentation, Manuals, Plans, Test Cases, Standards & Procedures, Awareness, Training, inclusion in DevSecOps, ITOM, ITSM, testing, Turnover, Certificate to Operate, Support, and Change Management



What we plan to accomplish and the resources needed.

Use of Resources and Delivery Schedule

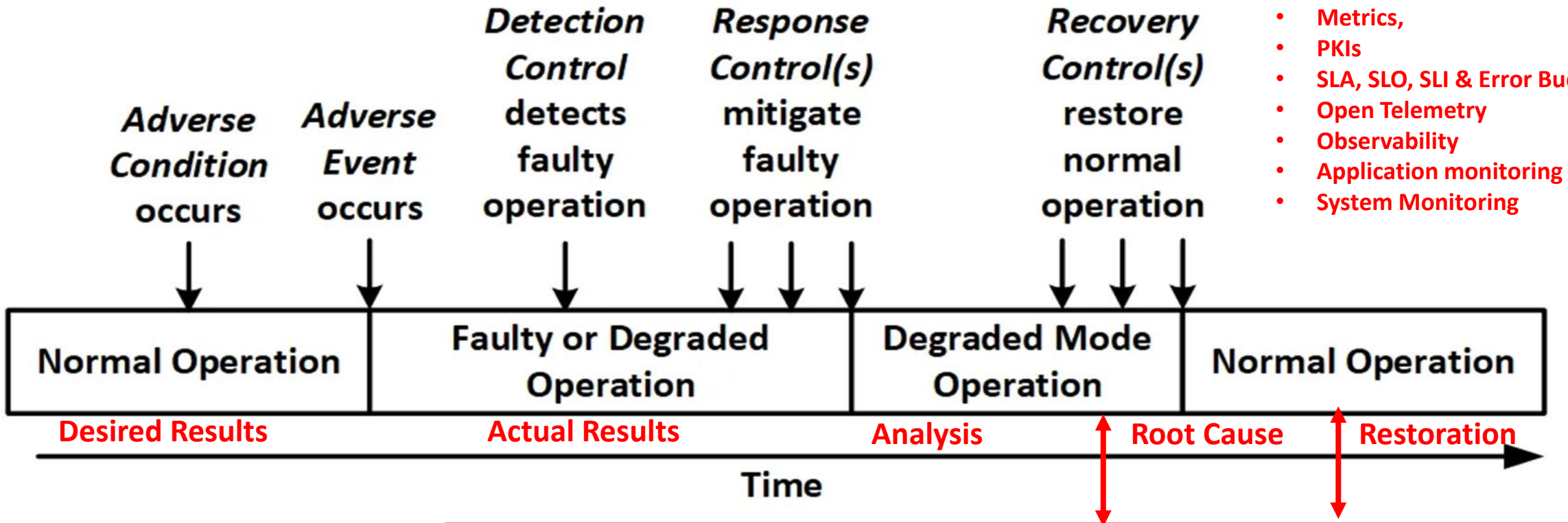
Analysis of Alternative (AOA) of tools and services. Selection, training, and utilization to document and achieve recovery goals. Integrate into everyday functions and provide continuous improvement.

Analysis of Risks to uncover Gaps, Exceptions, and Obstacles. Controsl and corrective actions to mitigate gaps and exceptions and mediate obstacles. Risk Register for problems yet to be resolved with POA&M.

Critical Applications rated via Recovery Group, RTO, RPO, RTC, and Vital Records Management

Monitoring Enterprise Resilience

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



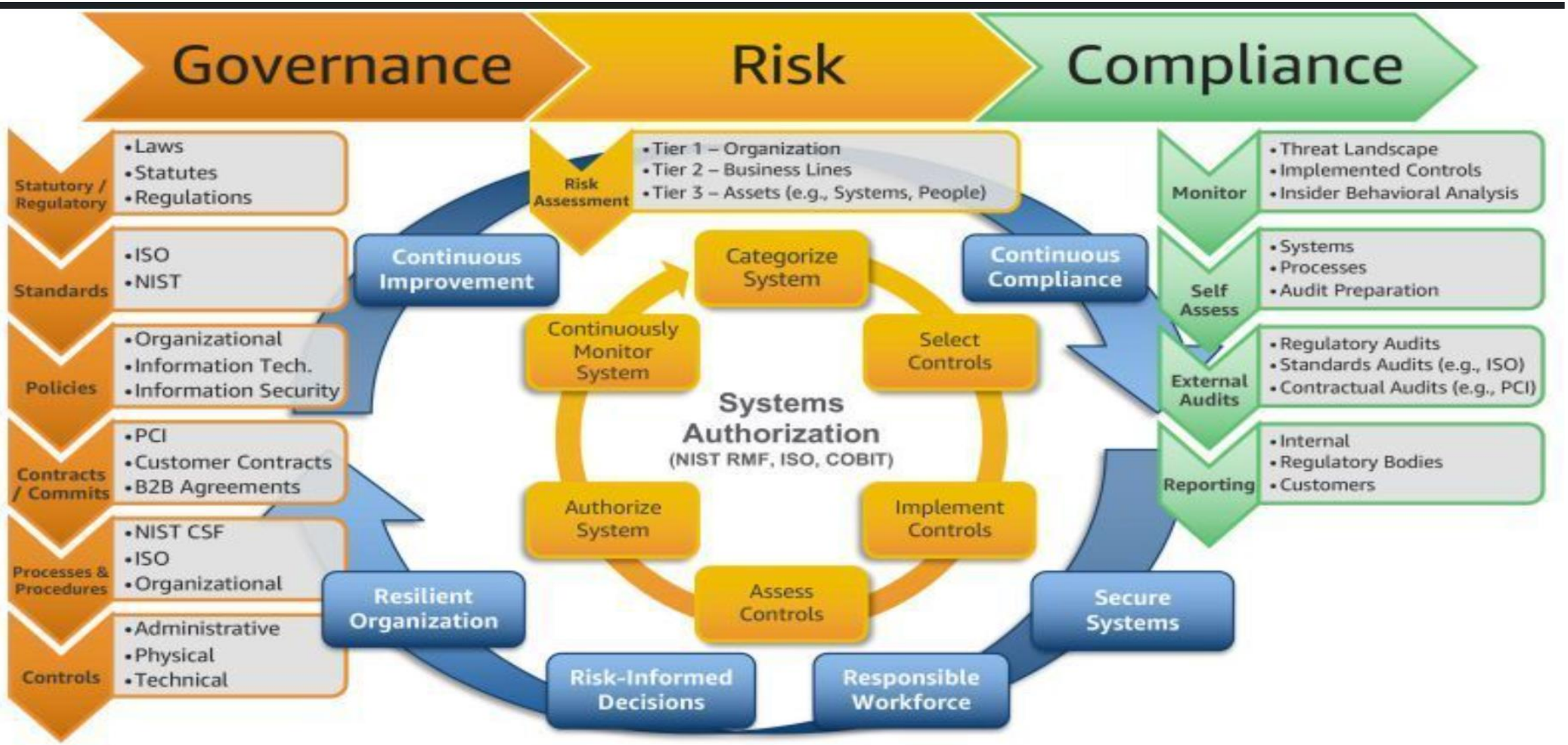
Use of:

- Metrics,
- PKIs
- SLA, SLO, SLI & Error Budget
- Open Telemetry
- Observability
- Application monitoring
- System Monitoring

1. Metrics Degraded and Crossing Threshols for undesired time period
2. Alarm is initiated to ward of an abnormality
3. Alert is issued to warn responsible parties of failure
4. Actions are taken to mitigate problem, mediate obstruction, or initiate recovery operation
5. Return to normal operations (even if at a different site)

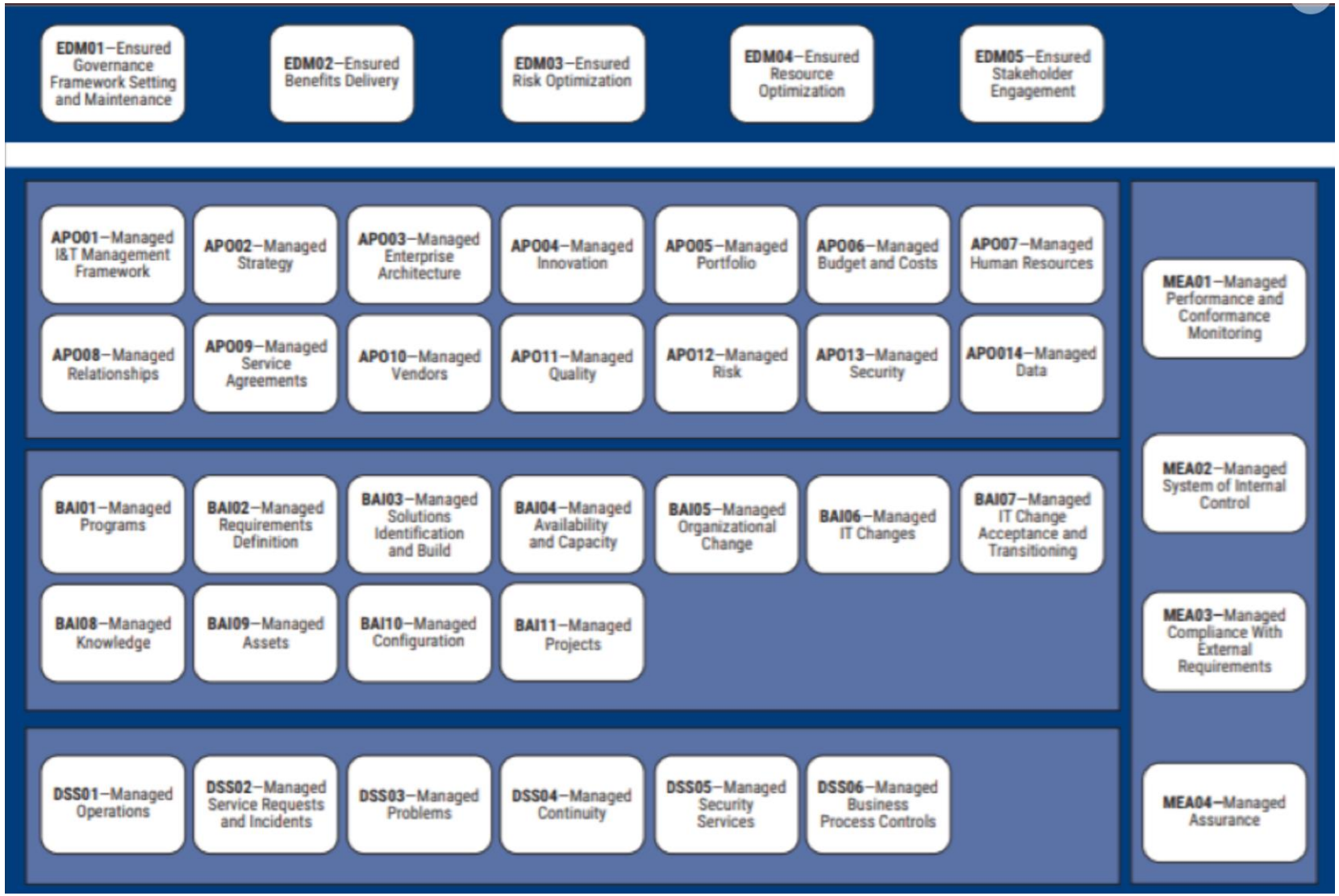
GRC and Risk Management to ensure compliance

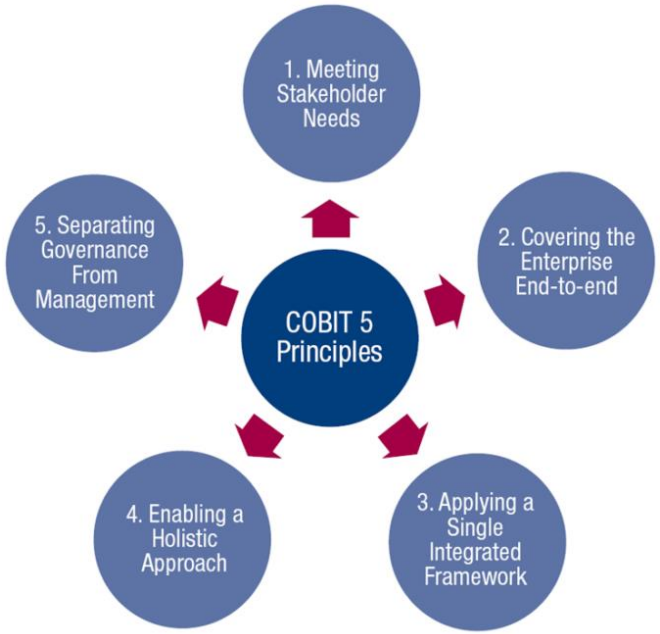
Thomas Bronack
Email: bronackt@gmail.com
Phone: (917) 673-6992



COBIT 5 Framework (Integrating Business with IT)

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

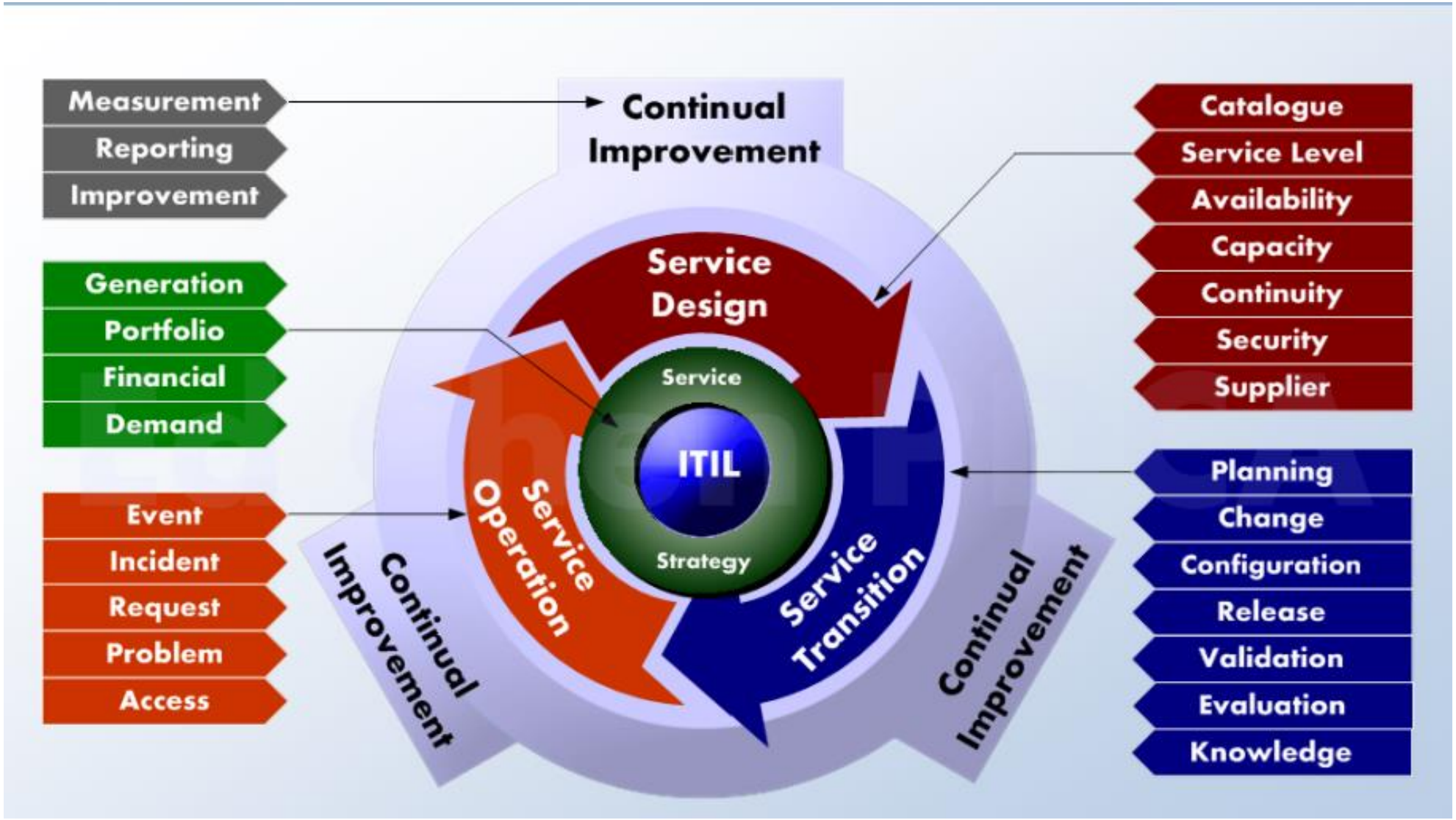




1. Metering Stakeholder needs.
2. Covering the Enterprise, end-to-end.
3. Applying a single integrated framework
4. Enabling a Holistic Approach
5. Separating Governance from Management

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.

Data Lifecycle – Protecting and Using Data

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

Data is either Static or Dynamic, with Dynamic being most important to protect.

Data Sensitivity

- Ownership
- Usage Authorization by Job Title
- Entitlements
- Access Controls
- Confidentiality, Integrity, Availability (CIA)
- Domestic & International Legal & Regularity Compliance

Data Categories

- Application
- Service
- Client
- IAM
- SIEM / SOAR
- Certificates
- Library Management
- Vital Records Management
- Backup / Recovery

Data Mining

- Data Lake
- Error Conditions
- Error Corrections
- Cyber Crimes
- Technical Impacts
- Metrics & Reporting
- Observability

Data Analysis

- Entitlements
- CIA / Security
- Usage Trends
- Cyber Crime
- Technical Impact
- Circumventions
- Patches
- Client Performance
- SLA / SLR
- Marketing& Sales

Data Reporting

- Capacity
- Performance
- Growth Direction
- MTTF / MTTR
- Time to Provision
- Total Cost of Ownership
- Service Reliability Engineer (SRE)

Data Usage

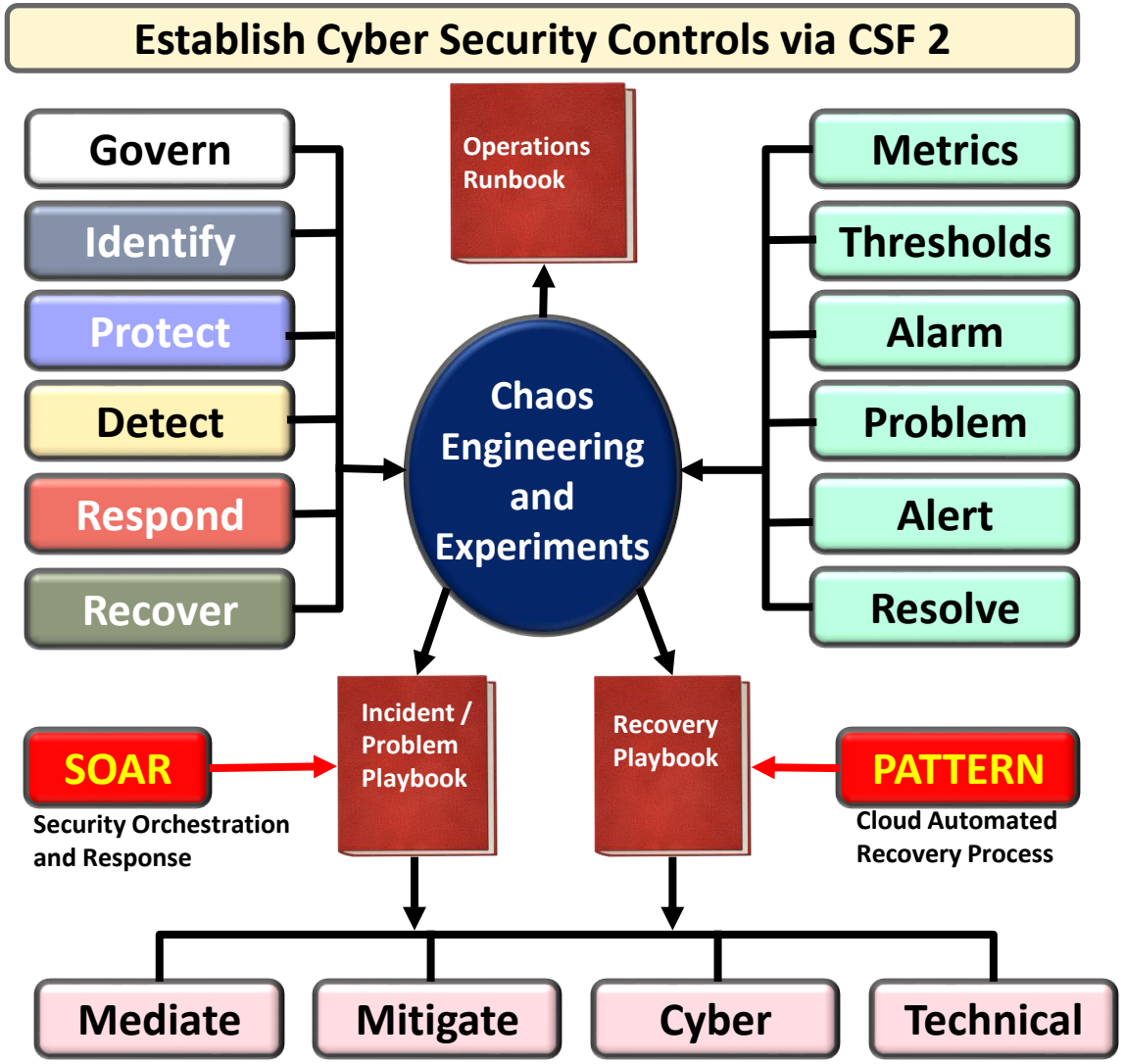
- Asset Management
- Infrastructure Management
- Configuration Management
- Existing Clients
- New Clients Capture
- Onboarding
- Reporting

BCM protects people, resources, and data. The above process will allow you to identify critical data, its ownership, sensitivity, and protection requirements via back-up / recovery and vaulting to adhere to Vital Records Management practices.

NIST CSF 2.0 Categories and Application

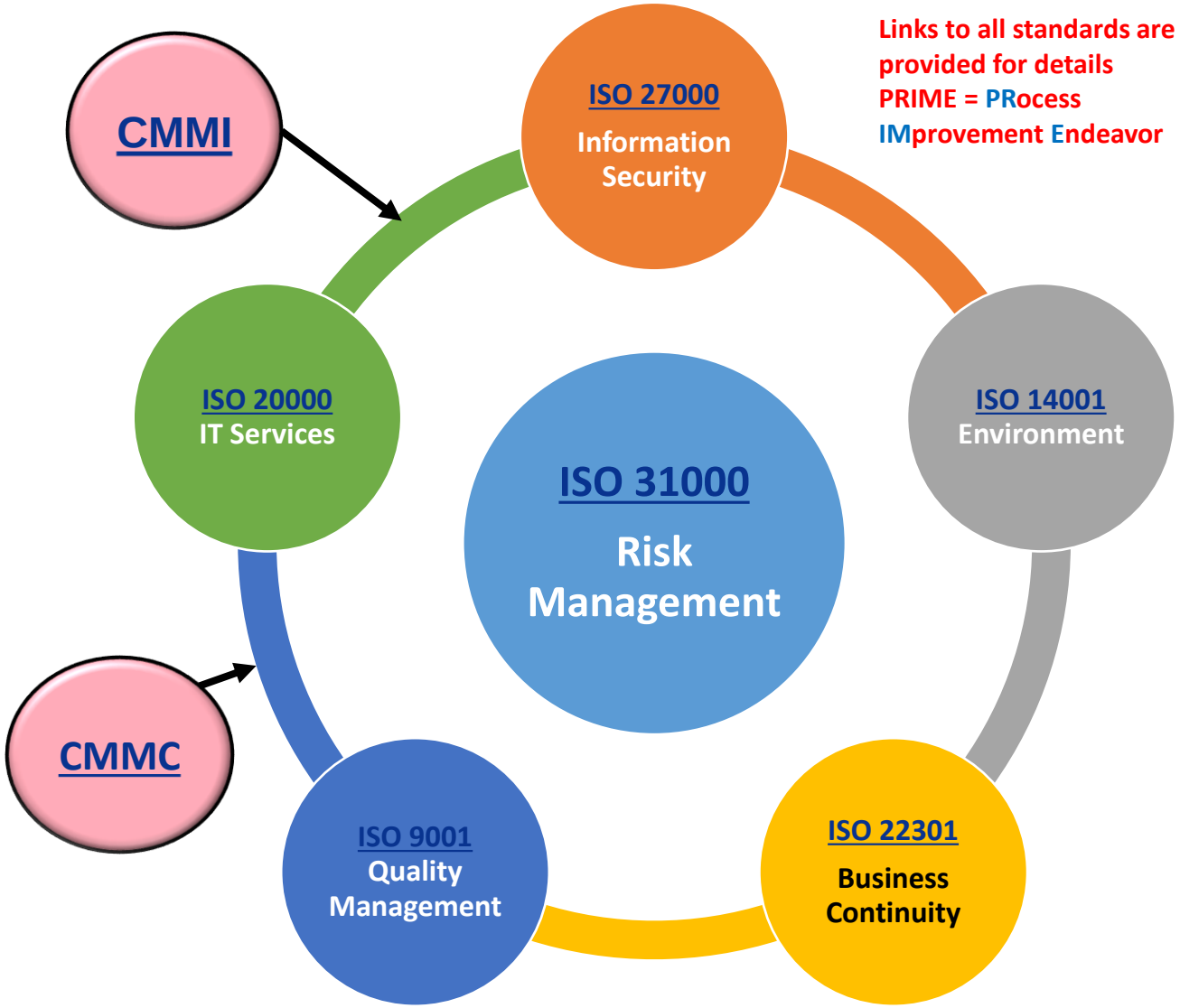
Thomas Bronack
Email: bronackt@gmail.com
Phone: (917) 673-6992

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



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.

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

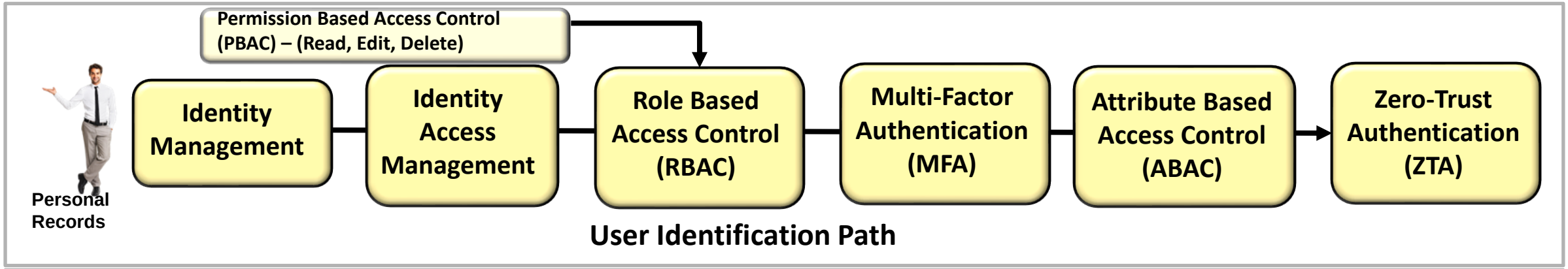
MFA Profile
- Userid / Pswd
- Secondary Validation
- PIN, Call Back

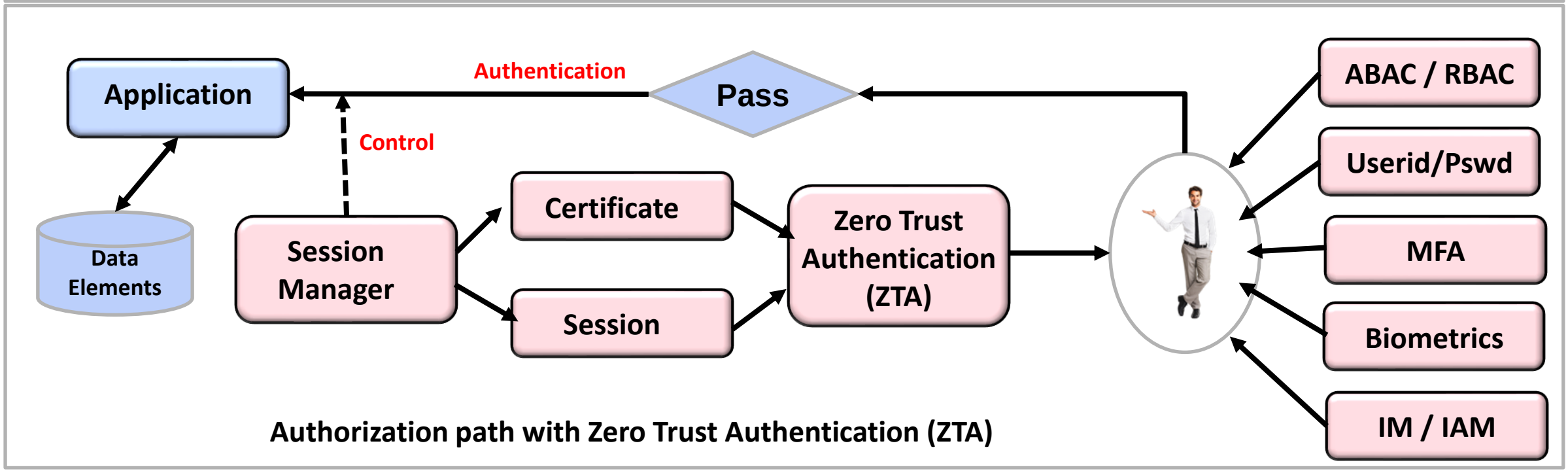
ABAC Profile
- Machine
- Location
- Authorization

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

Overview of a ZTA Session

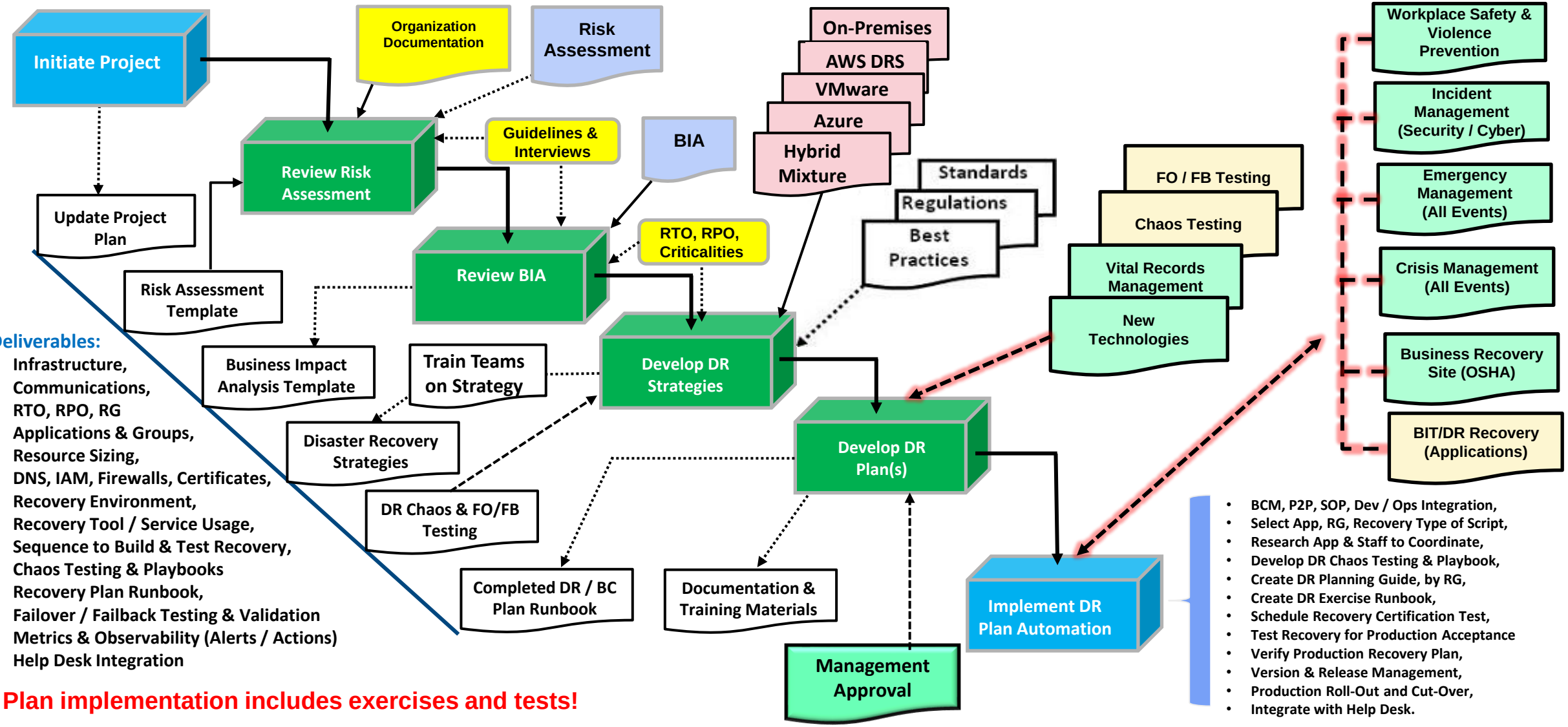
Thomas Bronack
Email: bronackt@gmail.com
Phone: (917) 673-6992





Sample Recovery Plan Methodology

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



Deliverables:

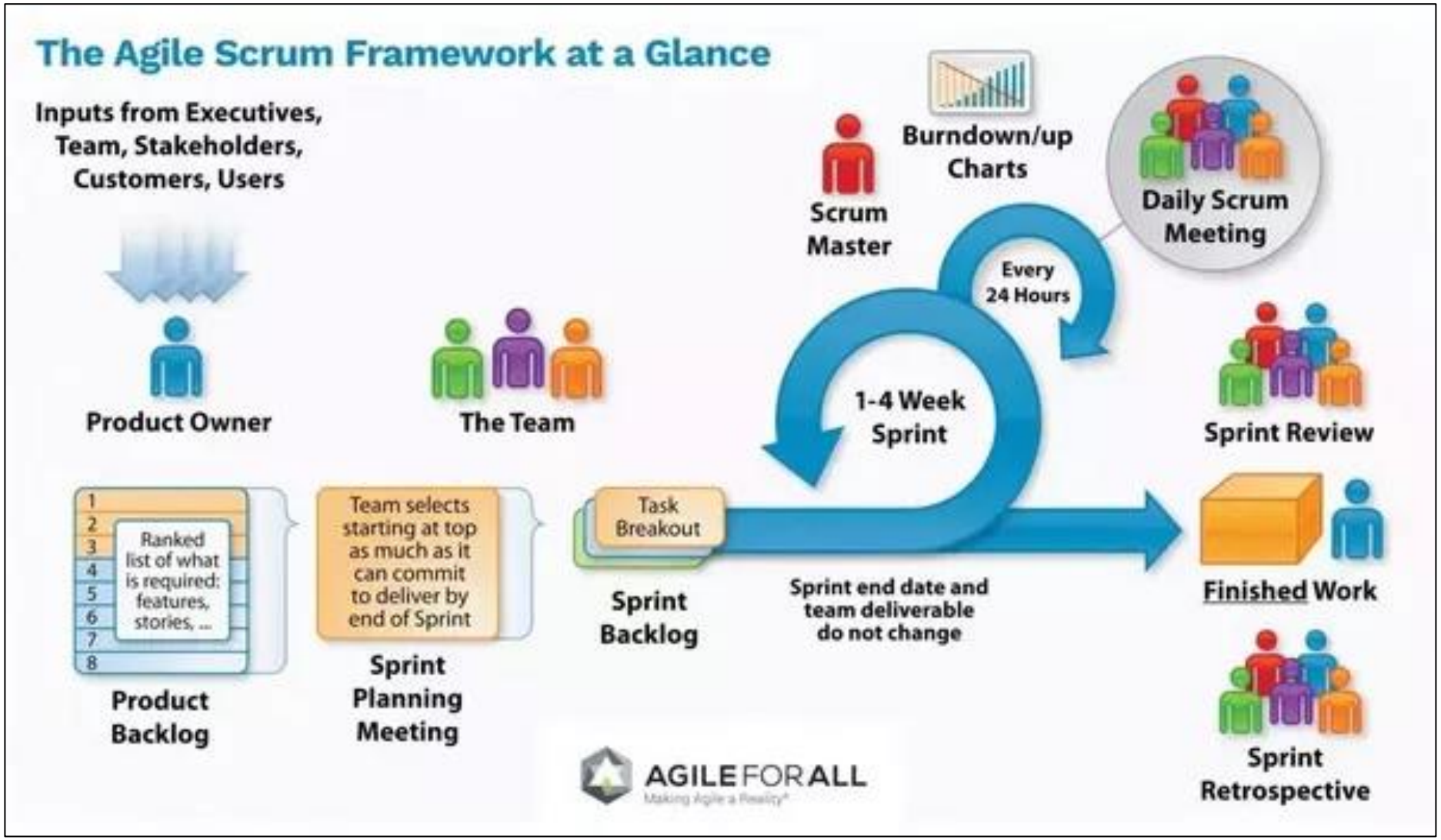
- Infrastructure,
- Communications,
- RTO, RPO, RG
- Applications & Groups,
- Resource Sizing,
- DNS, IAM, Firewalls, Certificates,
- Recovery Environment,
- Recovery Tool / Service Usage,
- Sequence to Build & Test Recovery,
- Chaos Testing & Playbooks
- Recovery Plan Runbook,
- Failover / Failback Testing & Validation
- Metrics & Observability (Alerts / Actions)
- Help Desk Integration

- BCM, P2P, SOP, Dev / Ops Integration,
- Select App, RG, Recovery Type of Script,
- Research App & Staff to Coordinate,
- Develop DR Chaos Testing & Playbook,
- Create DR Planning Guide, by RG,
- Create DR Exercise Runbook,
- Schedule Recovery Certification Test,
- Test Recovery for Production Acceptance
- Verify Production Recovery Plan,
- Version & Release Management,
- Production Roll-Out and Cut-Over,
- Integrate with Help Desk.

Plan implementation includes exercises and tests!

Agile vs Waterfall Systems Development

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

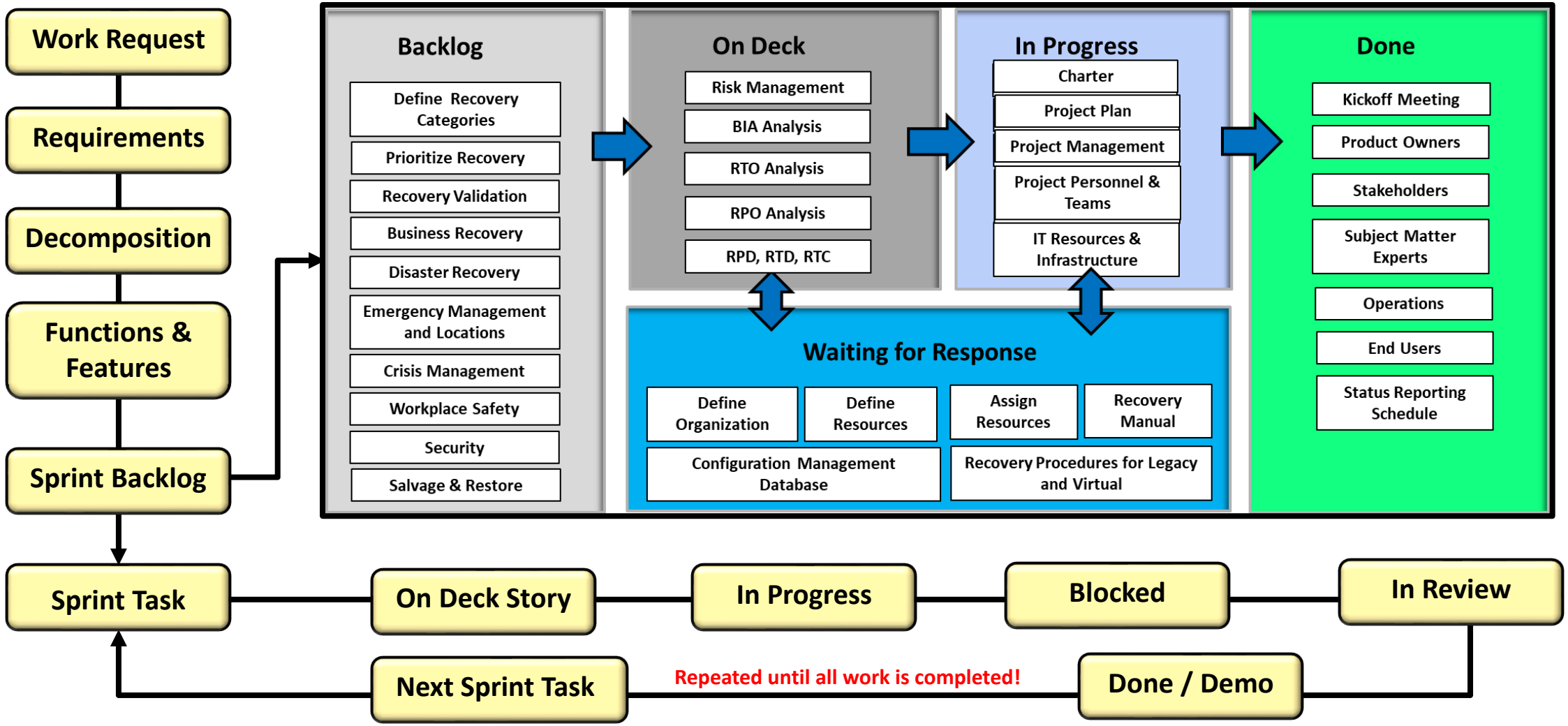


- Conception
- Initiation
- Analysis
- Design
- Construction
- Testing
- Deployment

Waterfall Model

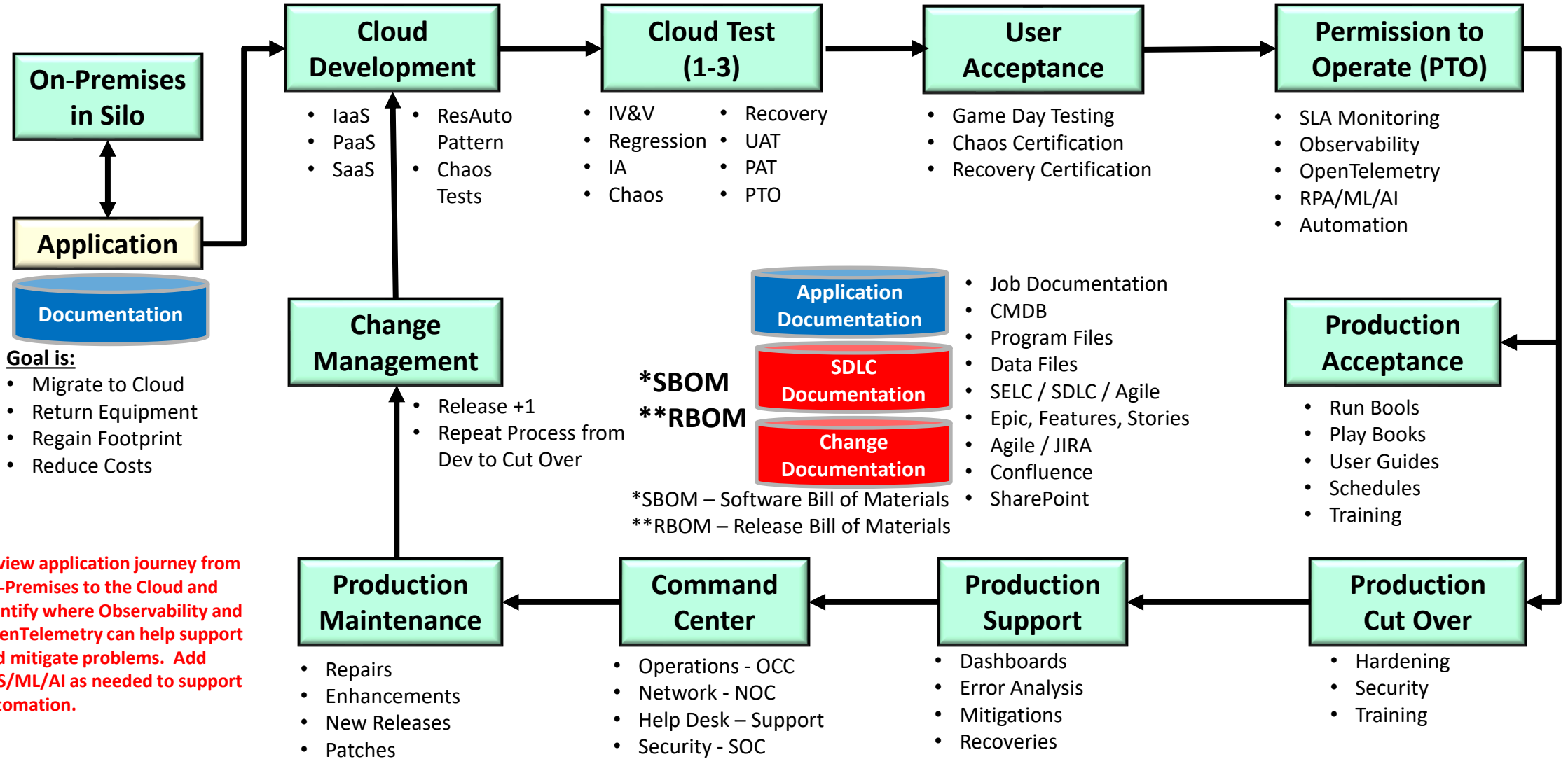
DR Workload, using the Agile method for Dev/Ops

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



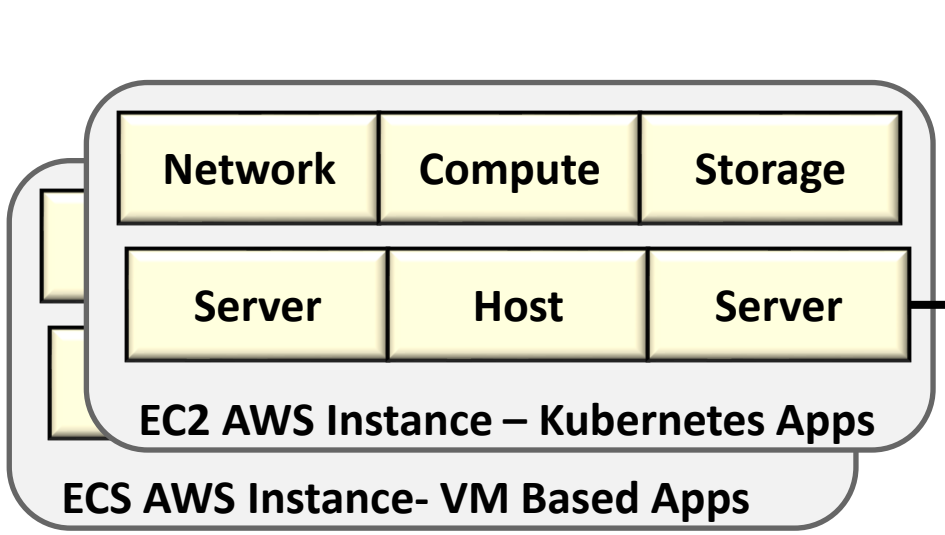
Migrating Applications to the Cloud

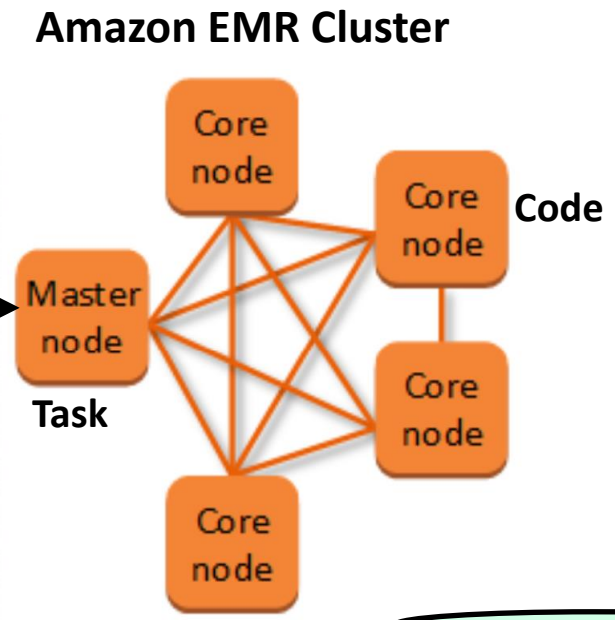
Thomas Bronack
Email: bronackt@gmail.com
Phone: (917) 673-6992



AWS Components and their usage

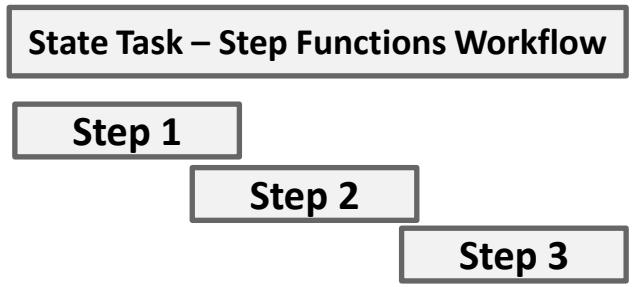
Thomas Bronack
Email: bronackt@gmail.com
Phone: (917) 673-6992

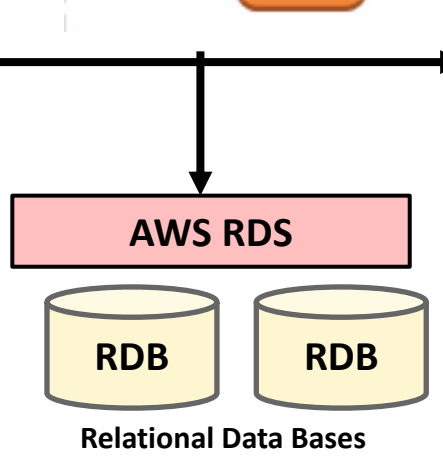




S3 Bucket and Lambda:

- Serverless
- S3 File Services
- Streaming Processing
- Web Apps
- IOT Backends
- Obile Backends
- Lambda Balances Workload
- AWS Glue runs Serverless ETL Jobs

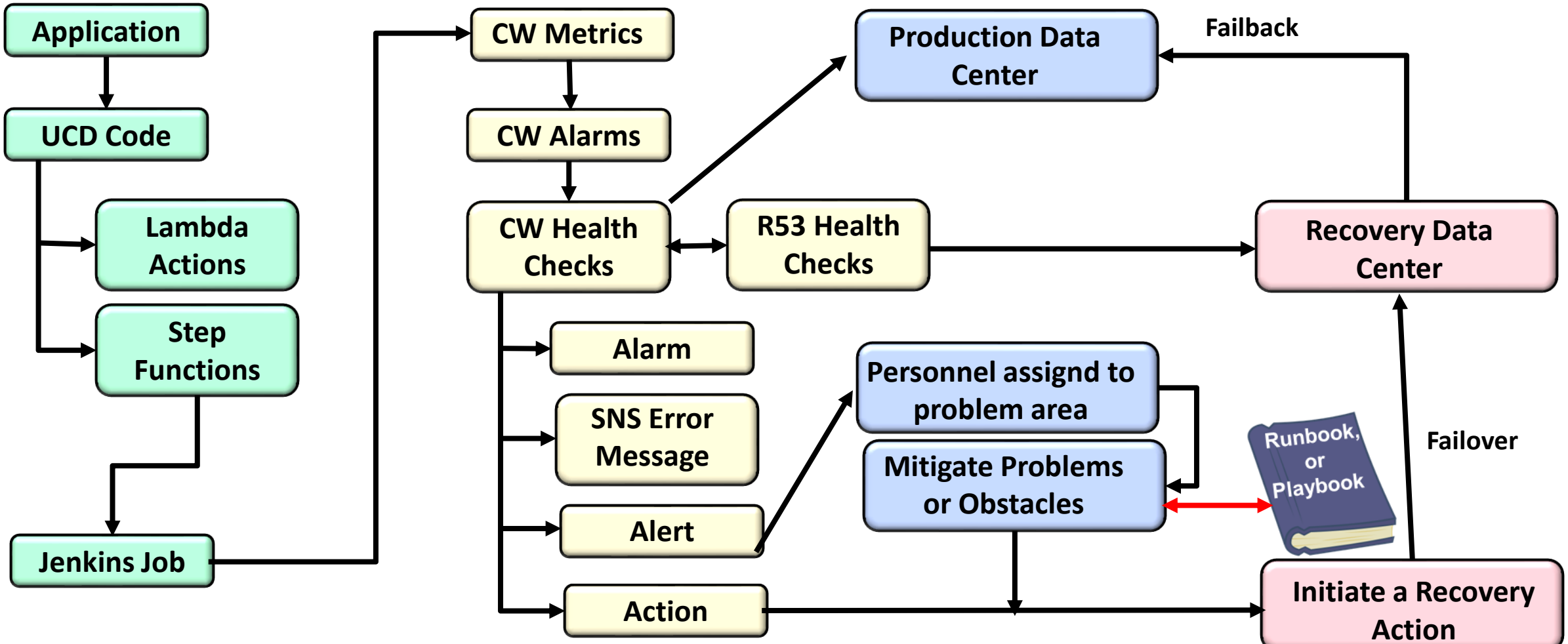




- Self Managed NoSQL Database
- Sizing and Backup by AWS
- Maintains by Deleting Expired Files
- Highly available and durable

AWS Amazon Automation Resilience Pattern – Health Checks

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



Define Application Component

Establish Metrics, Alarms, and Health Checks, with SNS Error Message to initiate Actions

An Automated Approach to SLA Adherence

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