

Enterprise Governance & Risk Management Continuity Management Framework & Awareness

- ❖ **Presenters:**
- ❖ **Lillibett Machado**, *CISA, CISM, CGEIT, CRISC*
**Chief Information Security Officer,
Cadence Bank, N.A.**
- ❖ **Charity Otwell**, *ABCP*
**Business Continuity Manager,
Cadence Bank, N.A.**



Today's Business Complexity

- The exponential change on regulations
- Globalization
- Distributed Environments
- Processes
- Competitive Velocity
- Business Relationships
- Technology
- Business Data

We must strive to keep this complexity synchronized!

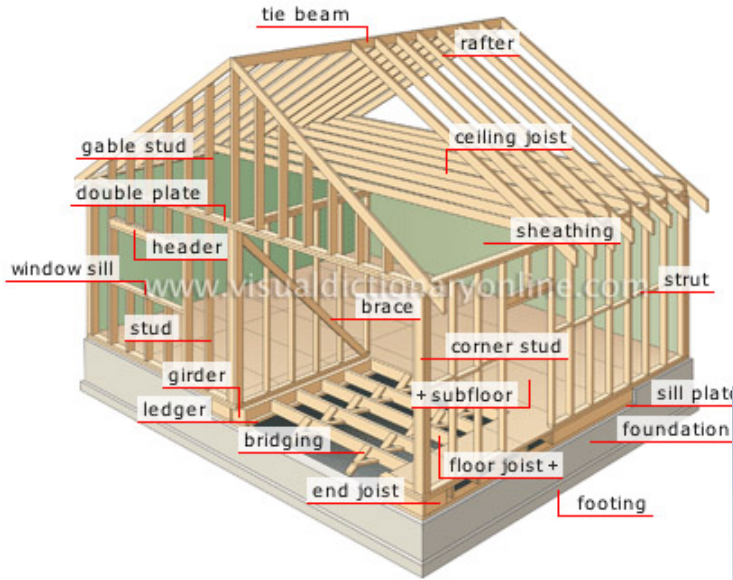
Companies are in Constant Metamorphosis Environment...

- They are **Dynamic** on a constant state of change
- They have **Distributed** operations complicated by a Web of Global suppliers, agents, business partners and client relationships
- They are **Disrupted** with change combined with complexity with governance, risk, compliance requirements

In this environment its required to have complete awareness of Governance, Risk & Compliance (GRC) across our operations, processes, relationships, systems, and data to see the big picture of risk and its impact on the bank's performance and strategy!



Why we need a Framework?



Technology Governance Framework

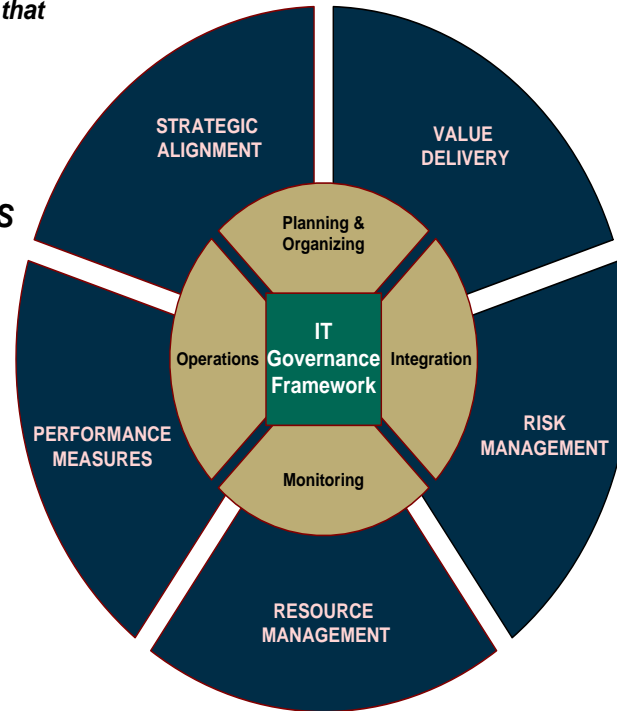
TECHNOLOGY ENTERPRISE GOVERNANCE GOAL

To provide strategic direction, ensuring that objectives are achieved, risk are managed appropriately and verifying that the enterprise's resources are used responsibly.

Dependant On...



IT GOVERNANCE FOCUS



Enterprise Governance “5” Buckets & Business Continuity

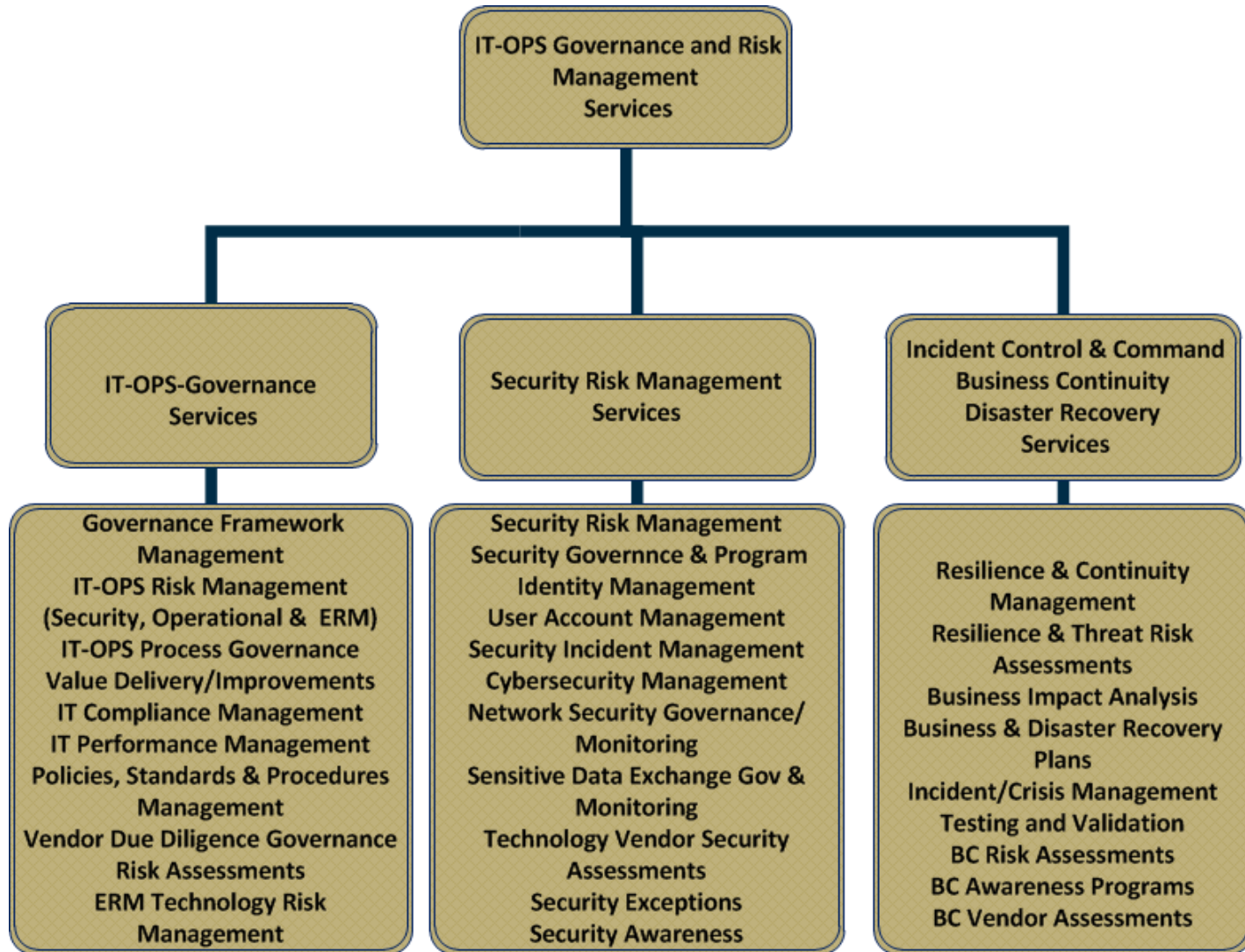
- **Ensure a BCM Governance Framework & Maintenance to provide a consistent approach and align to your Enterprise Governance and Risk Management:**
 - Establish a BCM Governance Framework
 - Direct the Governance framework
 - Monitor and Improve the Governance Framework
- **Ensure that BCM provides Optimal Value augmenting IT Initiatives, services and supporting business and technology asset availability efficiently and within the business risk profile:**
 - Continual evaluation and participation of the IT portfolio of investments , services and assets
 - Ensure value is deliver through the IT Portfolio economic life cycle
- **Ensure Risk Optimization by providing business and technology solutions and oversight to not exceed risk appetite and risk tolerance. Focus mostly on availability data integrity risk:**
 - Continues examination and evaluation of risk on the current and future use IT Services
 - Ensure Risk Management practices provide reasonable assurance risk is being managed
 - Monitor risk remediation to track and record deviations

BCM Governance “5” Buckets (Continue)

- **Ensure Resource Optimization to meet optimal resource requirements to maintain resilience and continuity to ensure readiness for future needs and changes:**
 - Continuously evaluate resources to define current and future needs to meet established objectives
 - Ensure the use of best practices to manage resources to enable optimal usage
 - Monitor resource allocations to meet objectives effectively
- **Ensure Stakeholder Transparency by communicating effectively and in a timely manner; by establishing reporting on performance, areas of improvement and confirming that BCM objectives are in line with the business objectives and strategies:**
 - Ensure Stakeholder Communication and reporting
 - Establish mechanisms to effectively manage stakeholder quality and completeness of information
 - Monitor the effectiveness of the information and communication requirements



IT Operations Governance & Risk Management Organization

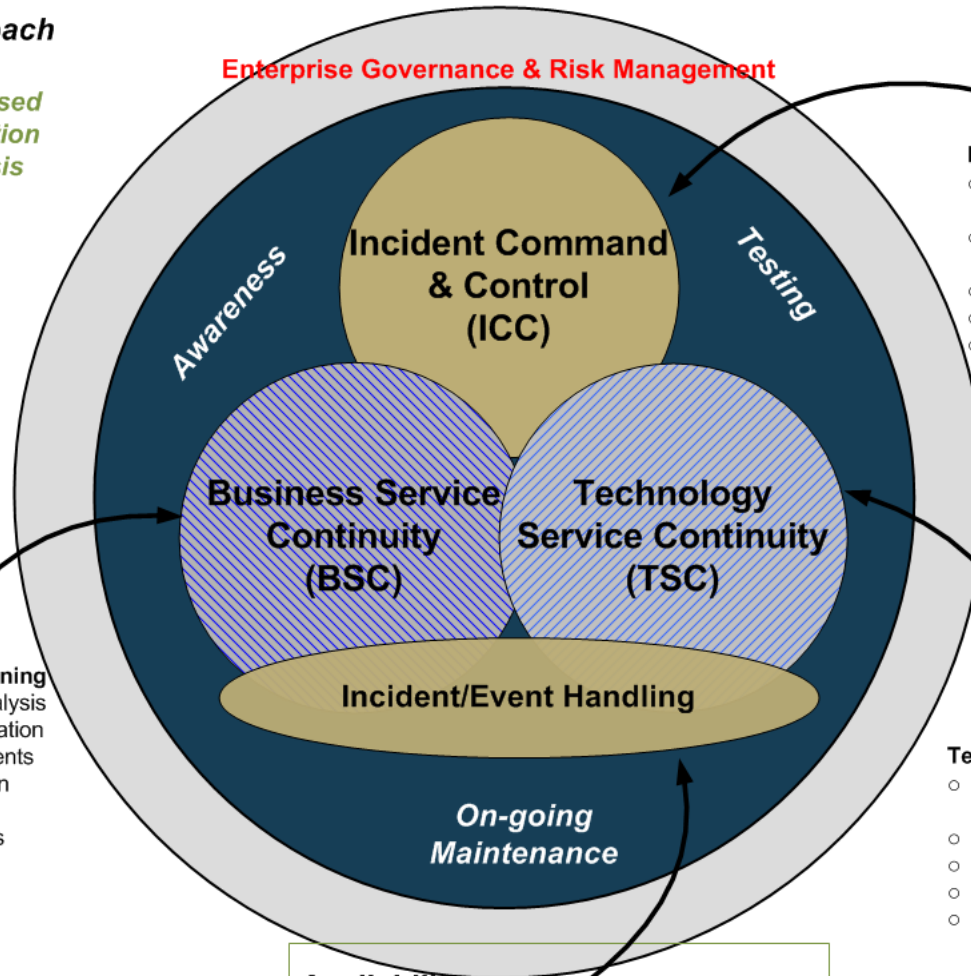


Business Continuity Framework

Enterprise-Wide Approach

- *Business Process Focused*
- *Operational Risk Mitigation*
- *Business Impact Analysis*
- *Resilience & Continuity Solutions*
- *Regulatory & Standards Integration*

- Business Service Planning**
- Business Impact Analysis
 - Incident/Event Escalation
 - Resource Requirements
 - Business Resumption Strategies
 - Testing & Awareness



Enterprise Governance & Risk Management

ICC- Crisis Management

- Emergency Planning & Response
- Command Center Operations
- Escalation/Communication
- Logistics Support
- Incident/Event Management

Technology Service Planning

- Technology Service Impact Analysis
- Incident/Event Escalation
- Recovery Strategies
- Resource Requirements
- Testing & Awareness

Availability

- *Continuous Operations*
- *Disaster Avoidance*
- *Preventive Capabilities*
- *Optimal Controls & Risk Mitigation*

Business Continuity Management Basic Governance

Alabama & Mississippi 2013-14



Houston & Florida 2014



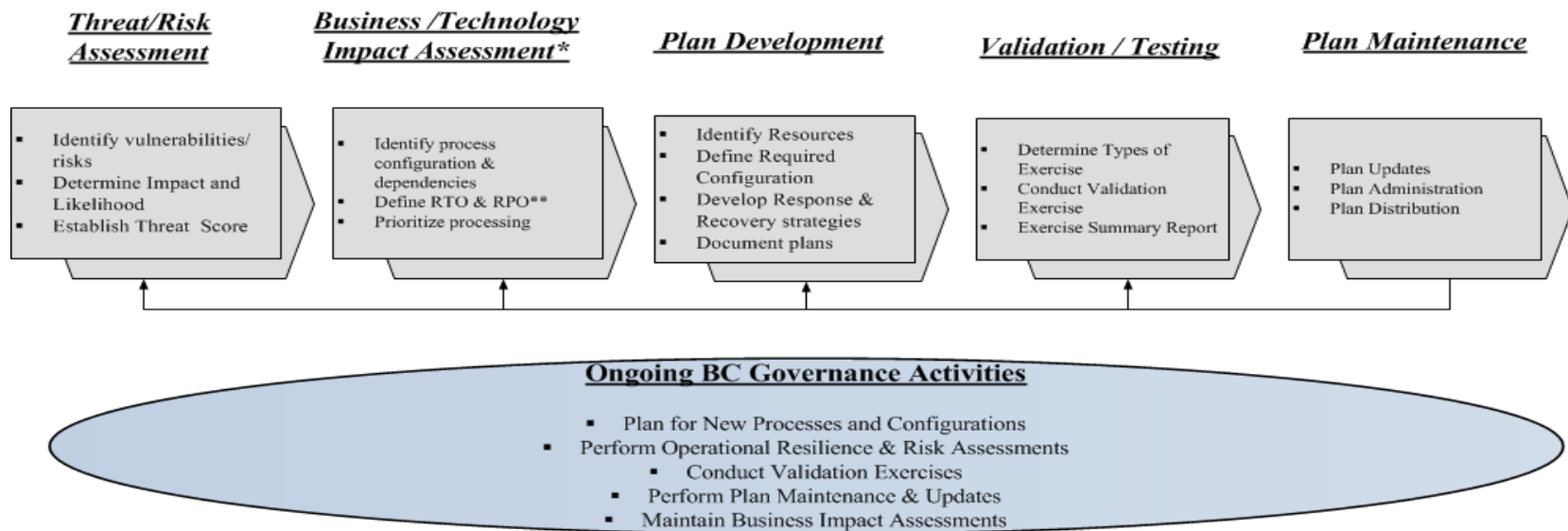
Business Continuity Management Services: What can we do for you?

- **Business Impact Analysis (BIA) for each critical process within the line of business**
- **Business Continuity Planning, Validation & Awareness for each line of business**
- **Technology Service Impact Analysis (TSIA) for each service within IT Operations**
- **Disaster Recovery Planning/Requirements and Testing**
- **Availability and Compliance Risk Assessments**
- **Incident Command & Control planning, coordination & support**
- **Business & Technology Service Catalog**



Business Continuity Management Process

Business Continuity (BC) Process



* BIA = Business Impact Analysis & IT Impact Assessment

** RTO & RPO = Recovery Time Objective & Recovery Point Objective

8-28-2014



Business Continuity Plan Structure

Statistics:

BCP: 20-30,

BIA: 85-95,

ICC: supported ~8 events in 2013

Validations/Testing: 30-40

Corporate-Wide Business Continuity Plan Structure 03-2014

Incident Command & Control (Crisis Management)

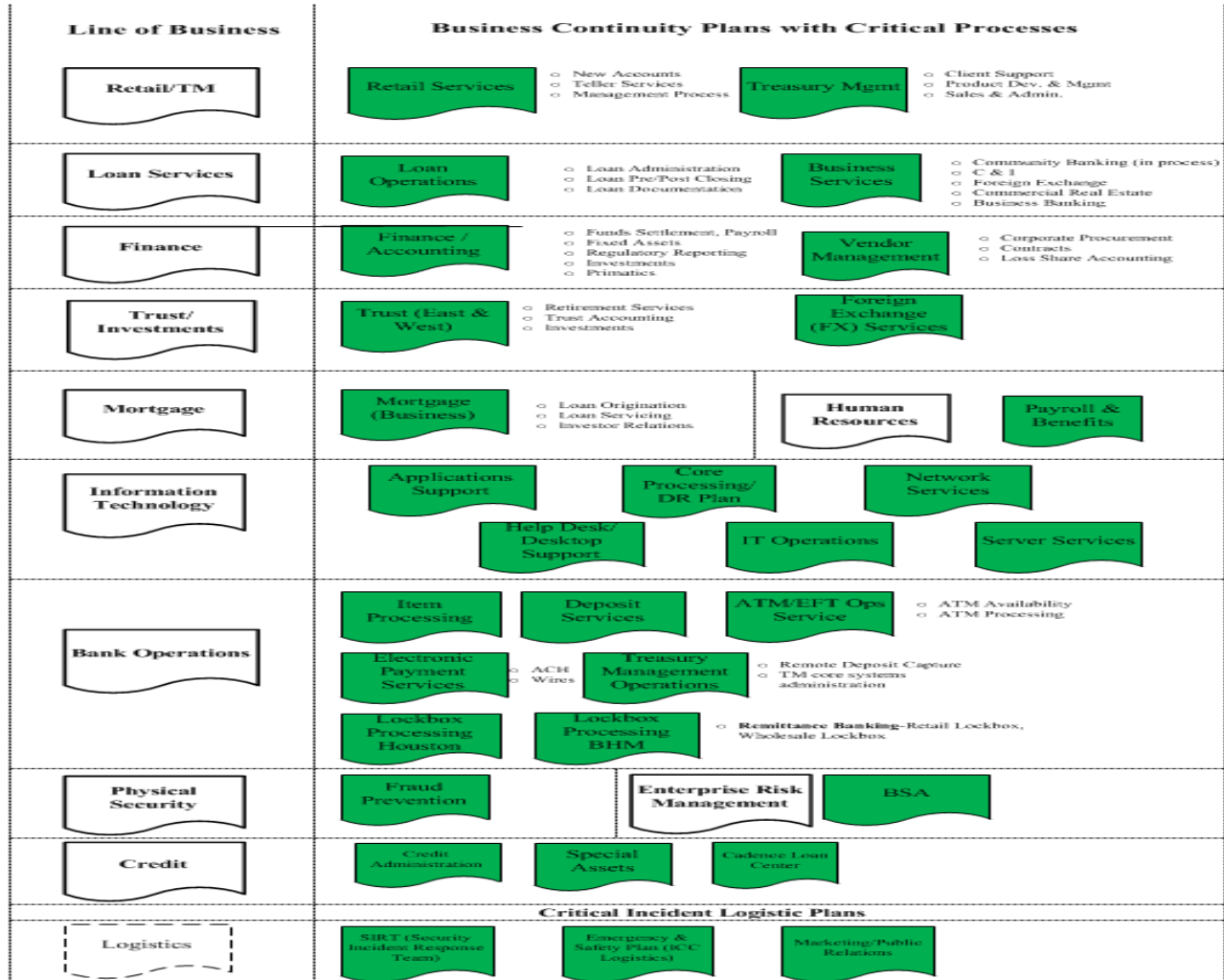
Executive Management - Review & approval of any actions which exceed the pre-planned and pre-approved response & recovery strategies

Incident Command & Control (ICC) Plan

- Logistics:**
- Facilities/Physical Security
 - Finance/Accounting
 - Human Resources
 - Marketing/Public Relations
 - Corp. Procurement
 - Technology Security

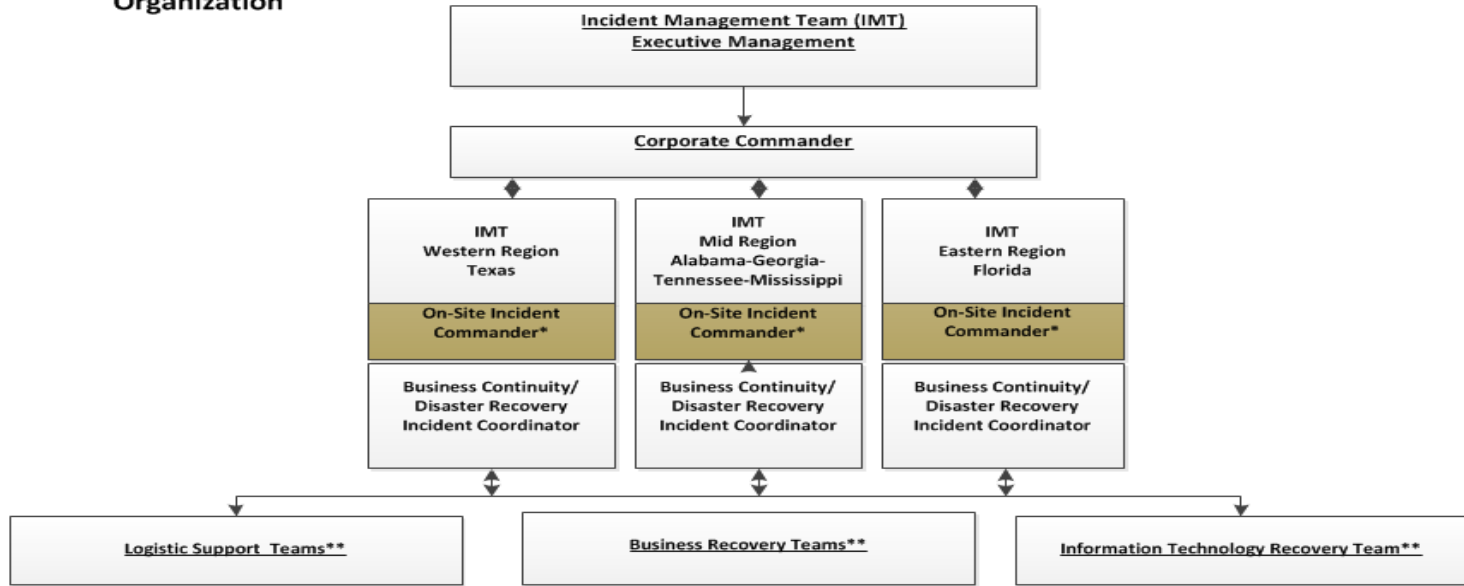
- Incident Command & Control:**
- Incident Commander *
 - All activated support personnel
 - Senior Management and/or executive from each affected Business Function & Management Team

* Incident Commander or On-Site commander - starts out as the Line of Business lead and/or Executive from affected business unit. The Incident Commander or Site Commander role changes as the severity of the incident increases.



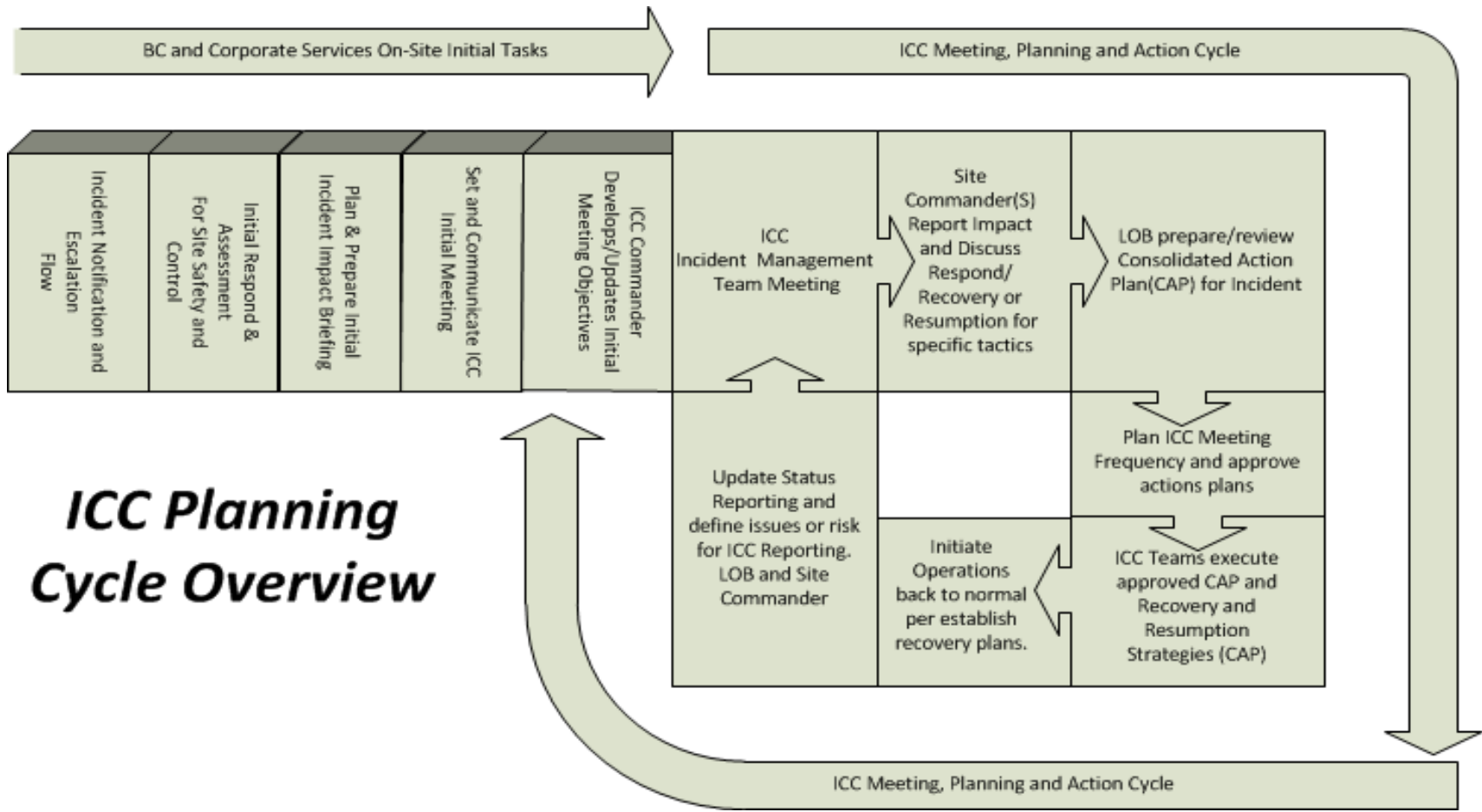
Incident Command & Control Team (Crisis Management)

Incident Command & Control (ICC) Organization



* Reference Region ICC Organization Team Roles within IMT Roles & Responsibility Section
 ** Alternate defined in unit Plan

Crisis Management Planning Flow (insert the P diagram)



ICC Planning Cycle Overview

Questions & Answers???

Thank You.

For more information, please contact:

Lilibett Machado, CISO, CISA, CISM CGEIT, ITIL
Chief Information Security Officer
713-871-3925 (O)
Lilibett.Machado@CadenceBank.com

Charity Otwell, ABCP
VP, Business Continuity Manager
205-488-3378 (O)
Charity.Otwell@CadenceBank.com

