plante moran | Audit. Tax. Consulting. Wealth Management.

Auditing Business Continuity Programs

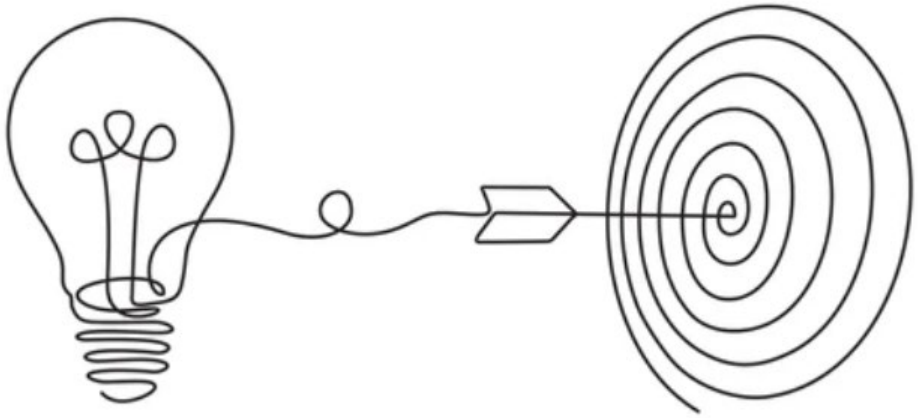
Presenter

Colin Taggart

Partner, Cybersecurity

Takeaway Goals

1. Outline of internal audit led BCP audit scope
2. Process to takeover audit responsibly from audit vendor
3. Key expectations for BCP content
4. Awareness of common issues found in BCP audits



Polling Question #1

How is your Business Continuity Program currently being audited?

A. Annually by Credit Union Internal Audit

B. On a multi-year rotation led by Credit Union Internal Audit

C. Annually by Internal Audit Vendor

D. On a multi-year rotation led by Internal Audit Vendor

E. Rotation between Internal Audit and Vendor

Audit - Migrating In-House

Independent assessment of following areas:

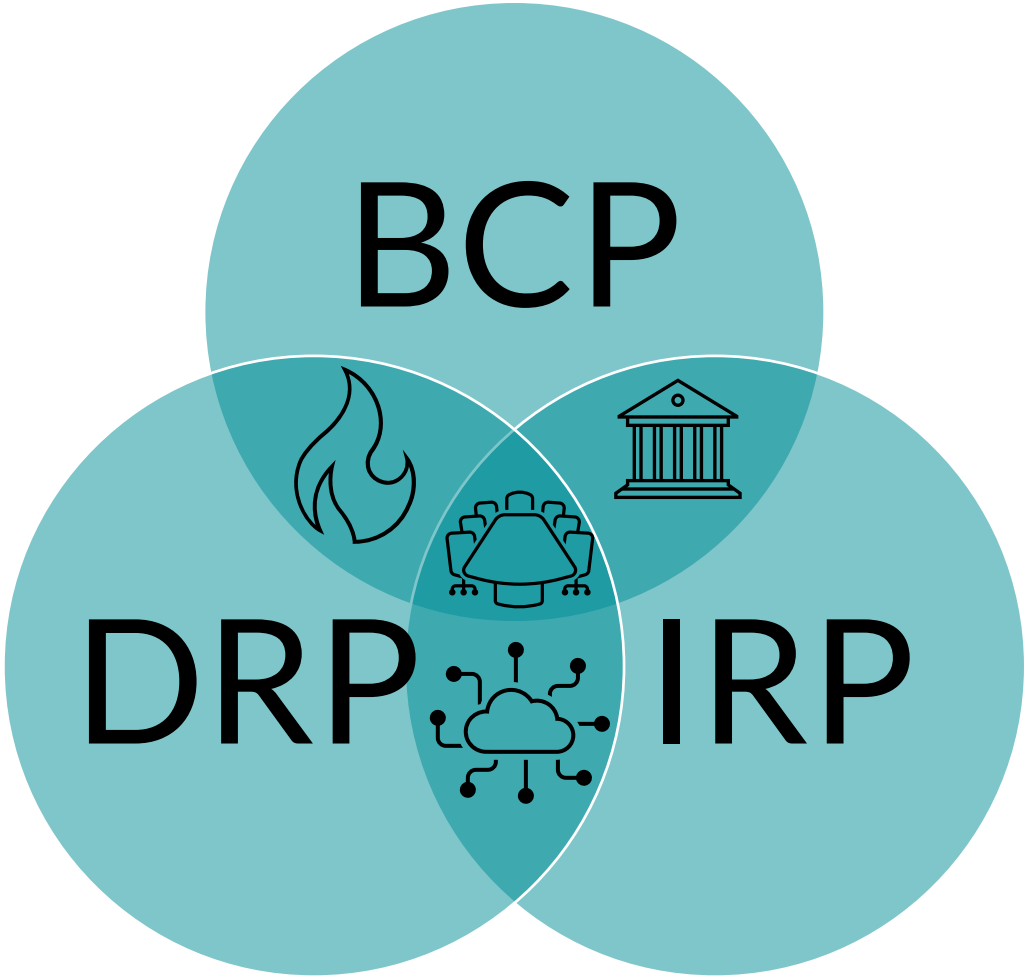
- BIA
- Risk assessments
- Controls supporting continuity and resilience
- Vendor supporting information
- Risk mitigation efforts compared to risk appetite
- Test plans and results
- Overall BCM program

Audit - Migrating In-House

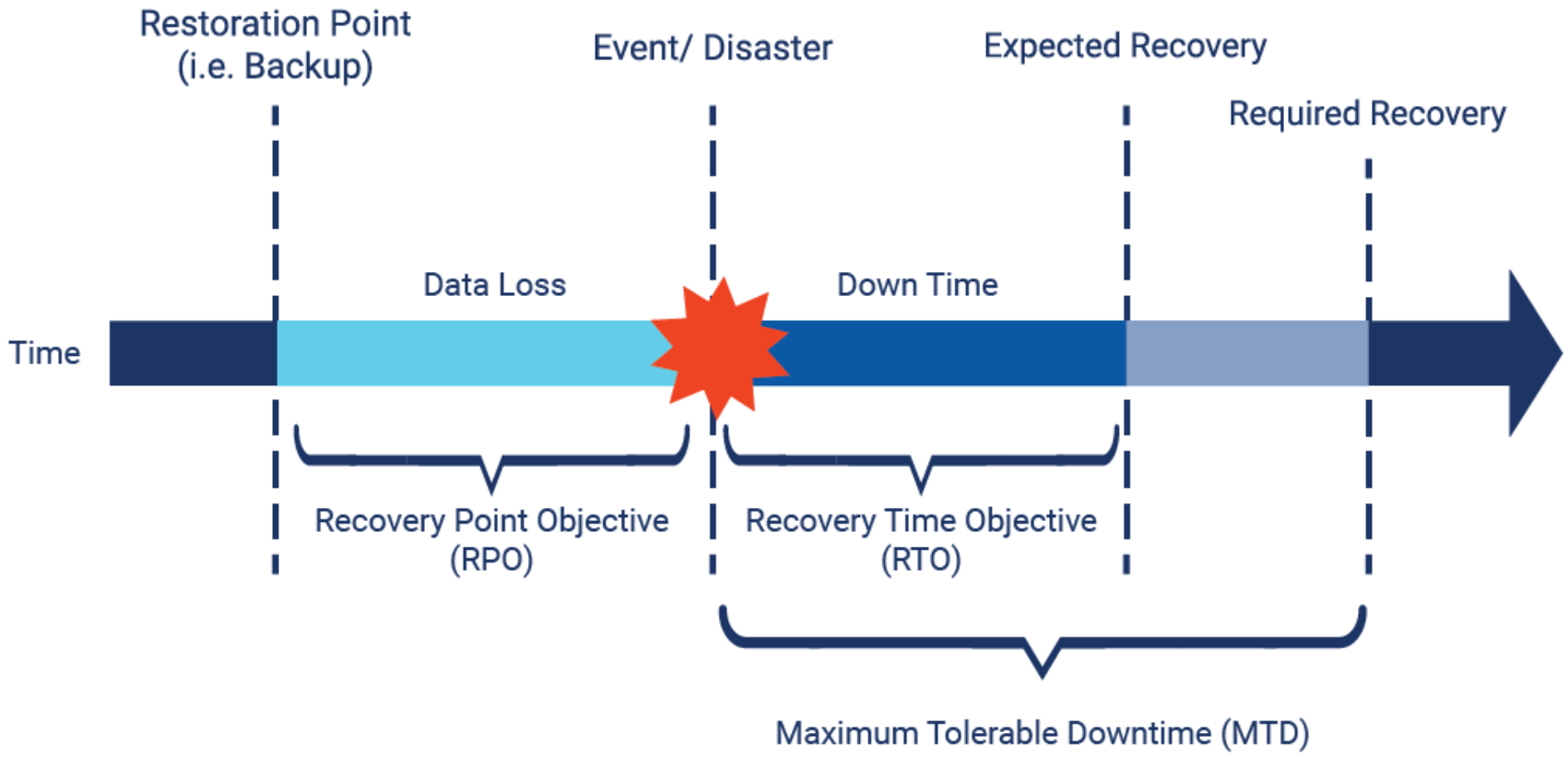
- Collaborative audit partner relationship
- Sharing audit procedures, prior year workpapers, etc.
- Co-sourced audit effort (including training)
- Rotational internal/external audit coverage

BCP Background

BCP vs. DRP vs. IRP

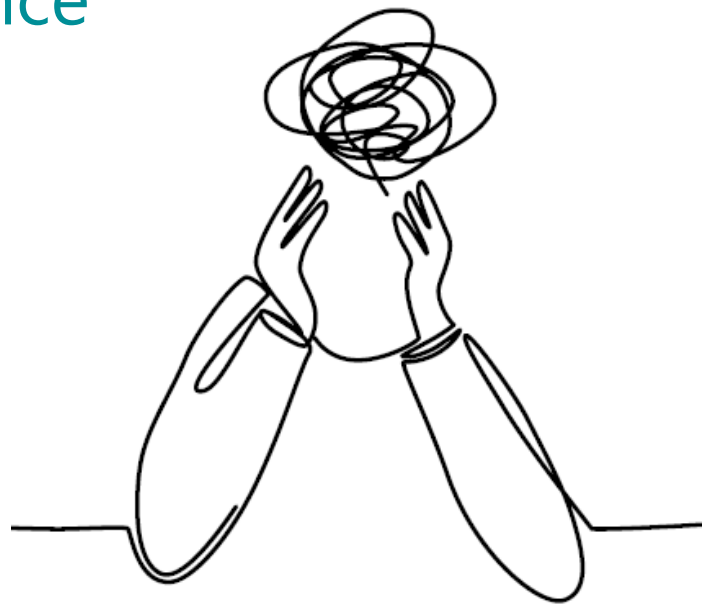


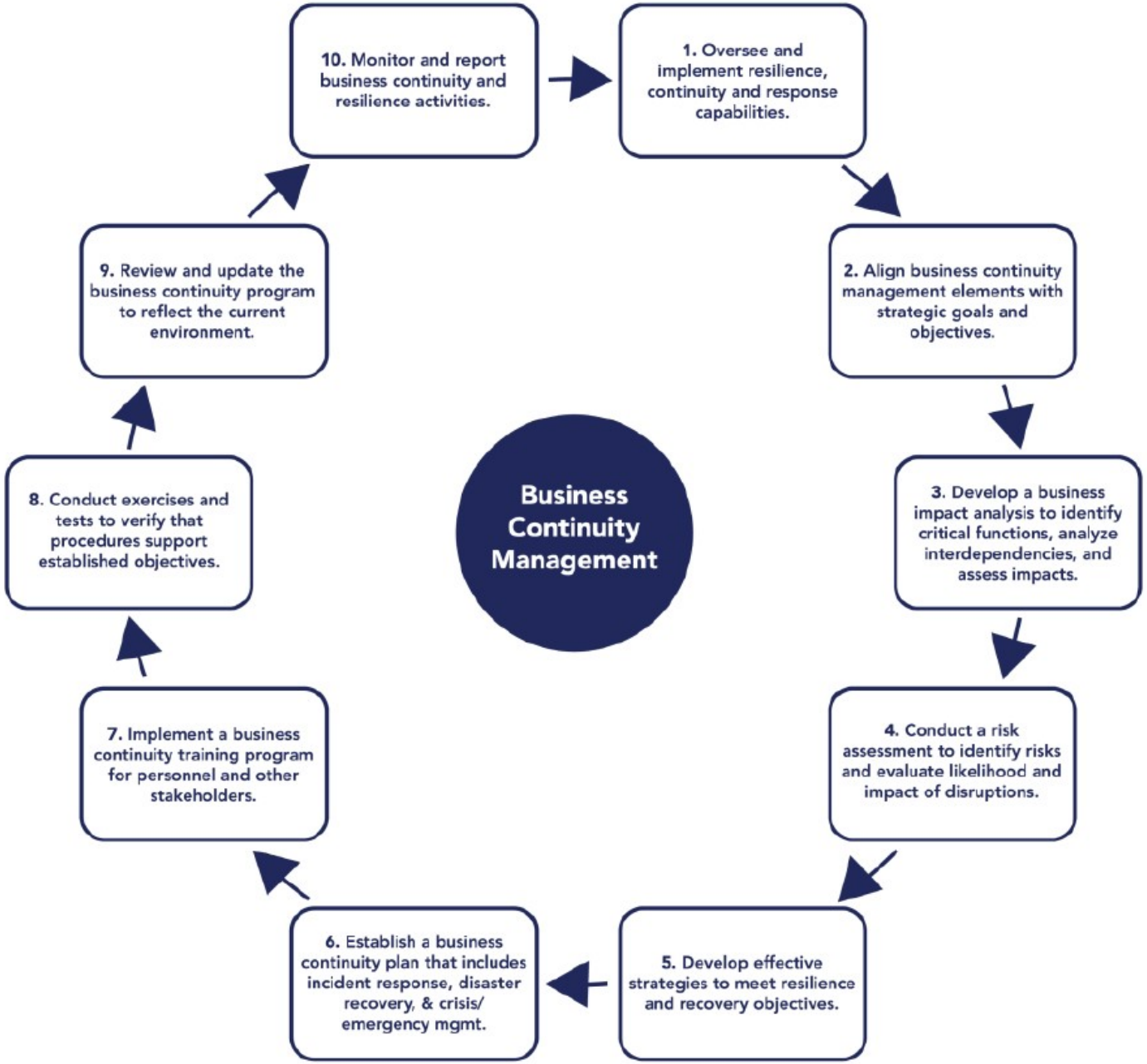
Key Concept Acronyms



Common Overall Issues

- Organization wide buy-in: Current relevant plans
- Template/excessive data – not used post-disaster
- BCP/DRP/IRP overlap over-reliance
- IT only focus




Business Continuity Management
1. Oversee and implement resilience, continuity and response capabilities.
2. Align business continuity management elements with strategic goals and objectives.
3. Develop a business impact analysis to identify critical functions, analyze interdependencies, and assess impacts.
4. Conduct a risk assessment to identify risks and evaluate likelihood and impact of disruptions.
5. Develop effective strategies to meet resilience and recovery objectives.
6. Establish a business continuity plan that includes incident response, disaster recovery, & crisis/ emergency mgmt.
7. Implement a business continuity training program for personnel and other stakeholders.
8. Conduct exercises and tests to verify that procedures support established objectives.
9. Review and update the business continuity program to reflect the current environment.
10. Monitor and report business continuity and resilience activities.

Board Oversight

1. Oversee and implement resilience, continuity and response capabilities

- Overall Leadership/Involvement
- Assigning Roles
- Allocating Resources & Knowledgeable Personnel
- Aligning BCM with Entity Strategy
- Understanding Risks & Adopting Policies
- Review Reporting/Testing/Auditing

- Provide a Credible Challenge to Management

Team Effort

Board

- Establish risk strategy

Executives

- Top-down support required

Business Units

- Input required from all areas

IT

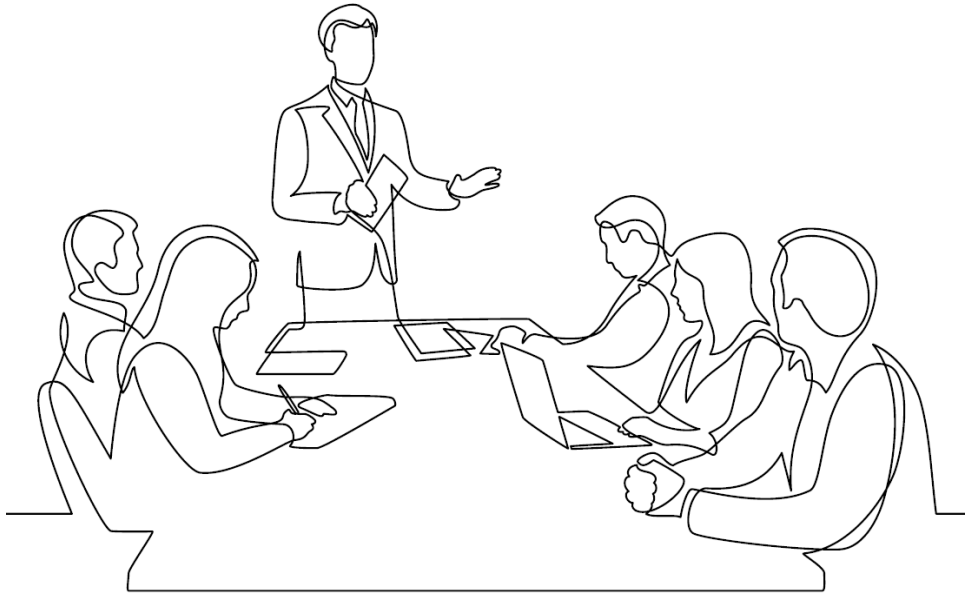
- Ensure infrastructure supports risk strategy

Board Reporting

10. Monitor and report business continuity and resilience activities

Written Presentation

- Business Impact Analysis
- Risk Assessment
- Business Continuity Plan
- Exercise + test results
- Identified issues/action plans



Common Issue: Board Involvement

Policies

The following policies were approved on a motion made by Mr. Martin, second by Mr. Finn; motion carried:

- Business Continuity Policy
- Disaster Recovery Plan
- Investment Policy
- Is Anyone Even Reading This Policy
- Salary Doubling Policy
- Three Day Workweek Policy

No Discussion or Questions?

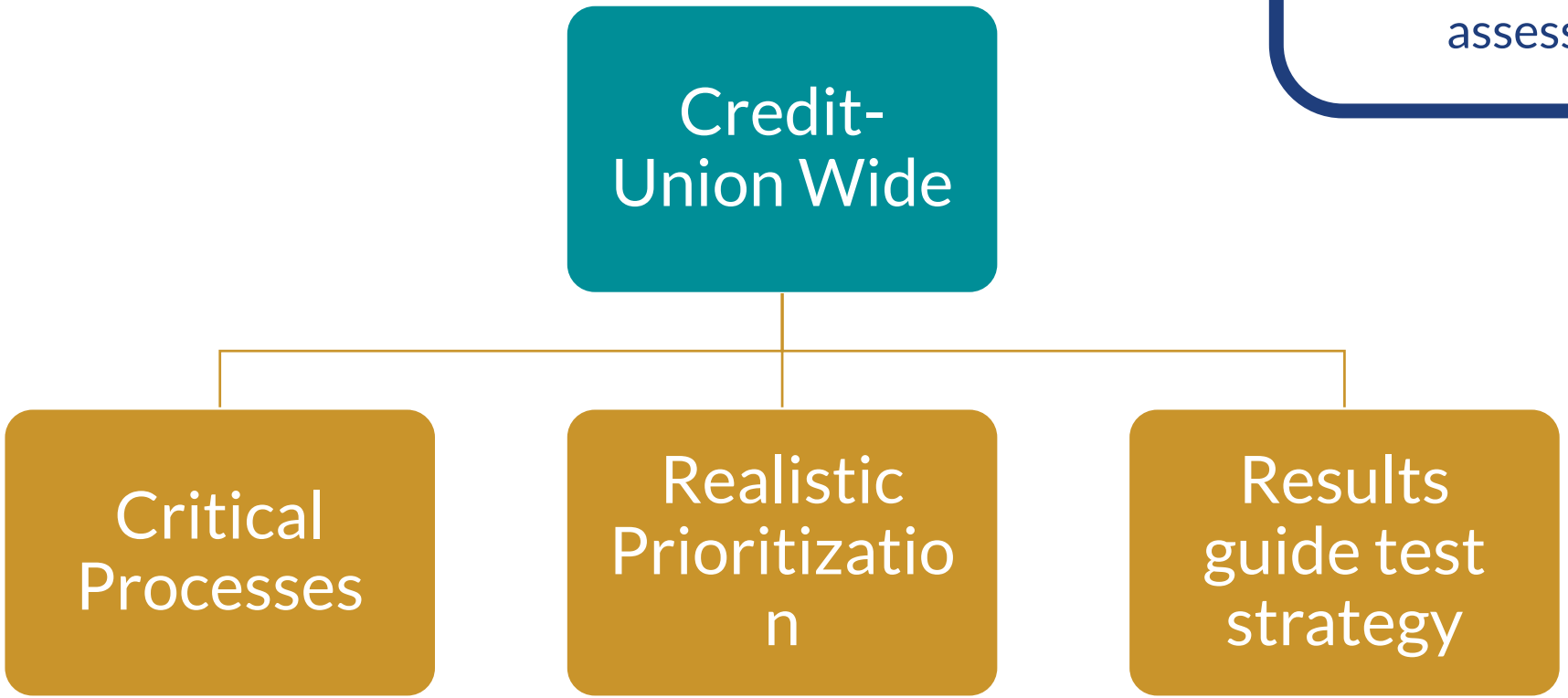
"A credible challenge involves being actively engaged, asking thoughtful questions, and exercising independent judgment."

Strategic Risk Management Alignment

2. Align business continuity management elements with strategic goals and objectives

Business Impact Analysis – What Matters?

3. Develop a business impact analysis to identify critical functions, analyze interdependencies and assess impacts.



Business Impact Analysis – What Do We Need?

Applications	• What systems does each business unit need to access?
Equipment	• What hardware is needed to complete operations? Does it change based on the type of scenario?
Connectivity	• What is the Maximum Tolerable Downtime (MTD) for each business unit?
Team members	• What is the minimum team required?
Vendors	• Where are we relying on third parties for critical business processes?

Common Issues: Business Impact Analysis

- IT only focus
- Completeness of critical business functions
- Missing interdependencies
- Reasonableness of recovery objectives
- Considering criticality of systems normally vs. post-disaster (Telephone Banking)

Risk Assessment

4. Conduct a risk assessment to identify risks and evaluate likelihood and impact of disruptions

- Geographically unique
- Vendor risks
- Natural disasters
- Technical events
- Malicious activity
- International events
- Low likelihood and high impact events (e.g., pandemic events).

Polling Question #2

What type of disasters are risk-rated the highest in your BCP risk assessments?

A. Natural disasters

B. Network/Internet/Communications outage

C. Pandemic

D. Vendor outage

E. Cybersecurity incident/breach

Common Issues: Risk Assessment

- Inherent vs. residual risk considerations
- Location specific risk considerations
- Missing vendor reliance/connectivity risks
- Risk appetite → Action plans to mitigate

Resilience and Recovery Strategies

5. Develop effective strategies to meet resilience and recovery objectives.

People

- Staffing
- Vendors

Processes

- Workaround system alternatives
- Communication protocols

Resilience and Recovery Strategies

Technology

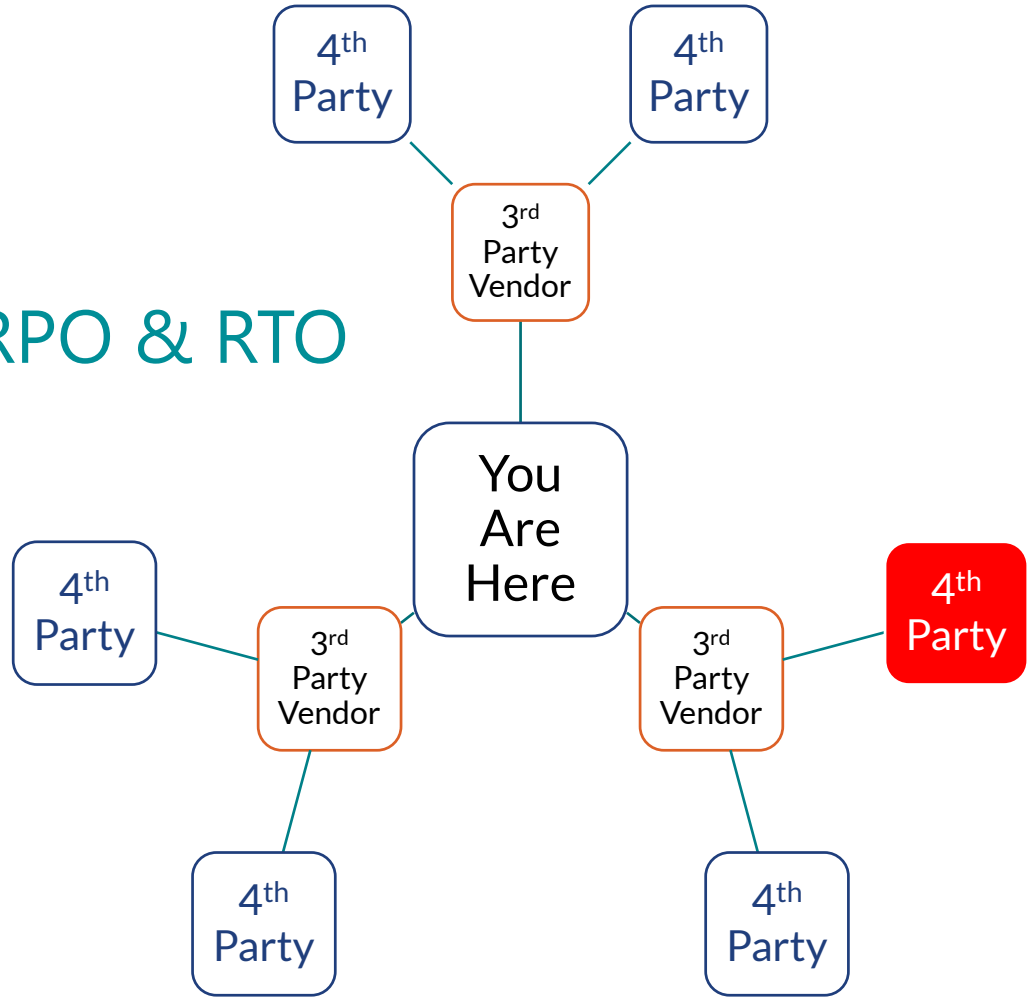
- Data backup & replication
- Cloud/offsite and offline recovery capabilities
- Cybersecurity resilience (ransomware mitigation)

Facilities & Connectivity

- Redundant telecommunications & power
- Geographic diversity

Vendor Reliance Strategies

- Vendor connectivity
- 4th party awareness
- Aligning SLA with Credit Union RPO & RTO
- Consider unique plans for
  - Credit Union disaster
  - Vendor disaster



Common Issues: Resiliency Plans

- Ongoing change management
- Testing failover plans with example of one vs. peak volume
- Single points of failure
- Weakened controls during failover plans

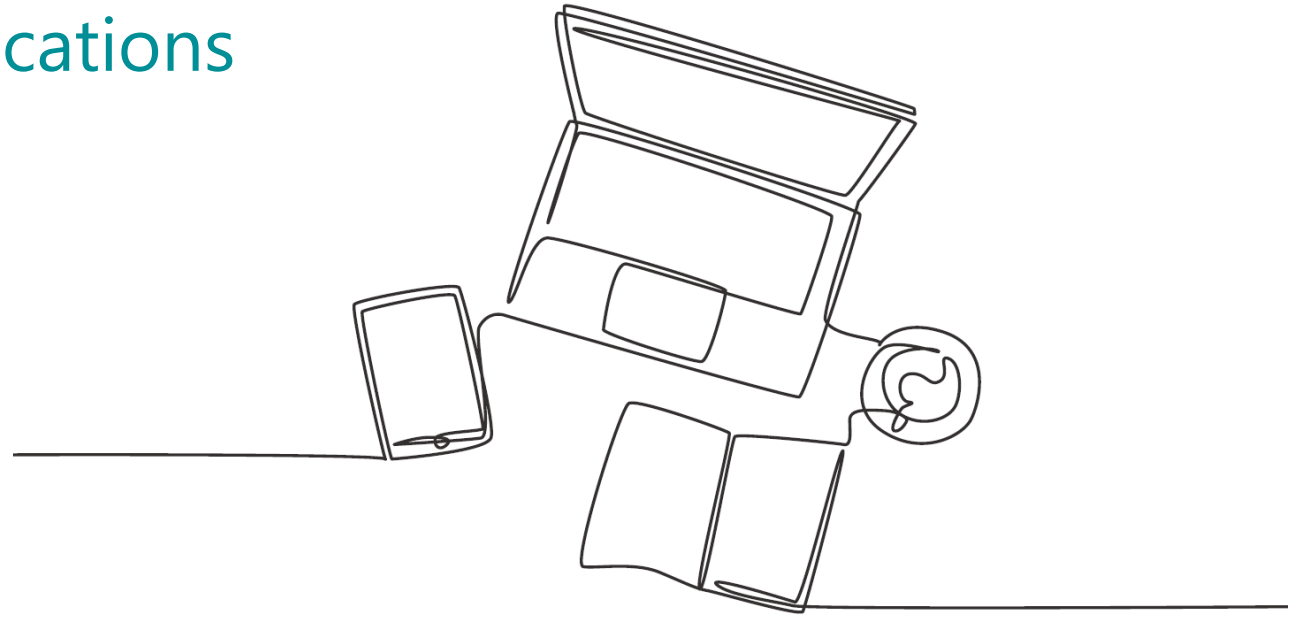
Business Continuity Plan

6. Establish a business continuity plan that includes incident response, disaster recovery & crisis / emergency mgmt.

- Roles and responsibilities
- Specific event solutions
- Immediate steps to protect personnel/members
- Critical information protection (Backups/DC recovery)
- Resumption of normal operations
- Alternative solutions – vendors, systems, personnel
- Site relocation plans – short/medium/long term

Communication Plans

- Employee communication channels
- Member/public communications
- Regulatory agencies
- Critical third parties



BCP Appendices/Related Documents

- Incident response plan
- Disaster recovery plan
- Departmental procedures
- Detailed based on risk, including manual procedures
- Actionable procedures

Common Issues: BCP Contents

"Business continuity plans and procedures should be clear, concise, accessible, and easy to implement in an emergency"

- Outsourced plan oversight
- Plans (content + actual strategies) aligns with risk

Polling Question #3

What type of training is relied upon most for your BCP responsibilities?

A. Online vendor-developed content

B. Online Credit Union-developed content

C. In person all-employee training

D. In person departmental training

E. Other

Business Continuity Training

7. Implement a business continuity training program for personnel and other stakeholders.

	All Employees	Executives	Board	Department-Specific	Branch-Specific
Overall Strategies	X		X		
Communication Plan	X				
Governance Responsibilities		X	X		
Detailed Procedures				X	X
Evacuation Plans					X
Relocation Strategies					X
Cross-Training				X	X

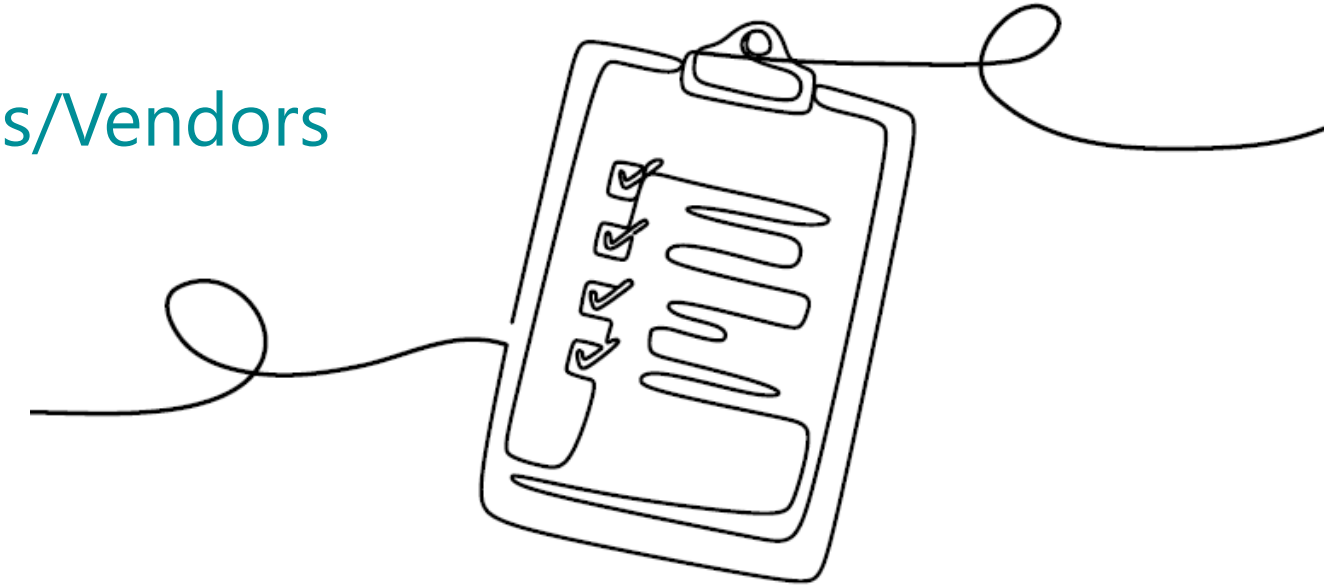
Common Issues: Training

- Canned generic online course
- Sole focus on cross-training vs. failover
- Low priority after turnover and system conversions

BCP: Testing Program

8. Conduct exercises and tests to verify that procedures support established objectives.

- Defined Program
- Coverage of Critical Processes (1-3 Year Horizon)
- Risk-Based Decisions
- Changes in Team/Systems/Vendors



BCP: Testing Program

- ✓ Roles
- ✓ Safeguarding production data
- ✓ Testing realistic/peak volume of activities
- ✓ Successful test expectations - RTO/RPO/SLA/MTD
- ✓ Training validation
- ✓ Detailed test plans
- ✓ Realistic scenarios
- ✓ Lessons learned

Program Testing

Risk-based program – frequency and scope

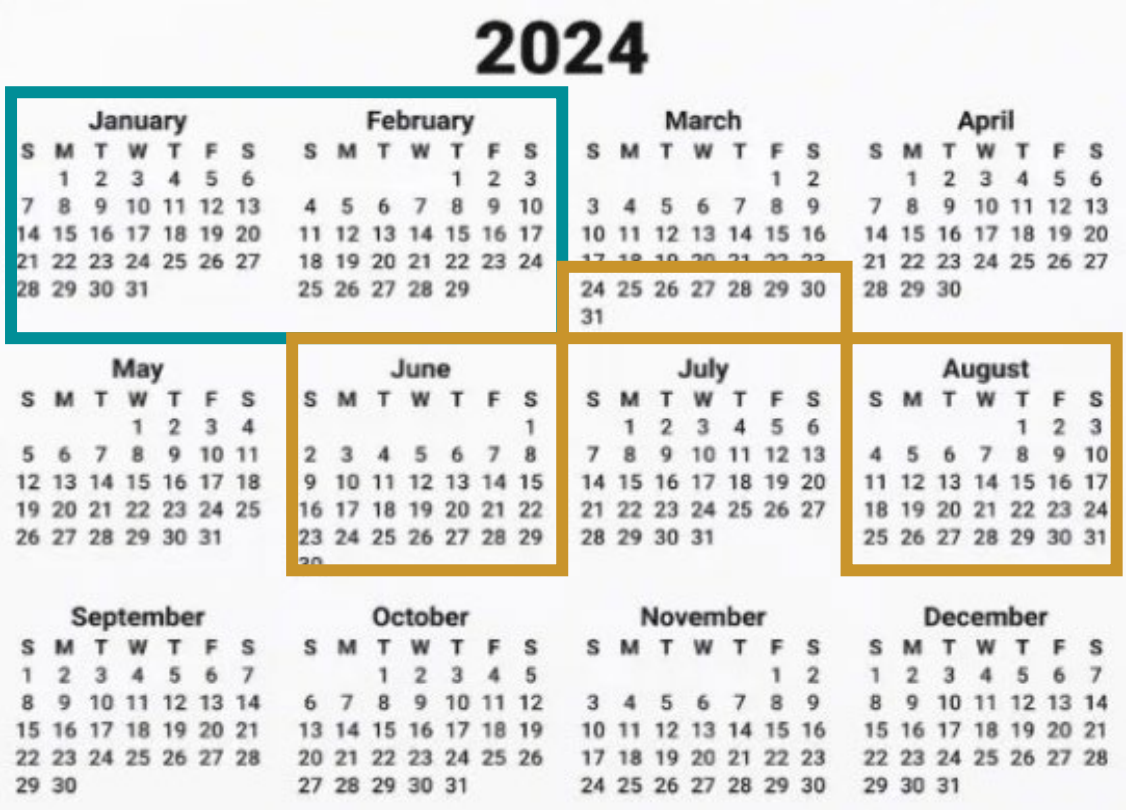
- ✓ Full-scale exercise
- ✓ Targeted exercise
- ✓ Tabletop walkthroughs
- ✓ System resilience tests (Data backups, manual workarounds, backup power)
- ✓ Third-party testing

Common Issues: Testing

- ✓ SALY
- ✓ Data backup focused
- ✓ Easy tabletop scenarios
- ✓ Accepted vendor generic test results

Program Maintenance

9. Review and update the business continuity program to reflect the current environment.

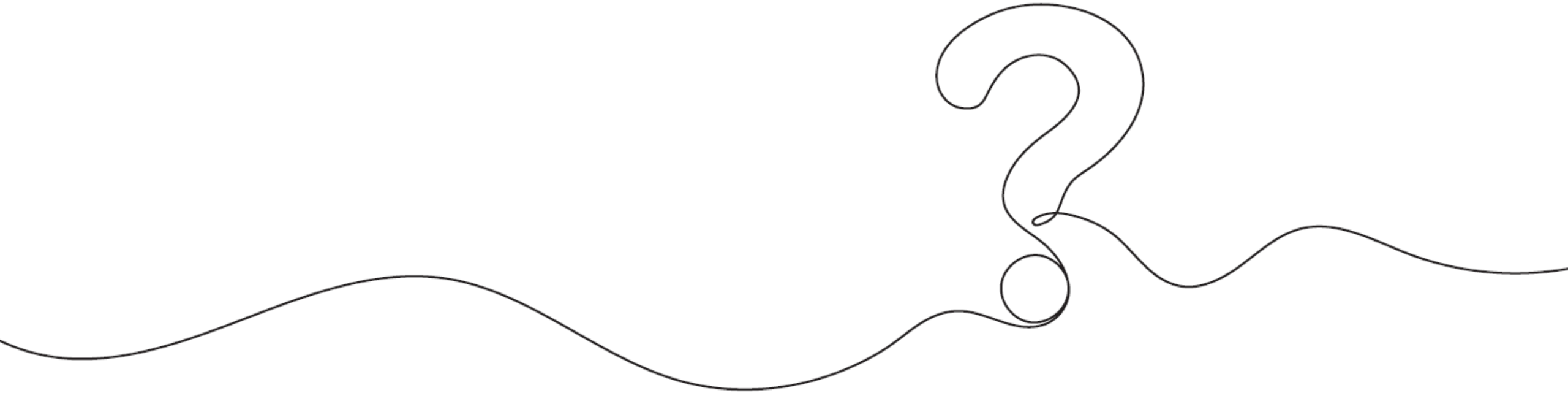


- Annual update efforts
- New branch
- Implement ITM's
- Replace key application vendor
- Turnover in key IT role

Recap on Common Issues

- Organization wide buy-in: Current relevant plans
- Template/excessive data – not used post-disaster
- IT only focus
- Limited training/testing

Questions?



Thank you!

Colin Taggart

Colin.Taggart@plantemoran.com

248-223-3235