Contingency Planning

State Of Arizona

Office Of The Auditor General

Jennie Snedecor & Katie Morris

ARIZONA
Auditor General
Making a Positive Difference

IT Controls Webinar Series

Part I – Overview of IT Controls and Best Practices

Part II – Identifying Users and Limiting Access

Part III – Network Controls

Part IV – Contingency Planning

ARIZONA AuditorGeneral

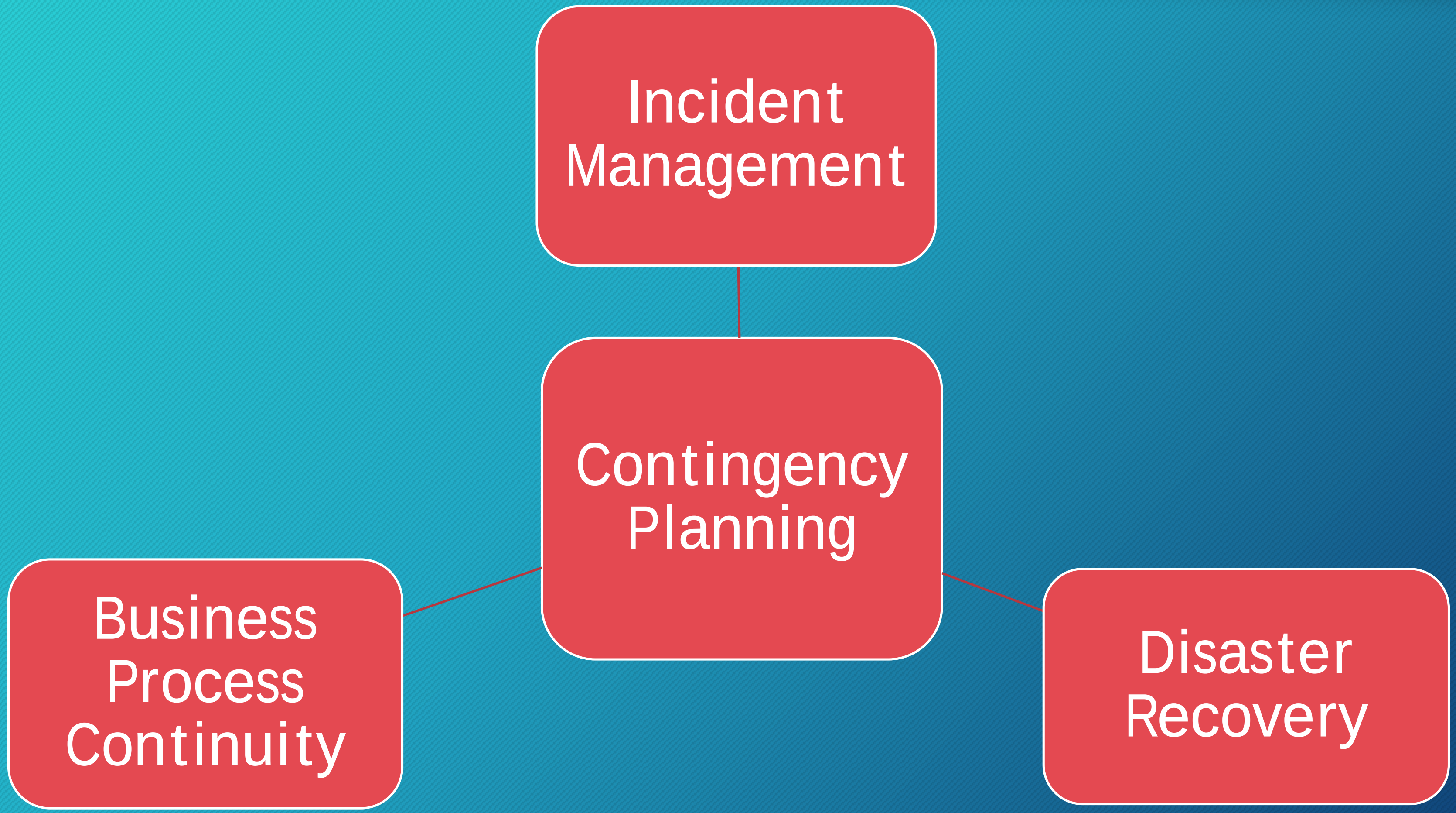
Making a Positive Difference

Contingency Planning Issues Covered in this Webinar

- What is Contingency Planning and why is it important?
- Creating a Contingency Plan (CP)
- Testing the Contingency Plan
- Best practices, tools, and resources

ARIZONA AuditorGeneral
Making a Positive Difference

What is Contingency Planning?



Incident Management

Contingency Planning

Business Process Continuity

Disaster Recovery

ARIZONA Auditor General

Making a Positive Difference

What is Contingency Planning

- Procedures and measures may include:
  - Use of alternate equipment
  - Use of alternate/manual processing
  - Moving to an alternate location
  - Implementing controls

What is a Disruption (in relation to IT)?

Interruption of service or destruction of hardware

Adversarial

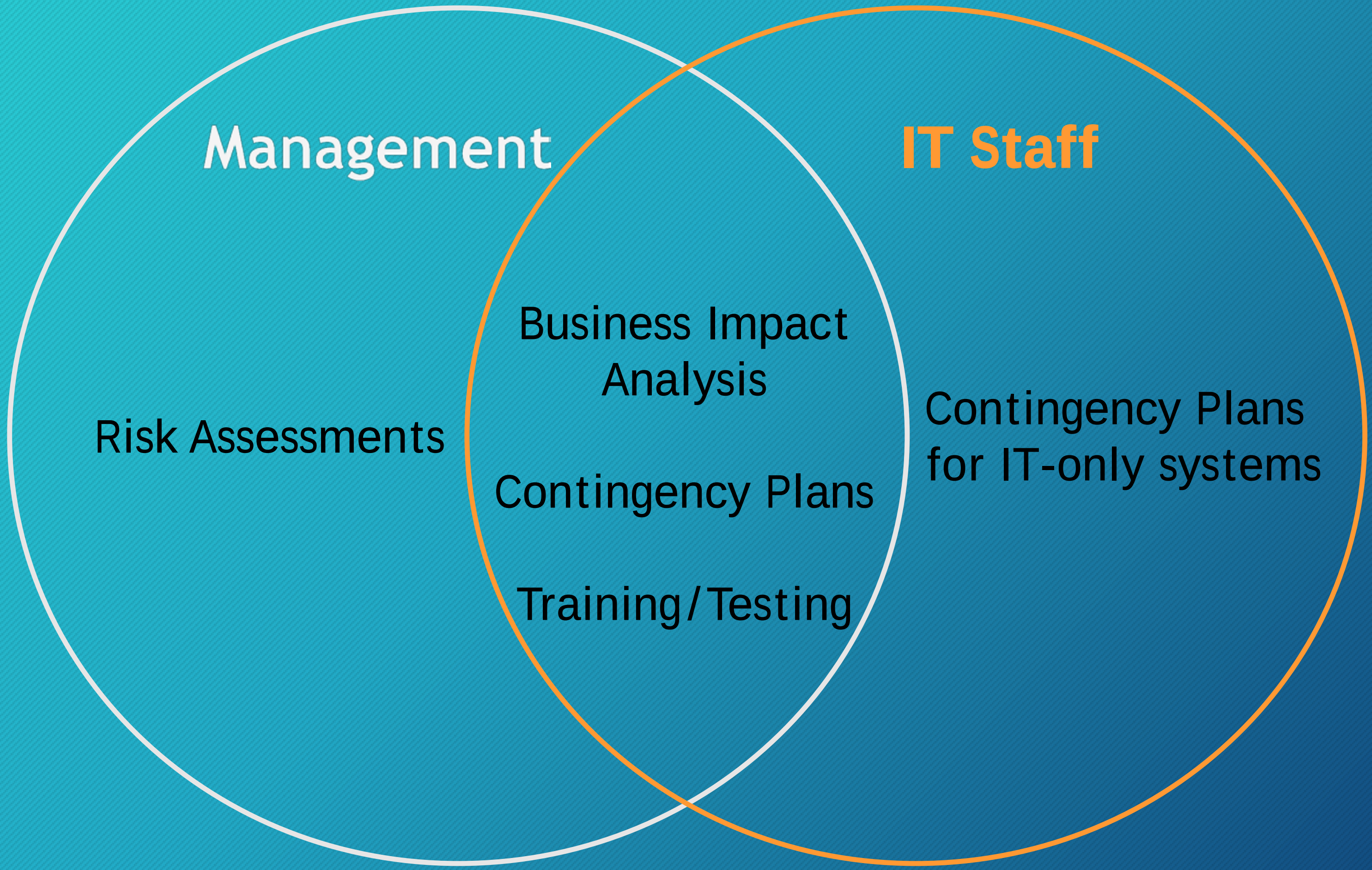
Accidental

Structural

Environmental

ARIZONA
AuditorGeneral
Making a Positive Difference

Management and IT roles in Contingency Planning



Management

IT Staff

Risk Assessments

Business Impact Analysis

Contingency Plans

Training/Testing

Contingency Plans for IT-only systems

Risk Management

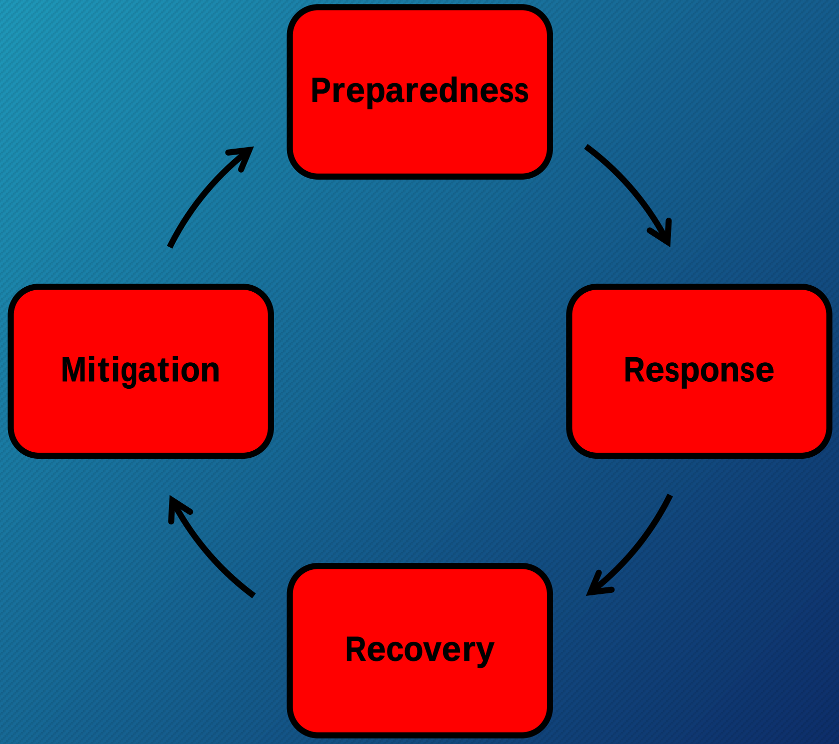
Disruption /Threat	Threat Type	Range of Effects	Likelihood of occurrence	Vulnerabilities	Severity	Likelihood Event Results in Adverse Impact	Overall Likelihood	Level of Impact	Risk
lightning at Data Center	Environ-mental	High	Moderate	Contingency Plan does not exist for all systems	High	High	Moderate	Moderate	Moderate

ARIZONA Auditor General Making a Positive Difference

NIST SP 800-30r1 and NIST SP 800-39

Why is Contingency Planning important?

- Reduces risk system and service unavailability
- Minimizes effect of system and service unavailability
- Allows for continuity of operations
- Prevents worsening the actual disruption



Preparedness

Response

Recovery

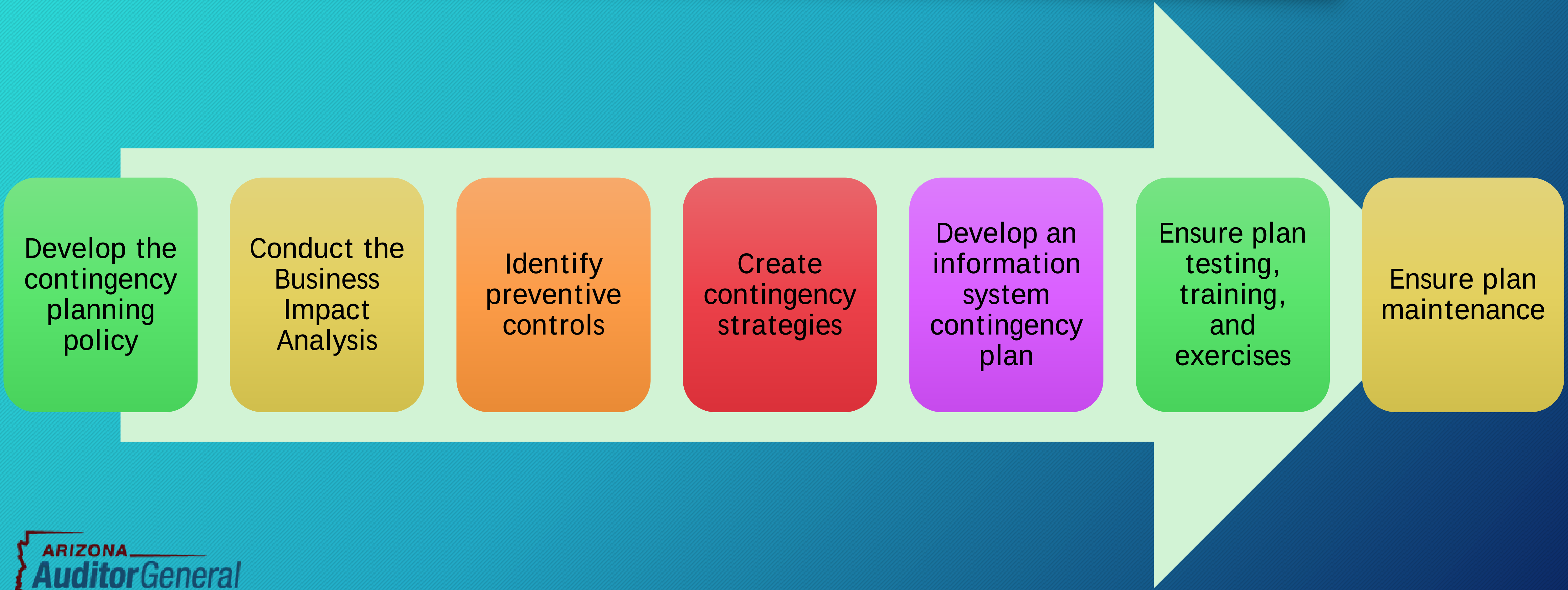
Mitigation

Does One Size Fit All?

Contingency plans should:

- Fit the size of the district
- Be tailored to the district’s needs
- Address individual information systems

Contingency Planning Process



Develop the contingency planning policy

Conduct the Business Impact Analysis

Identify preventive controls

Create contingency strategies

Develop an information system contingency plan

Ensure plan testing, training, and exercises

Ensure plan maintenance

ARIZONA Auditor General
Making a Positive Difference

Develop the Contingency Planning Policy

Roles and Responsibilities

Scope

Resource Requirements

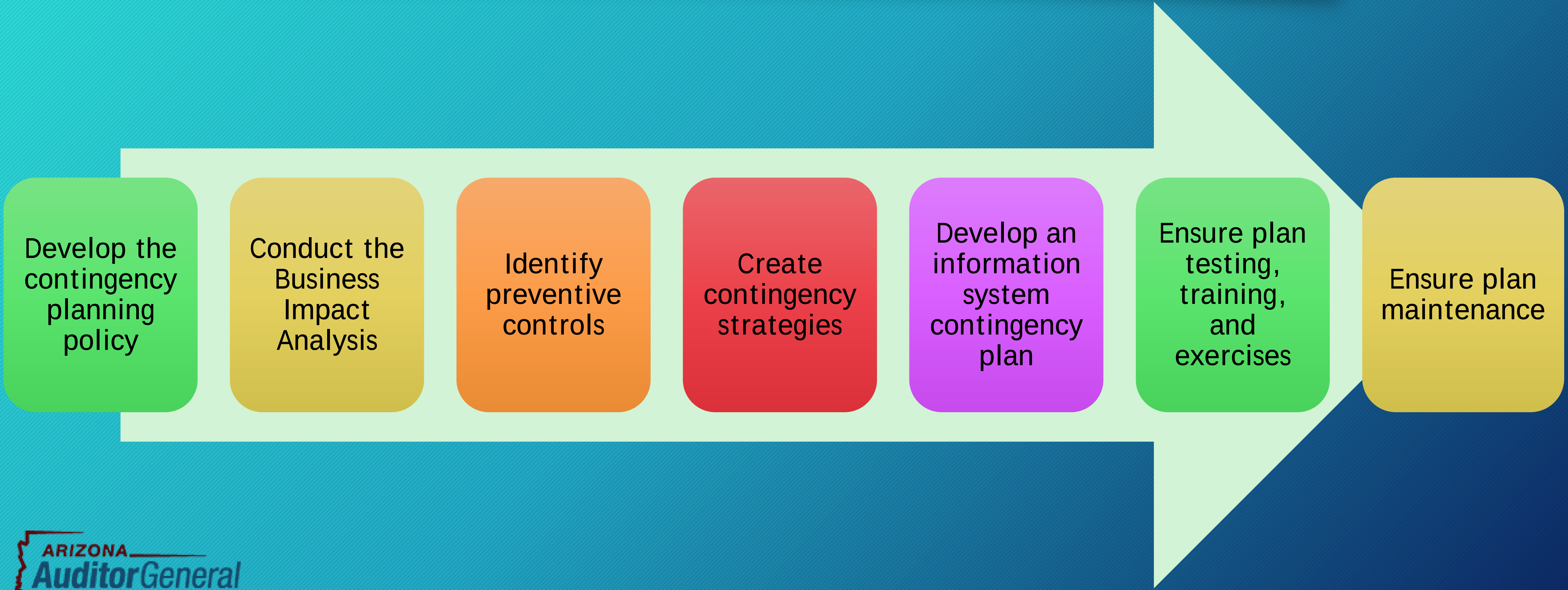
Training Requirements

Testing Schedules

Plan Maintenance Schedule

Backup Requirements

Contingency Planning Process



Develop the contingency planning policy

Conduct the Business Impact Analysis

Identify preventive controls

Create contingency strategies

Develop an information system contingency plan

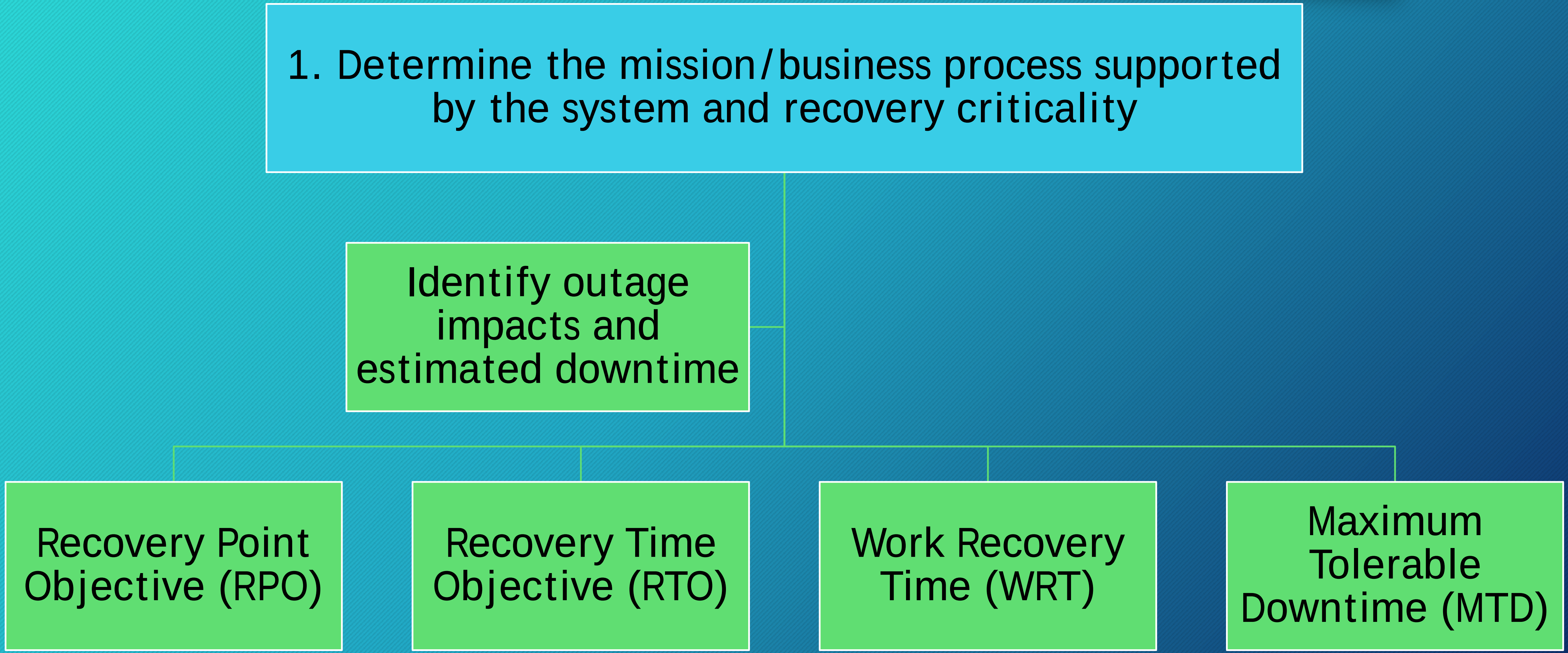
Ensure plan testing, training, and exercises

Ensure plan maintenance

ARIZONA Auditor General

Making a Positive Difference

Conduct the Business Impact Analysis



1. Determine the mission/business process supported by the system and recovery criticality

Identify outage impacts and estimated downtime

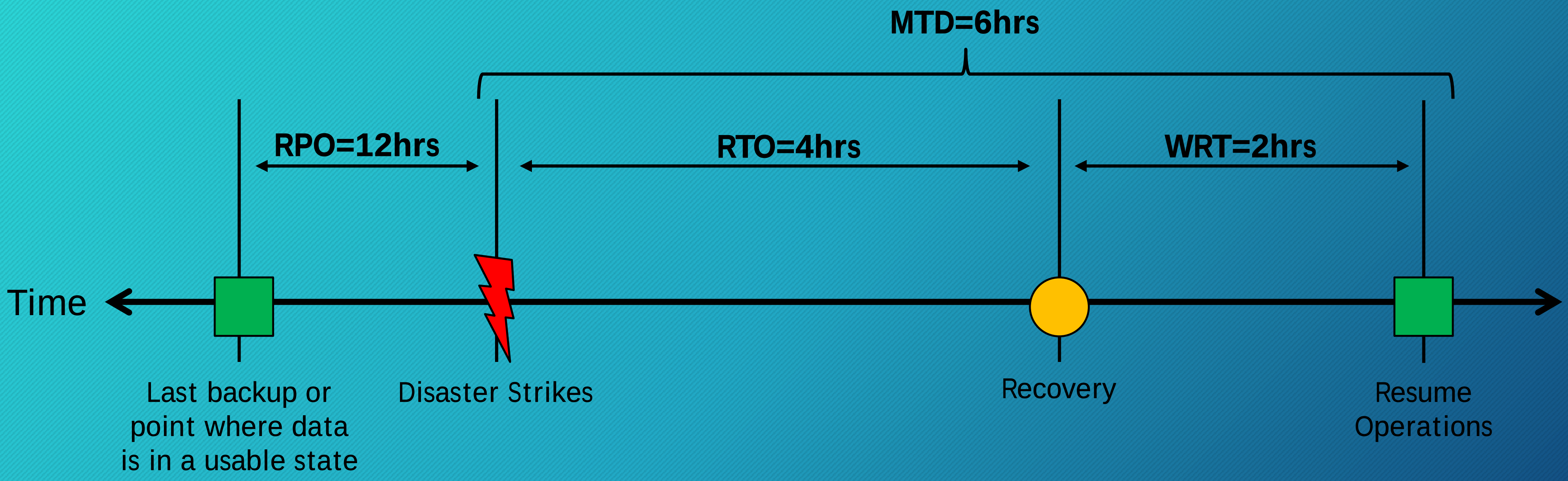
Recovery Point Objective (RPO)

Recovery Time Objective (RTO)

Work Recovery Time (WRT)

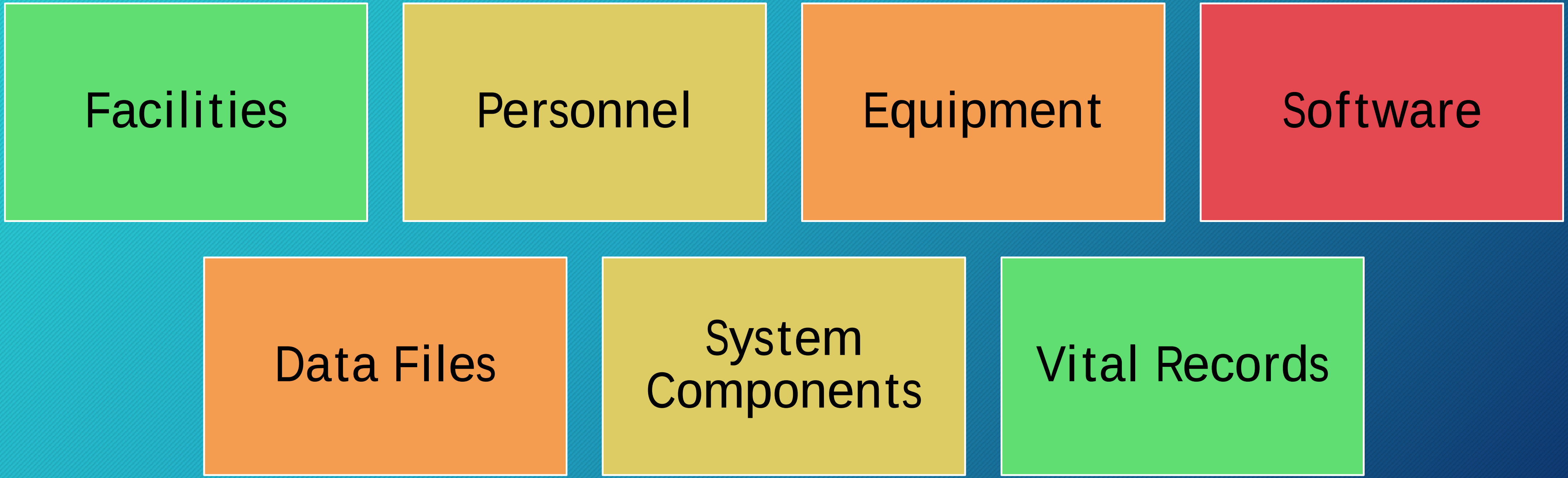
Maximum Tolerable Downtime (MTD)

Conduct the Business Impact Analysis – Estimated Downtime



Conduct the Business Impact Analysis

2. Identify resources required to resume mission/business processes:



Facilities

Personnel

Equipment

Software

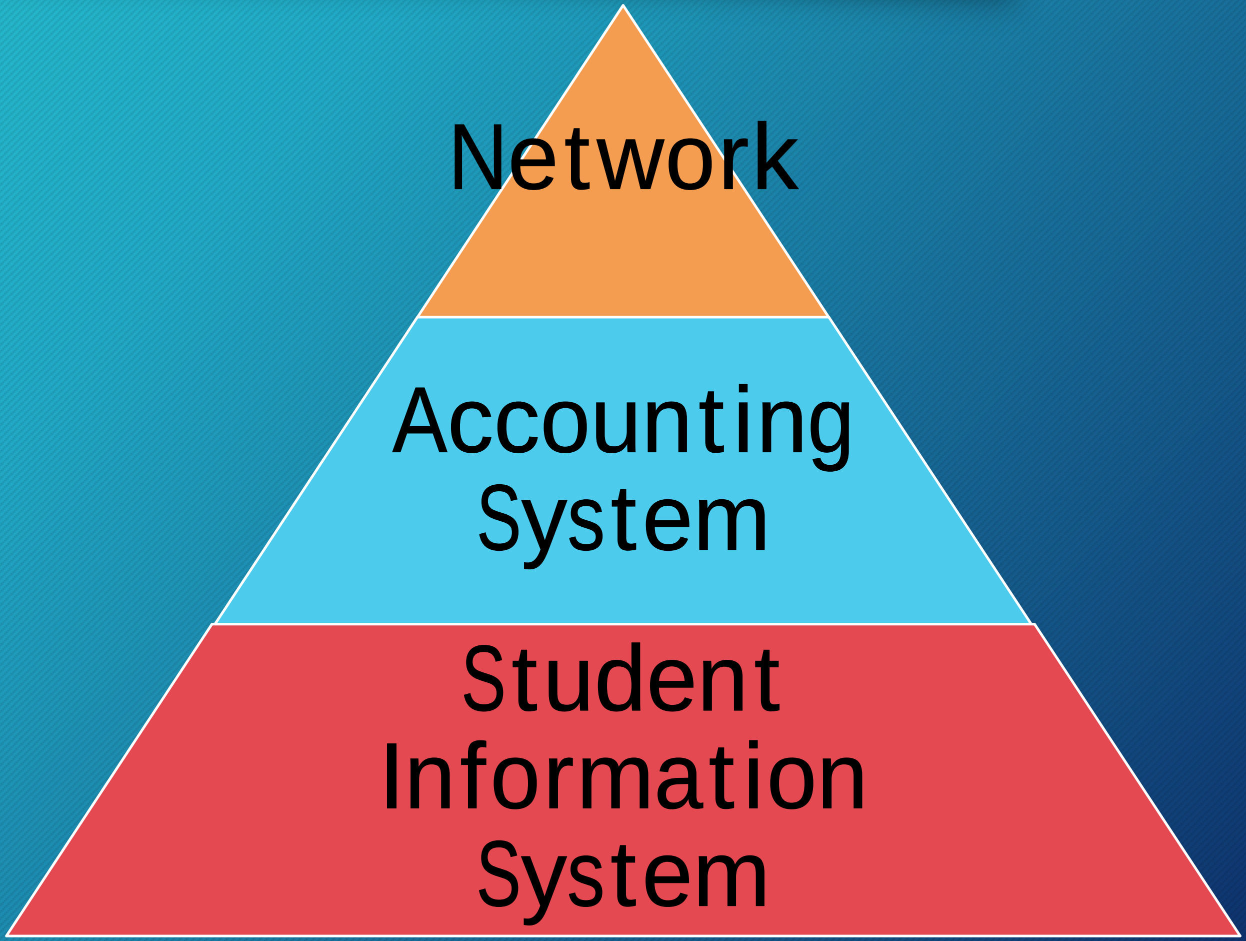
Data Files

System Components

Vital Records

Conduct the Business Impact Analysis

3. Identify recovery priorities: Creating a system recovery hierarchy based on critical business processes, outage impacts, MTD, and system resources

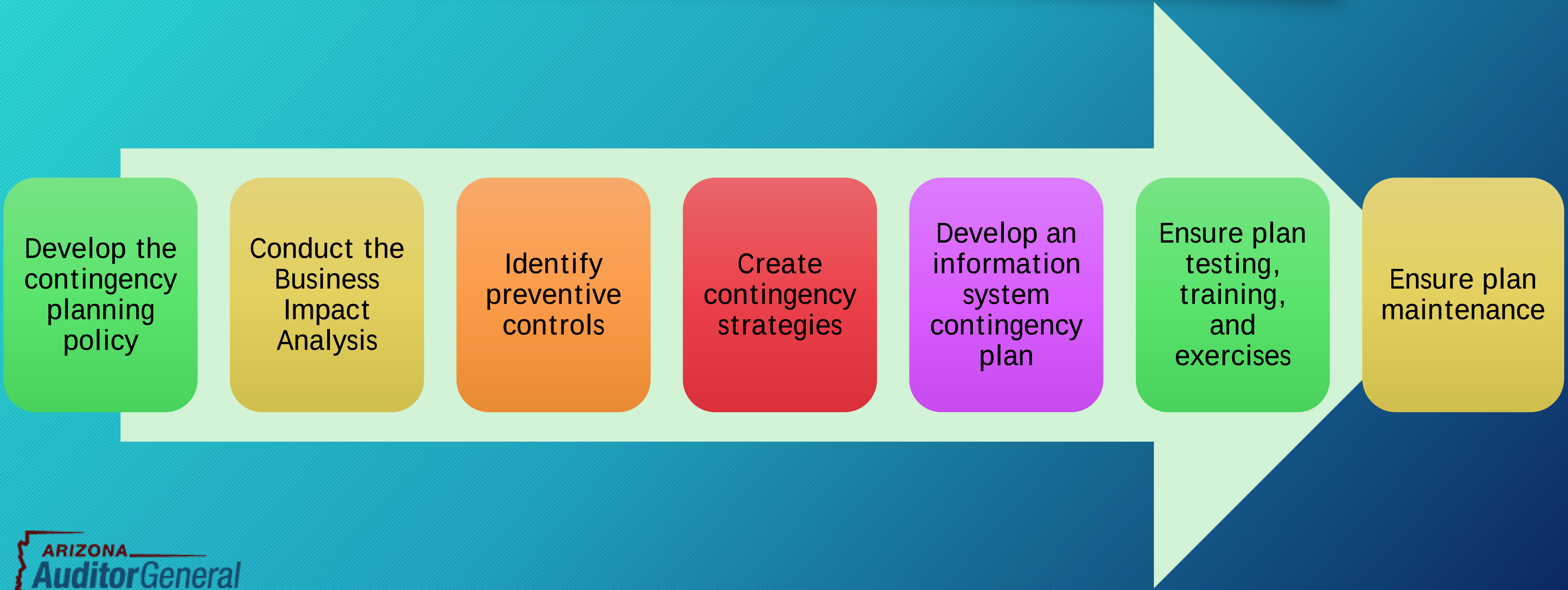


Network

Accounting System

Student Information System

Contingency Planning Process



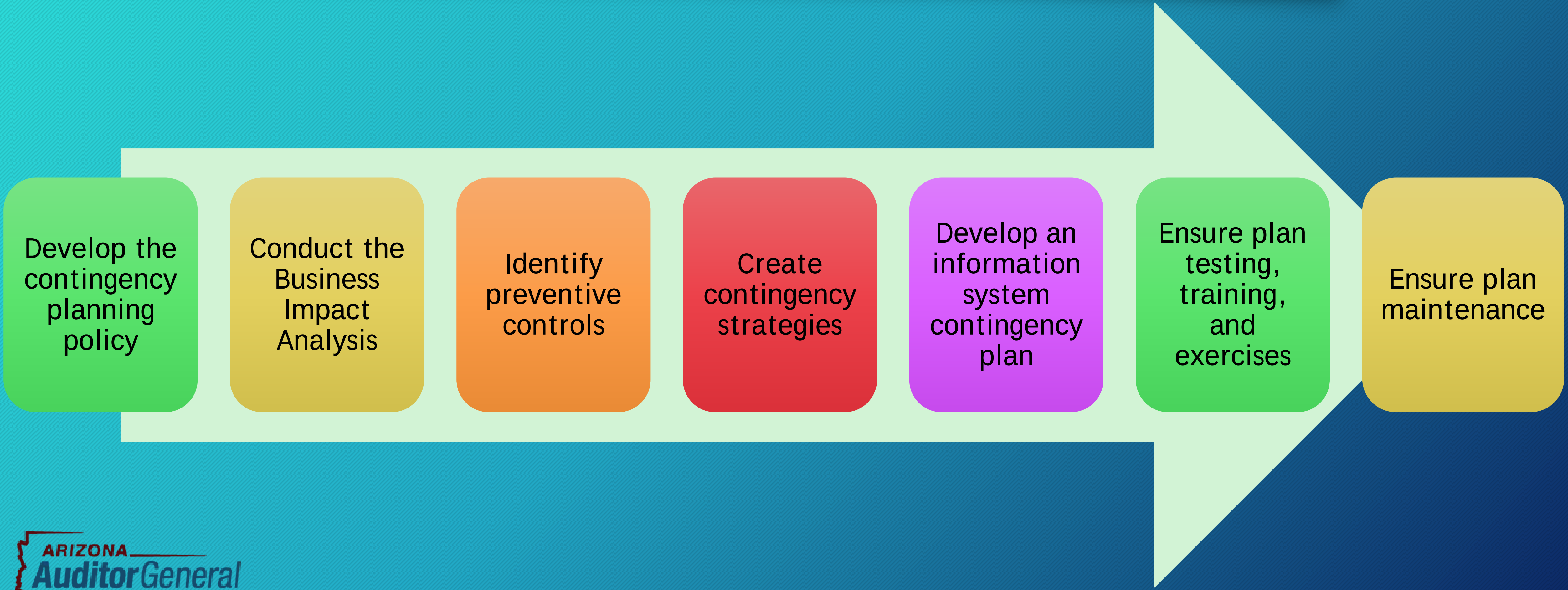
1. Develop the contingency planning policy
2. Conduct the Business Impact Analysis
3. Identify preventive controls
4. Create contingency strategies
5. Develop an information system contingency plan
6. Ensure plan testing, training, and exercises
7. Ensure plan maintenance

Identify Preventative Controls

Environmental Controls

- Protect power equipment and cabling
- Short-term uninterruptible power supply (UPS)
- For data centers, server rooms, and mainframe computer rooms provide:
  - Emergency shutoff switches
  - Automatic emergency lighting
  - Fire suppression and detection devices
  - Temperature and humidity levels monitoring
  - Master shutoff for water or isolation valves

Contingency Planning Process



1. Develop the contingency planning policy
2. Conduct the Business Impact Analysis
3. Identify preventive controls
4. Create contingency strategies
5. Develop an information system contingency plan
6. Ensure plan testing, training, and exercises
7. Ensure plan maintenance

Create Contingency Strategies

Backups

- Policies should designate:
  - Frequency
  - Scope
  - Location of stored data
  - File naming
  - Rotation frequency
  - Method for transporting data offsite

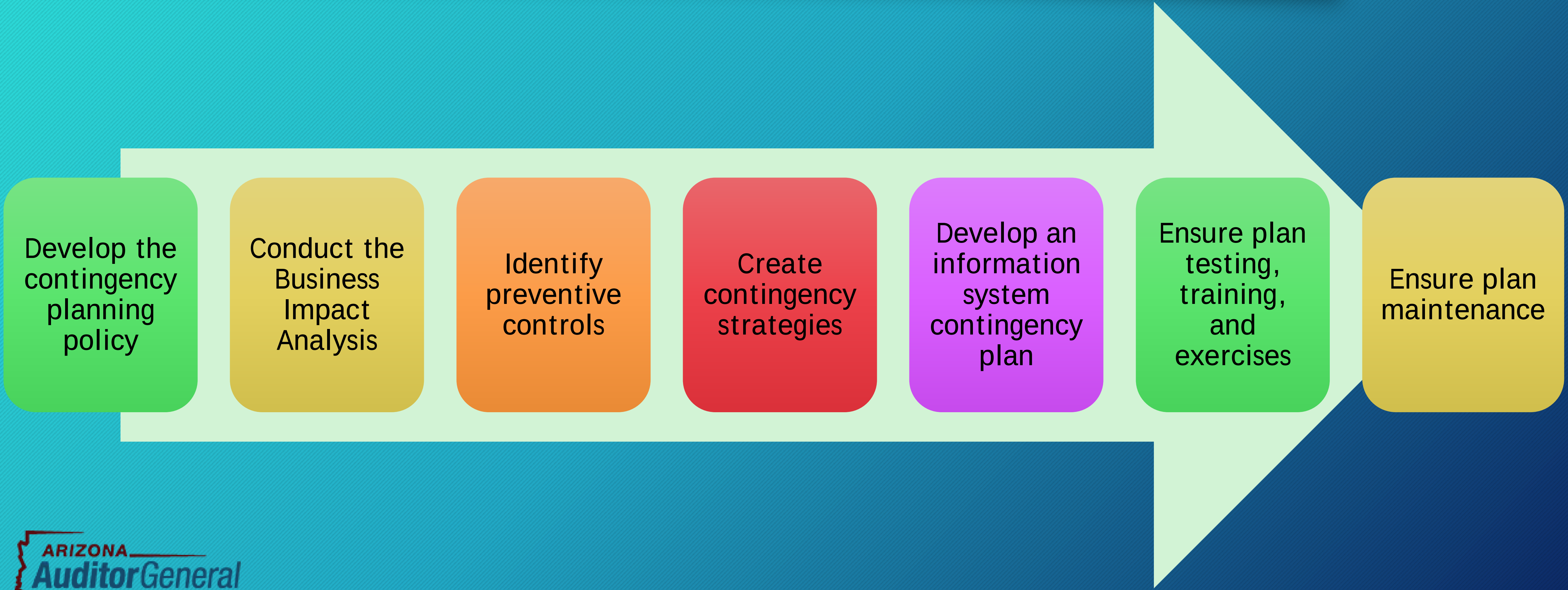
Alternate Processing Site

- Cold sites
- Warm sites
- Hot sites
- Mirrored sites

Third Party Agreements

- Specify emergency maintenance service
- For third party hosts (including county) - Contingency Plan is still required
- Responsibilities of each party included in plan and vendor contracts

Contingency Planning Process



Develop the contingency planning policy

Conduct the Business Impact Analysis

Identify preventive controls

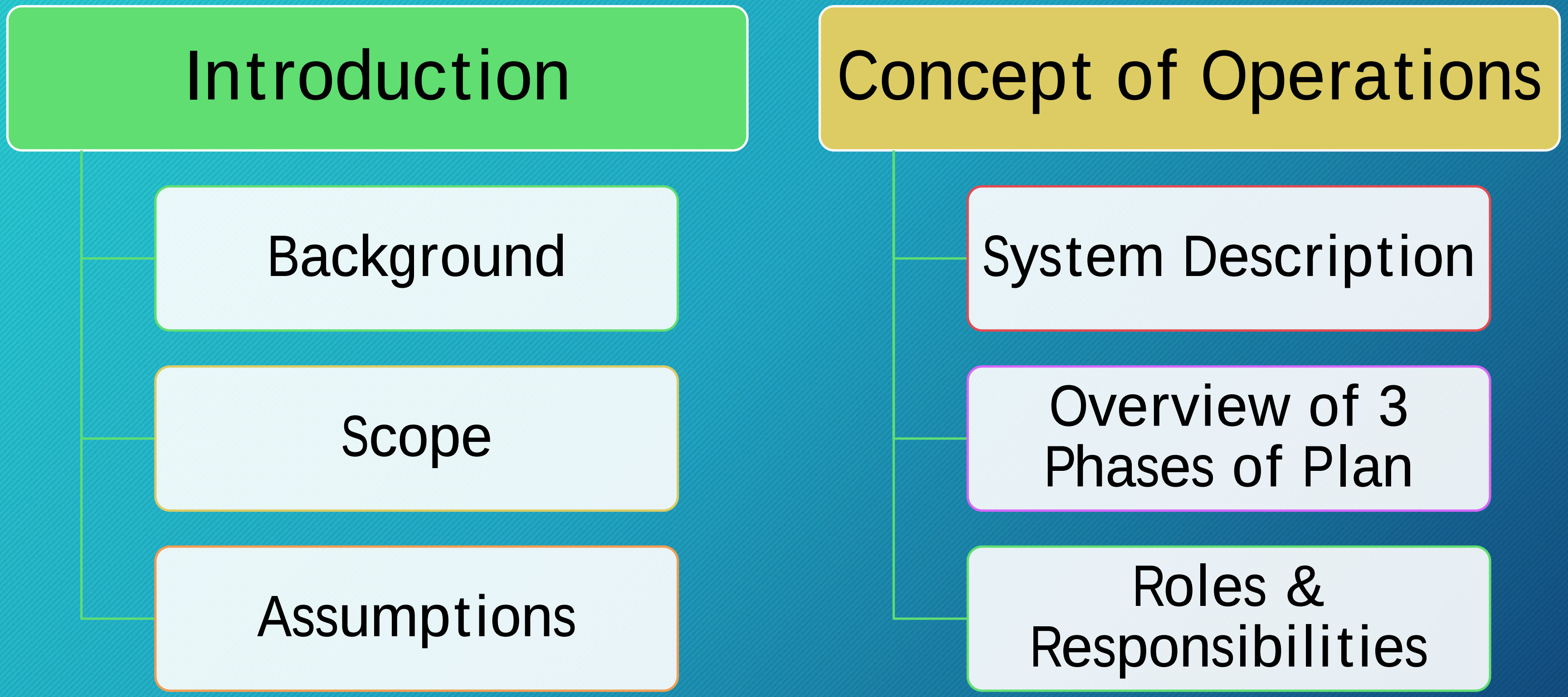
Create contingency strategies

Develop an information system contingency plan

Ensure plan testing, training, and exercises

Ensure plan maintenance

Developing a Contingency Plan – Supporting Information



Introduction

- Background
- Scope
- Assumptions

Concept of Operations

- System Description
- Overview of 3 Phases of Plan
- Roles & Responsibilities

Developing a Contingency Plan – Activation and Notification

Activation Criteria

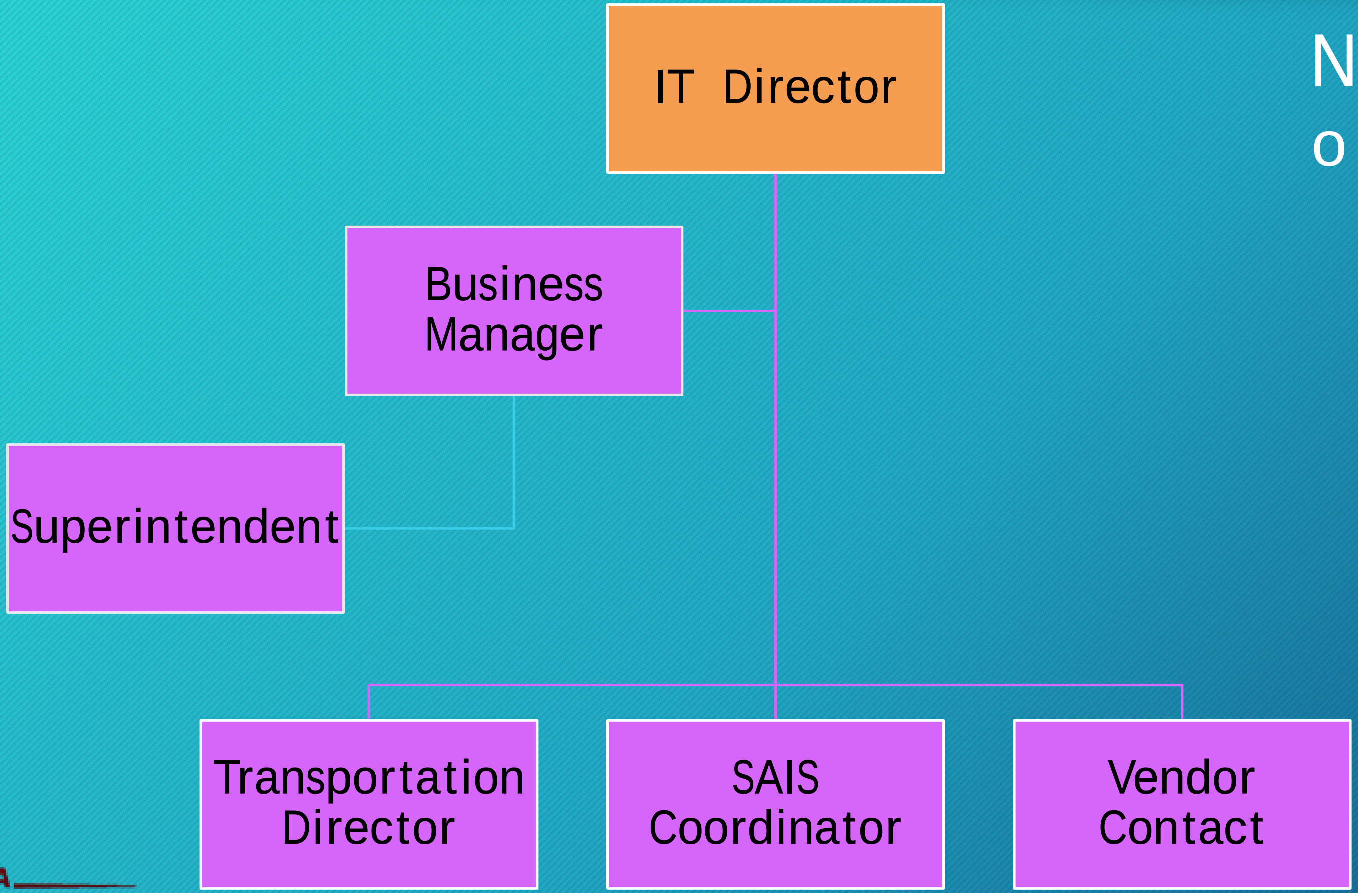
Notification Procedures

Outage Assessment

Developing a Contingency Plan – Activation and Notification

- Activation criteria should be based on:
  - Extent of damage to the system
  - Importance of the system to the district’s mission
  - Expected duration of the outage is within the RTO

Developing a Contingency Plan – Activation and Notification



IT Director

Business Manager

Superintendent

Transportation Director

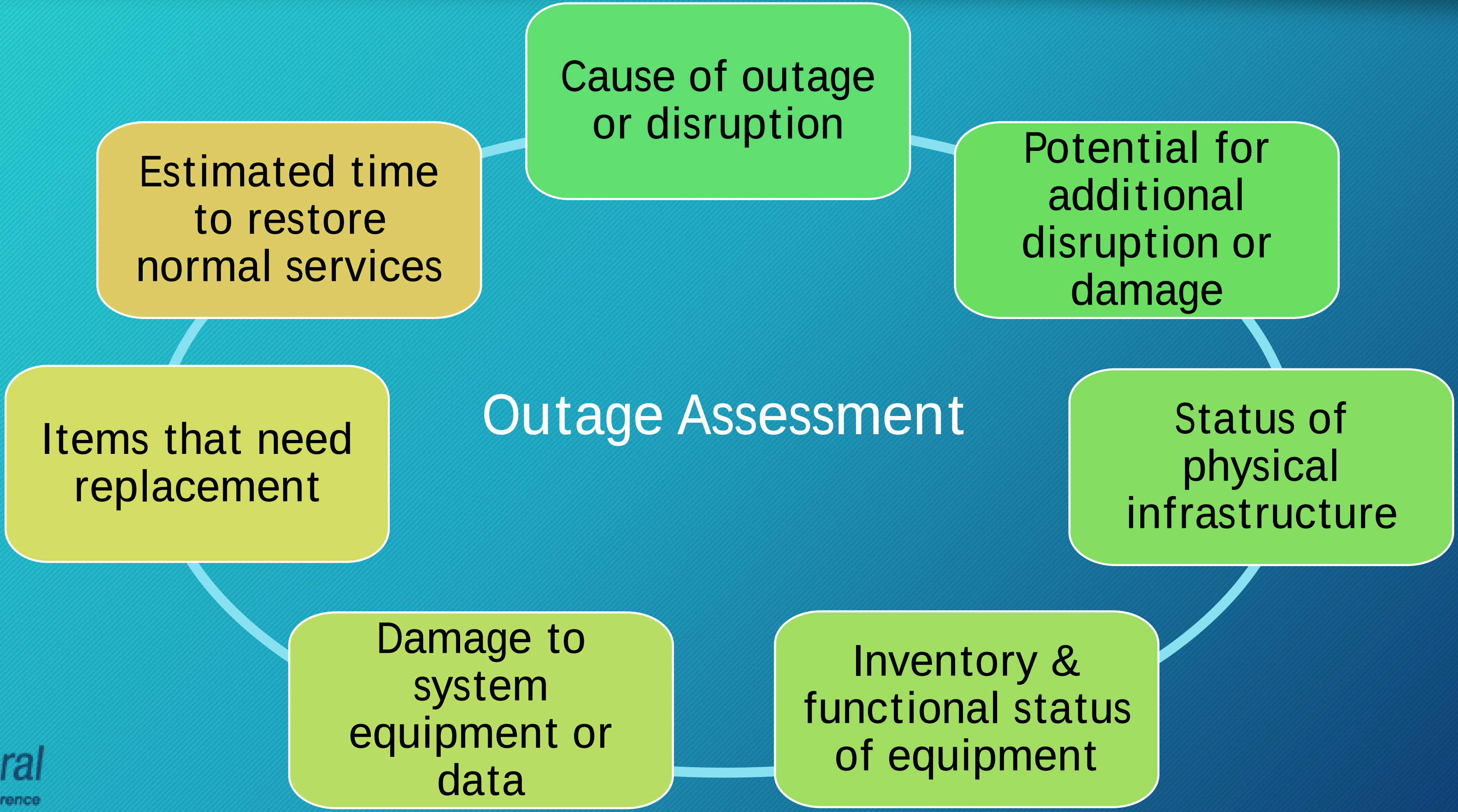
SAIS Coordinator

Vendor Contact

Notification Procedures

- Utilize a call tree
  - Include primary and alternate contact methods
  - Include contacts for vendors and third party service providers
  - Document the type of information that should be passed along during notification

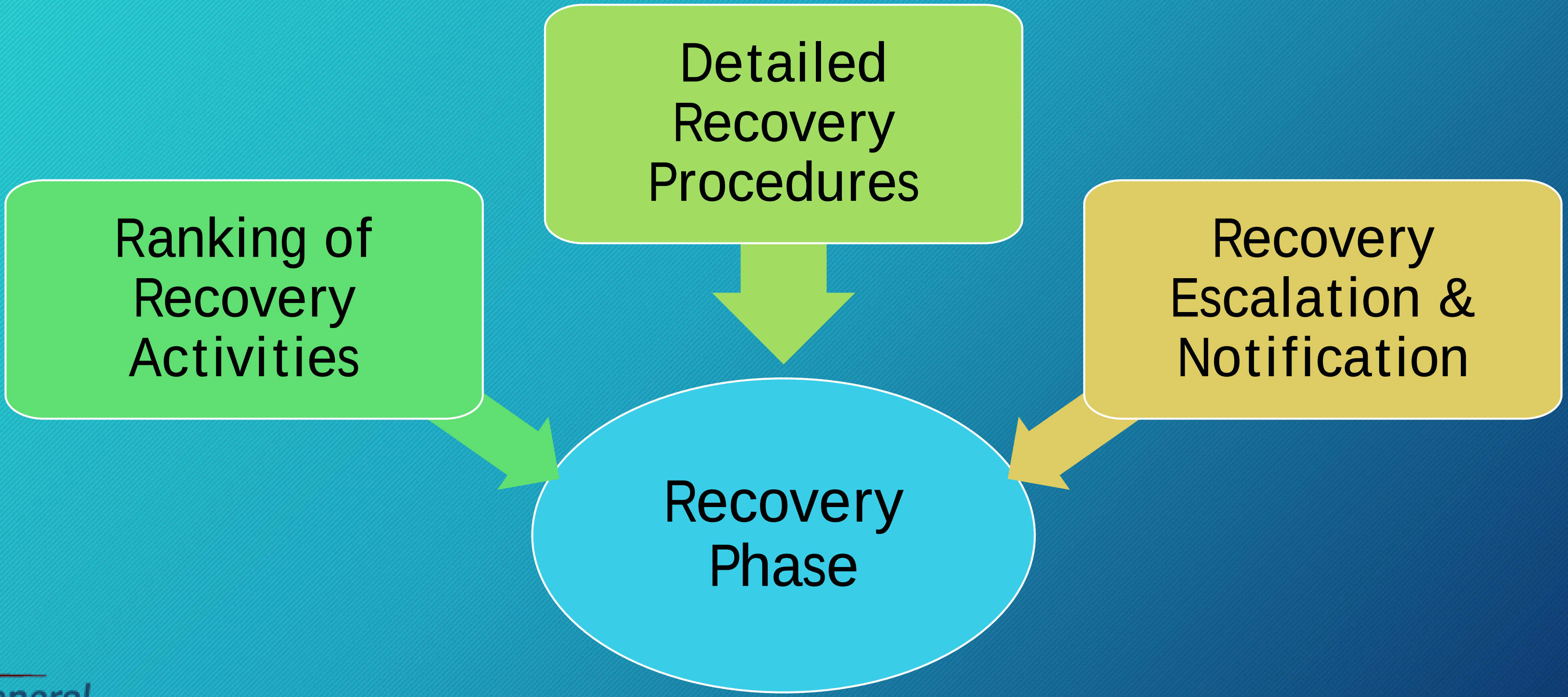
Developing a Contingency Plan – Activation and Notification



Cause of outage or disruption
Potential for additional disruption or damage
Status of physical infrastructure
Inventory & functional status of equipment
Damage to system equipment or data
Items that need replacement
Estimated time to restore normal services
Outage Assessment

ARIZONA Auditor General
Making a Positive Difference

Developing a Contingency Plan – Recovery



Detailed Recovery Procedures

Ranking of Recovery Activities

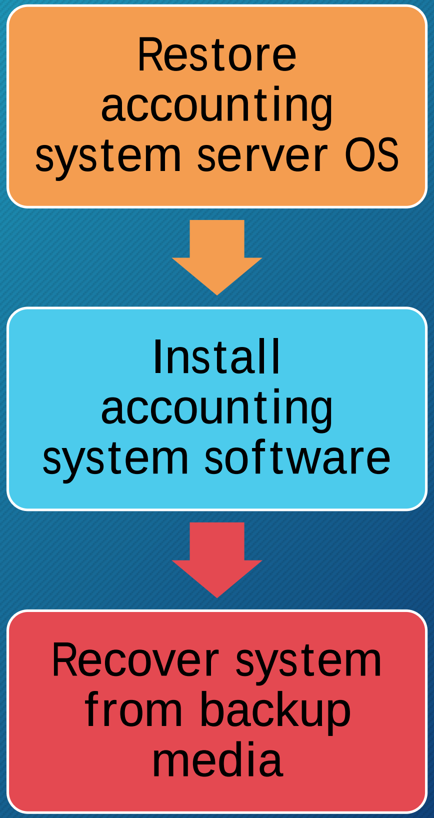
Recovery Escalation & Notification

Recovery Phase

Developing a Contingency Plan – Recovery

Sequential Order of Recovery Activities

- Align with the MTD
- Reflect priorities identified in BIA
- Include escalation steps to address:
  - Actions not completed within expected timeframe
  - Completion of key steps
  - Need to purchase item(s)
  - System-specific concerns



Restore accounting system server OS

Install accounting system software

Recover system from backup media

Developing a Contingency Plan – Recovery

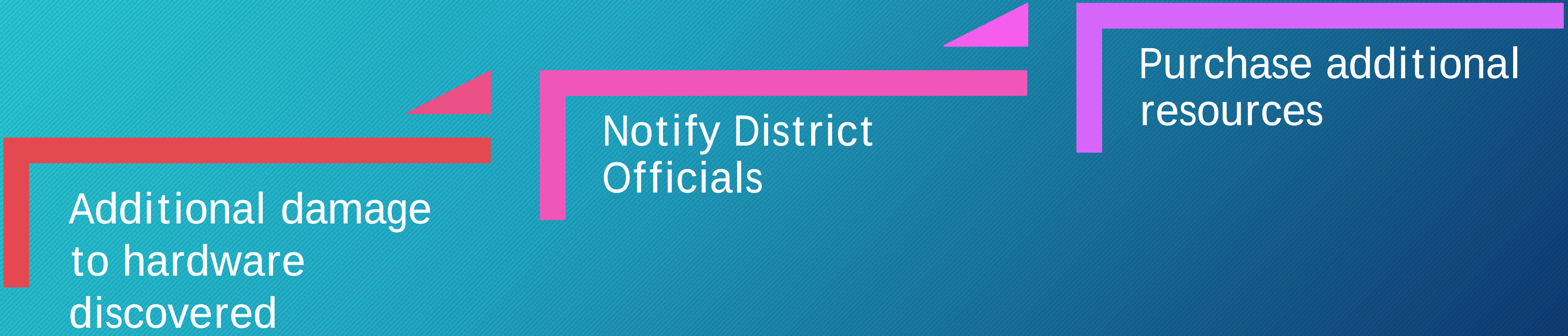
Detailed Recovery Procedures

- Obtaining authorization to access damaged facilities and/or geographic area
- Notifying internal and external system owners/users
- Obtaining necessary office supplies and work space
- Obtaining and installing necessary hardware components
- Obtaining and loading backup media
- Restoring critical operating system and application software
- Restoring system data to a known state
- Testing system functionality including security controls
- Connecting system to network or other external systems
- Operating alternate equipment successfully

Developing a Contingency Plan – Recovery

Recovery Escalation & Notification

- Describe events, thresholds, or other triggers that require additional action
- Establish clear set of events, actions, and results



Additional damage to hardware discovered

Notify District Officials

Purchase additional resources

ARIZONA Auditor General
Making a Positive Difference

Developing a Contingency Plan - Reconstitution

Actions taken to test and validate system capability and functionality

Validation

- Concurrent Processing
- Validation Data Testing
- Validation Functionality Testing

Deactivation

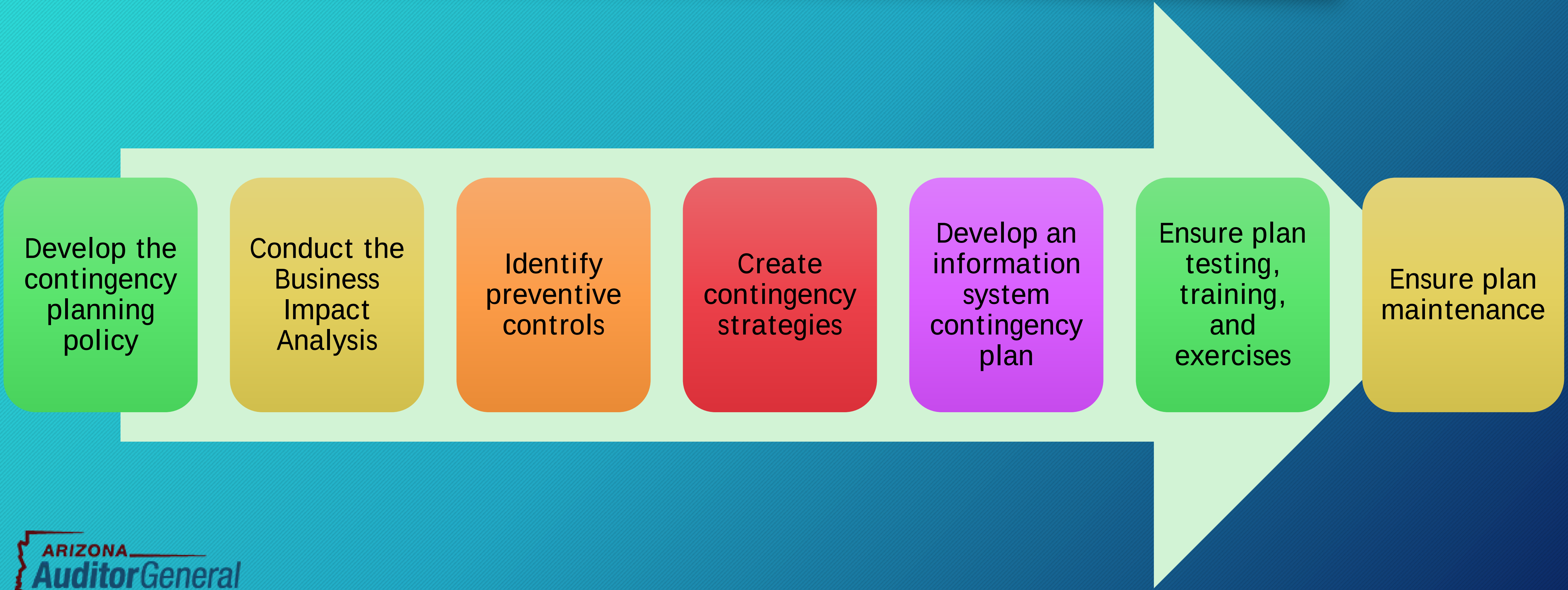
- Notifying Users
- Cleanup
- Offsite Data Storage
- Data Backup
- Documentation of events

ARIZONA Auditor General
Making a Positive Difference

Developing a Contingency Plan – Appendices

- Contact information for team personnel
- Vendor contact information
- Business impact analysis
- Detailed recovery procedures
- Detailed validation testing procedures
- Equipment and system requirements lists
- Alternate business processing procedures
- Contingency plan testing
- System interconnections
- Vendor SLAs, agreements with other organizations, and other vital records

Contingency Planning Process



1. Develop the contingency planning policy
2. Conduct the Business Impact Analysis
3. Identify preventive controls
4. Create contingency strategies
5. Develop an information system contingency plan
6. Ensure plan testing, training, and exercises
7. Ensure plan maintenance

ARIZONA Auditor General
Making a Positive Difference

Training

Who

- Only personnel required for each systems contingency plan

When

- At least annually
- Employees newly assigned to contingency role

What

- Purpose of the plan
- Reporting procedures
- Security requirements
- Individual responsibilities for activation & notification, recovery, and reconstitution

Testing the Contingency Plan

Who

- All personnel involved in the contingency plan process

When

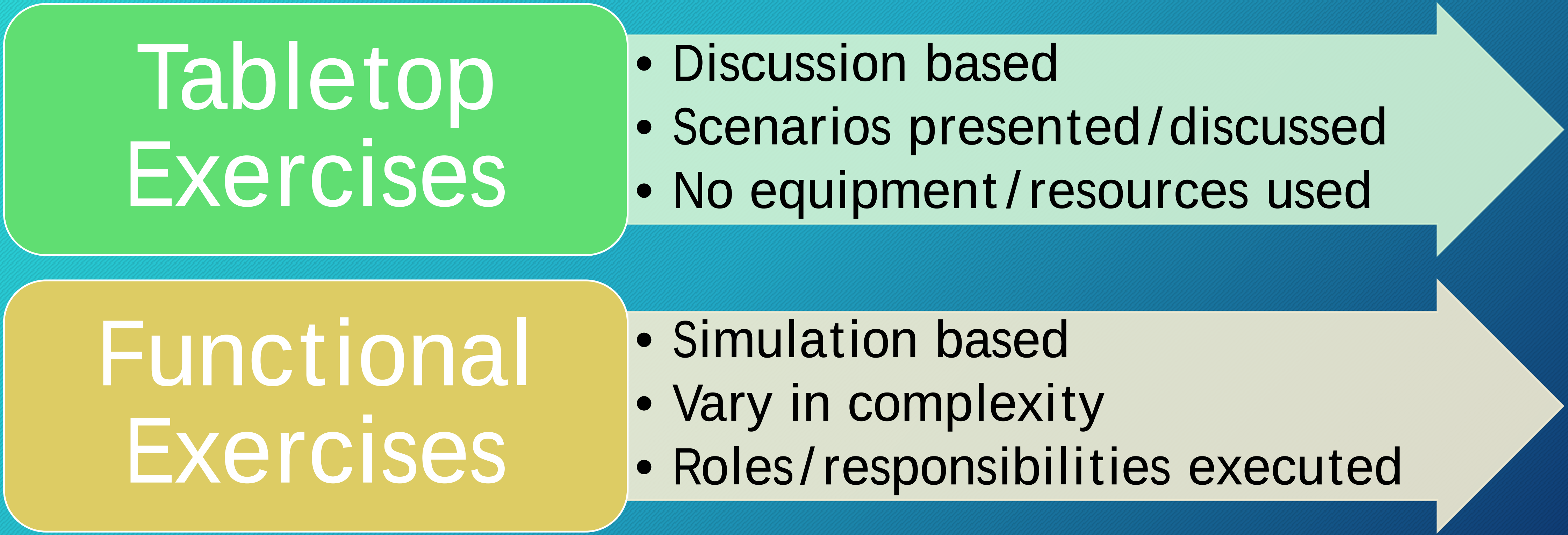
- At least annually
- Change in circumstance (system, personnel)

What

- Notification procedures
- System recovery on alternate platform from backup media
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Other areas as needed

ARIZONA
Auditor General
Making a Positive Difference

Testing the Contingency Plan



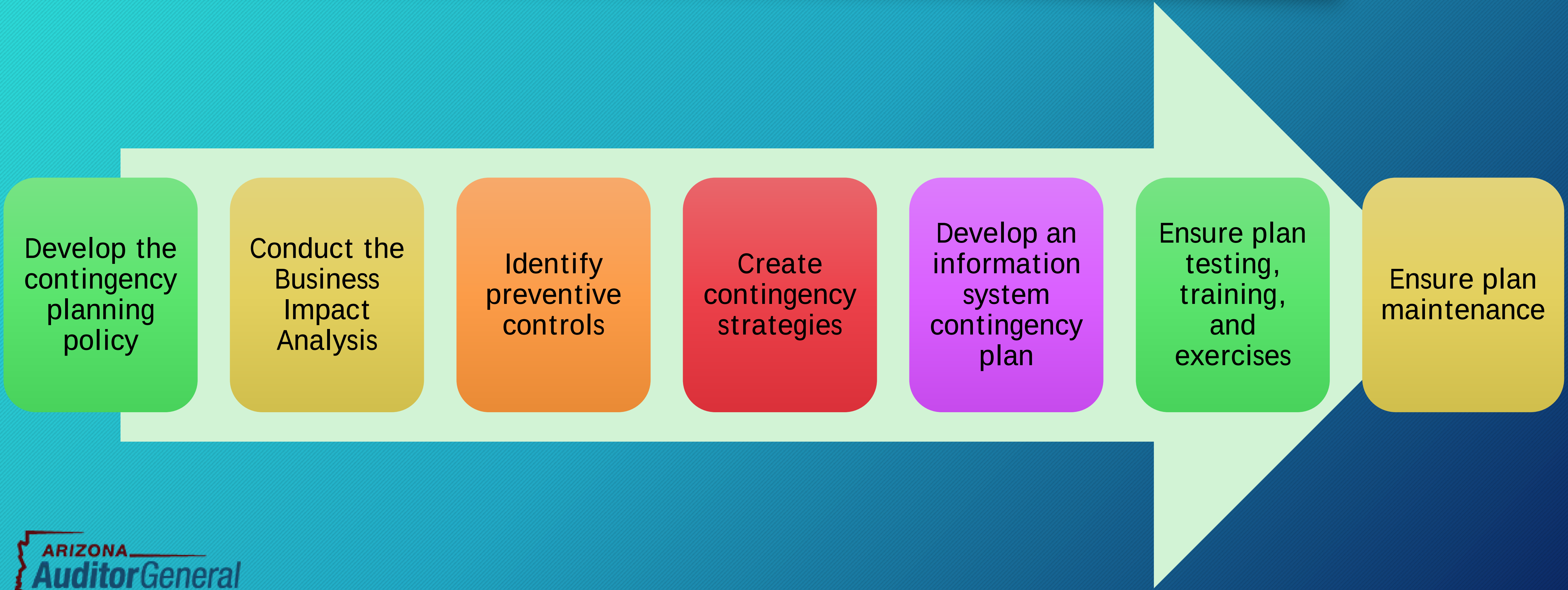
Tabletop Exercises

- Discussion based
- Scenarios presented/discussed
- No equipment/resources used

Functional Exercises

- Simulation based
- Vary in complexity
- Roles/responsibilities executed

Contingency Planning Process



1. Develop the contingency planning policy
2. Conduct the Business Impact Analysis
3. Identify preventive controls
4. Create contingency strategies
5. Develop an information system contingency plan
6. Ensure plan testing, training, and exercises
7. Ensure plan maintenance

Best practices, tools, and resources

National Institute of Standards and Technology (nist.gov)

- Special publication 800-34 (Contingency planning guide)
- Special publication 800-53 r4 (Assessing security and privacy controls
- Special publication 800-30 r1 (Guide for Conducting Risk Assessments)
- Special publication 800-39 (Managing Information Security Risk)

Arizona Office of the Auditor General (azauditor.gov)

- Reports and Publications/School Districts/Manuals/Memorandums View USFR. Information Technology (page 235)

Questions

Questions?

- Contact Us:
- By phone: 602-553-0333
- By email: asd@azauditor.gov

References

- *Closing the Security Gaps: Baseline Configuration Management* (Tech.). (2011). Retrieved April 27, 2016, from TDi Technologies website: http://www.tditechnologies.com/wp-content/uploads/2011/09/BaselineConfigurationManagementSecurityWhitePaper.pdf
- Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency planning guide for federal information systems. doi:10.6028/nist.sp.800-34r1
- Zdrojewski, M. (2013). RPO, RTO, WRT, MTD…WTH?! - Default Reasoning. Retrieved May 23, 2016, from http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/