

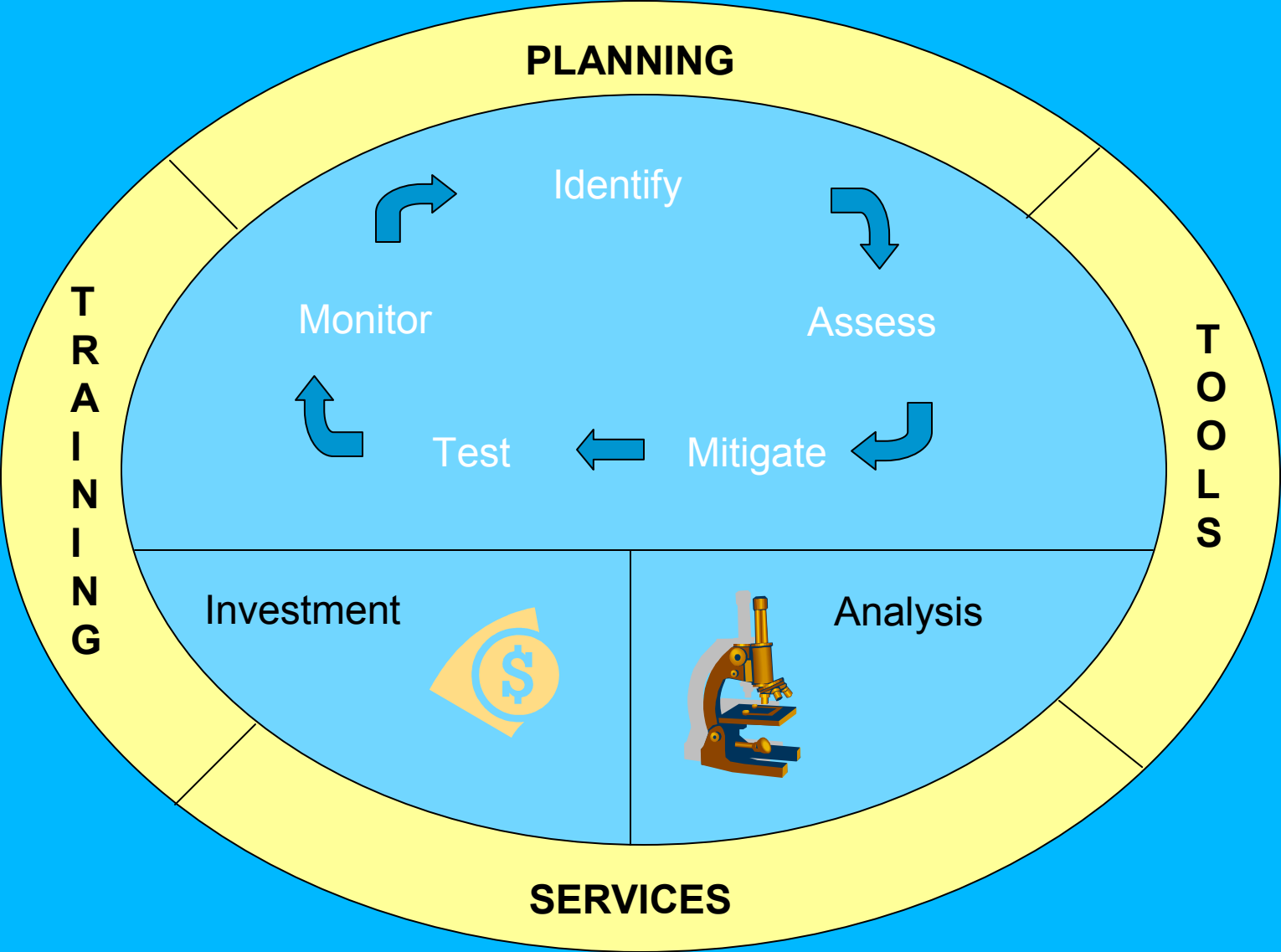
# IT CONTINUITY MANAGEMENT ROADMAP

**A PROCESS FOR IDENTIFYING  
AND REDUCING  
IT VULNERABILITIES**

Dan Hill, SRA International

Kevin Haslag, Northrop-Grumman

# IT Continuity Program Management



# IT Continuity Management

IT Continuity Management draws upon a set of established business continuity processes to help ensure that IT systems supporting essential business functions remain functioning.

- Provides for developing “tiers” of IT systems and services.
- Enables direct linkage between IT systems and the critical functions they support.
- Allows organization to focus on the most critical needs.
- Assists CIOs in their role as stewards of the IT infrastructure.
- Helps address the problem of investment vs. spending to solve continuity problems.

# IT Continuity Management

- Part of the continuity environment
  - Business Continuity Planning
  - Emergency Management/Incident Management
  - Continuity of Operations (COOP)
  - IT Security Management
  - Disaster Recovery

# IT Continuity Management

Business Continuity Planning

Emergency Management

---

IT Security Management

IT Continuity Management

Disaster Recovery

COOP

Contingency Planning

Incident Management

# IT Continuity Management

- Essential Functions of IT Continuity Management

Business Process Analysis (BPA)

Business Impact Analysis (BIA)

Evaluate Vulnerabilities

Plan Mitigation Strategies

Conduct Cost Assessments

Certify Solutions

Develop Enterprise Solutions

Evolve Solutions, Services and Strategies

# IT Continuity Management

- Taxonomy
  - Building a hierarchy
  - Tiering
  - Based on some distinguishing feature or characteristic
- Lexicon discussion
  - Taxonomy depends on the words
  - E.g. “essential” vs “critical”
  - Many sources in government and private

# IT Continuity Management

## Business Process Analysis (BPA)

- A BPA identifies the most critical business functions of the organization. It can be used to establish the recovery time and recovery point objectives of the business.
- Critical business functions are the life blood of the organization. IT Continuity Management always works best when it's business-driven.
- Recovery times and recovery points are driven by business recovery requirements – not IT capabilities. IT capabilities evolve to achieve business recovery requirements.
- Be an optimistic pessimist – hope for the best but plan for and be prepared for the worst.

# IT Continuity Management

## Business Impact Analysis (BIA)

- A BIA identifies the potential harm that threats and vulnerabilities pose to the organization and considers mitigation strategies to address them.
- Identifies high priority IT systems and infrastructures, allowing the organization to address them first as part of the overall business continuity plan.

# IT Continuity Management

## Evaluate Vulnerabilities

This process identifies those critical IT systems whose recovery capabilities are insufficient, i.e., do not meet recovery time and recovery point requirements of the business.

- Uses objective or subjective measures to prioritize systems by how urgently they need improved recovery capabilities.
- Provides a focus for applying limited resources – personnel, funding.

# IT Continuity Management

## Plan Mitigation Strategies

This process uses enterprise business requirements to drive strategy:

- Consolidation of systems and services
- Risk acceptance
- Dispersion
- Active-Passive sites (e.g. hot, cold, warm)
- Active-Active sites (e.g. load balancing)

and the use of technologies suited for improving recovery:

- Virtualization (hardware, software, application)
- Mobility
- High Availability
- Replication, mirroring, snapshots

# IT Continuity Management

## Cost Assessments

- At this stage cost/benefit studies help select the best short-term and long-term recovery strategies. Consolidation of strategies can be used to take advantage of economies of scale.
- Tactical planning (short-term) is integrated with strategic planning (long-term)
- Supports immediate and strategic goals
- Enterprise recovery solutions vs. “stove-pipe” solutions
  - Enterprise recovery solutions provide services to the organization
  - Stove-pipe solutions focus only on a particular niche.
- Makes the case for Investment over Spending
  - Investment brings more over time to the organization at less cost
  - Spending solves a problem only once and costs more over time

# IT Continuity Management

## Certify Solutions

- This process provides a high degree of confidence in the organization's ability to recover its critical IT.
- It's not about compliance. It's about demonstrating recovery readiness, and accountability.
- A certification process becomes the basis for recovery auditing
- Process is based on internal standards, legal requirements and industry best practices.

# IT Continuity Management

## Develop Enterprise Solutions

- At this stage develop a service approach to recovery.
- It's not just the data. How will you read it? How will you access it?
- It's not operational unless it's usable, and encompasses all aspects of recovery: All facets of recovery are important (systems, personnel, facilities, plans, networks and data). Without any one of them recovery fails
- Enforced through service level agreements for recovery not just for each system separately.
- Business Process Reengineering opportunities save money and improve performance.

# IT Continuity Management

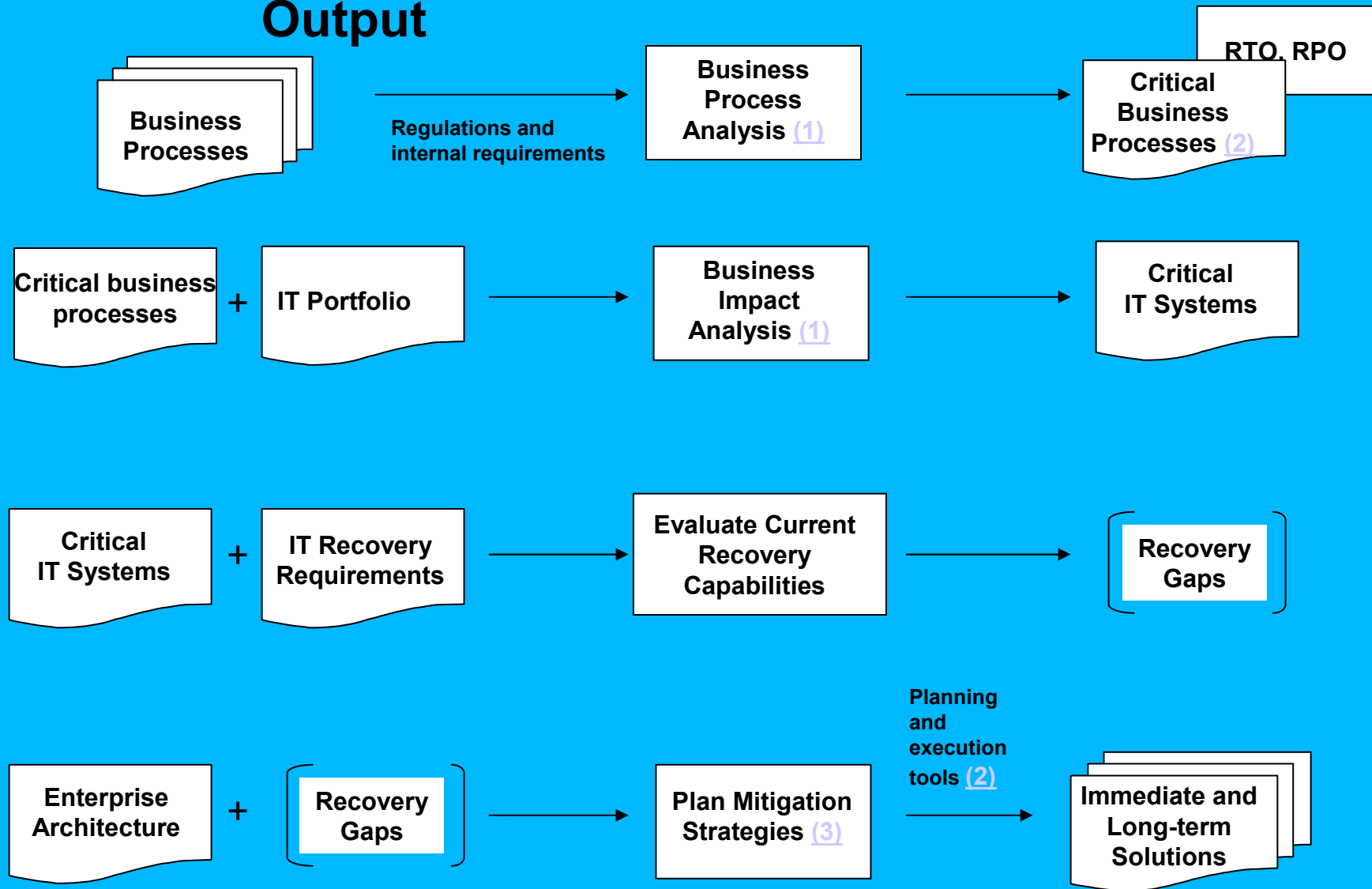
Evolve solutions, services and strategies

- Recovery is a continuous process that needs to be maintained and ingrained into the organization.
- Make this a cyclical, repeatable process of training, testing, evaluating and monitoring.
- Improve the efficiencies and effectiveness of IT continuity by using tools for:
  - Business Process Analysis
  - Business Impact Analysis
  - Modeling and Simulation (improving exercises and tests)
  - Workflow (automating plan execution)
  - Plan development and documentation tools

# Input

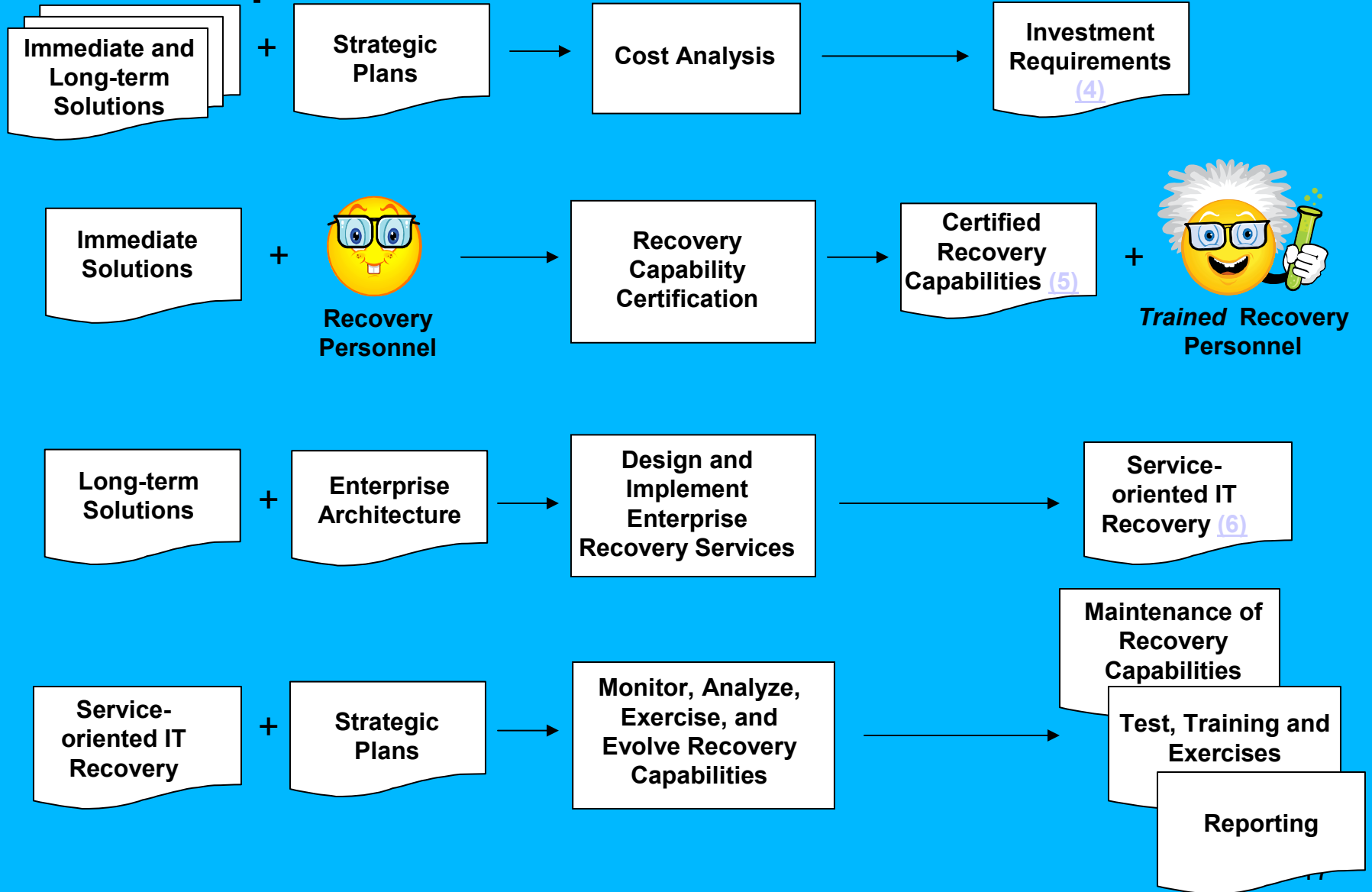
# Output

# Process



# Input Output

# Process



# IT Continuity Management

## Program level approach

- To be fully successful IT Continuity Management should be orchestrated through a program level organization that has a charter approved by a "C" level executive in the organization.
- Avoids an ad hoc approach likely to result in uncoordinated plans and funding.
- Avoids a distributed approach where different parts of the organization are responsible for different parts the process again resulting in uncoordinated plans and funding.
- Provides the program with the visibility and authority to address cross-organization IT continuity issues.

# IT Continuity Management

- Maturity Model
  - Develop a maturity model to assist program progress
  - Identifies key areas and critical success factors
  - Many sources available

# IT Continuity Management

**Teneo, ergo sum paratus!**

**(I *know*, therefore I'm prepared!)**

**Facebook Group:  
IT Continuity Management**



# QUESTIONS?

**Note:** The next 6 slides are “talking points” which are referenced as hyperlinks on slides 16 and 17.

# 1 – Business Criticality

- **Critical Business Requirements**

- Critical business processes are the life blood of the organization.
- IT Continuity Management always works best when it is business-driven.
- Recovery times and recovery points are driven by the business recovery requirements not the IT capabilities.
- IT capabilities evolve to achieve the business recovery goals.

- **Worst Case Assumption**

- Be an optimistic pessimist - plan for and be prepared for the worst but hope it never comes.

# 2 – Planning and Execution Tools

- **Improve the efficiencies and effectiveness of IT continuity by using tools for:**
  - Business Process Analysis
  - Business Impact Analysis
  - Modeling and Simulation (improving exercises and tests)
  - Workflow (automating plan execution)
  - Plan development and documentation tools

# 3 – Mitigation Strategies

- **Data center and server consolidation create enterprise recovery solutions.**
- **Technology strategies create enterprise recovery capabilities:**
  - Virtualization (hardware, software, application)
  - Mobility
  - High Availability
  - Replication, mirroring, snapshots
- **Business requirements drive mitigation strategies:**
  - Risk acceptance
  - Data backup
  - Dispersion
  - Active-Passive sites (e.g. hot, cold, warm)
  - Active-Active sites (e.g. load balancing)

# 4 – Investment Model

- **Tactical planning (short-term) is integrated with Strategic planning (long-term).**
  - Supports the strategic goals.
  - Can be leveraged to provide enterprise solutions.
- **Investment vs. spending**
  - Investment brings more over time to the organization at less cost.
  - Spending solves a problem only once and costs more over time.
- **Enterprise recovery solutions vs. “stove-pipe” solutions**
  - Enterprise recovery solutions provide services to the organization.
  - Stove-pipe solutions focus only on a particular niche.

# 5 – Certification

- **It's not about compliance.**
- **It's about demonstration and accountability.**
- **Certification of recovery capability**
- **Continuous monitoring and reporting**
- **Based on internal standards, legal requirements and industry best practices**

# 6 – Service-Oriented IT Recovery

- **It's not just protecting the data**
  - How will you read it?
  - How will you access it?
  - It's not operational unless its usable
- **Encompasses all aspects of recovery**
  - Data, systems/applications, networks, facilities, personnel, processes
  - Enforced through service level agreements
- **Business Process Reengineering opportunities**
  - Save money
  - Improve performance