IBM

IBM IT Risk Management Seminar

When Your Organisation is Not Risk-aware: Engraining risk-related policies and procedures in the corporate culture

Scott Ramsey

Director

Business Continuity & Resilience Services

Global Technology Services

IBM Asia Pacific

IBM

IBM IT Risk Management Seminar

Mitigating IT Risk in an Ever Changing World

Scott D. Ramsey, CDRP, CISM

AP BCRS SME Lead

agenda

1	Today's risks and the impact to your business
2	Risk management challenges
3	Resilient Enterprise Blueprint - IBM's approach to addressing IT risk

Areas of Risk

1. **Core Enterprise Risk –** Risks associated with the operations of the business on an enterprise-wide basis.
2. **Financial Risk –** Risks pertaining to internally controllable financial variables in relation to funding, cash base decisions and reporting
3. **Operational Risk –** Risks that result from internal business decisions on people, places, processes and equipment used to enact operational functions
4. **Information and Information Technology Risks –** Risks due to theft, fraud or system failure in relation to proprietary information, protected rights with intrinsic value, or systems controlling the flow and security of the information
5. **Regulatory Compliance Risk –** Risks due to government or industry regulation noncompliance
6. **Economic Risk –** Risks due to fluctuating external economic conditions
7. **Competitive/Strategic Risk –** Risks that result from either external competitor maneuvering or internal decisions on market positioning
8. **Litigation Risk –** Risks that derive from lawsuits related to management decisions, operations, employee actions, products and services
9. **Catastrophic Risk –** Uncontrollable or unforeseen risks and hazards caused by either internal employees or external sources

Demands on IT infrastructure are increasing

90%

Reduction
in manual process
increasing reliance on IT.

Major New York Bank

70%

Percentage of retail banking customers who have had at least one negative experience during the past year.

IBM Internal Research

50%

Percentage of customers who would give their bank only two chances to fail before considering a change in banks.

IBM Internal Research

INTERCONNECTION

- The Internet is 1 billion people strong and growing.
- Some 35% of online banking households will be using mobile banking by 2010.

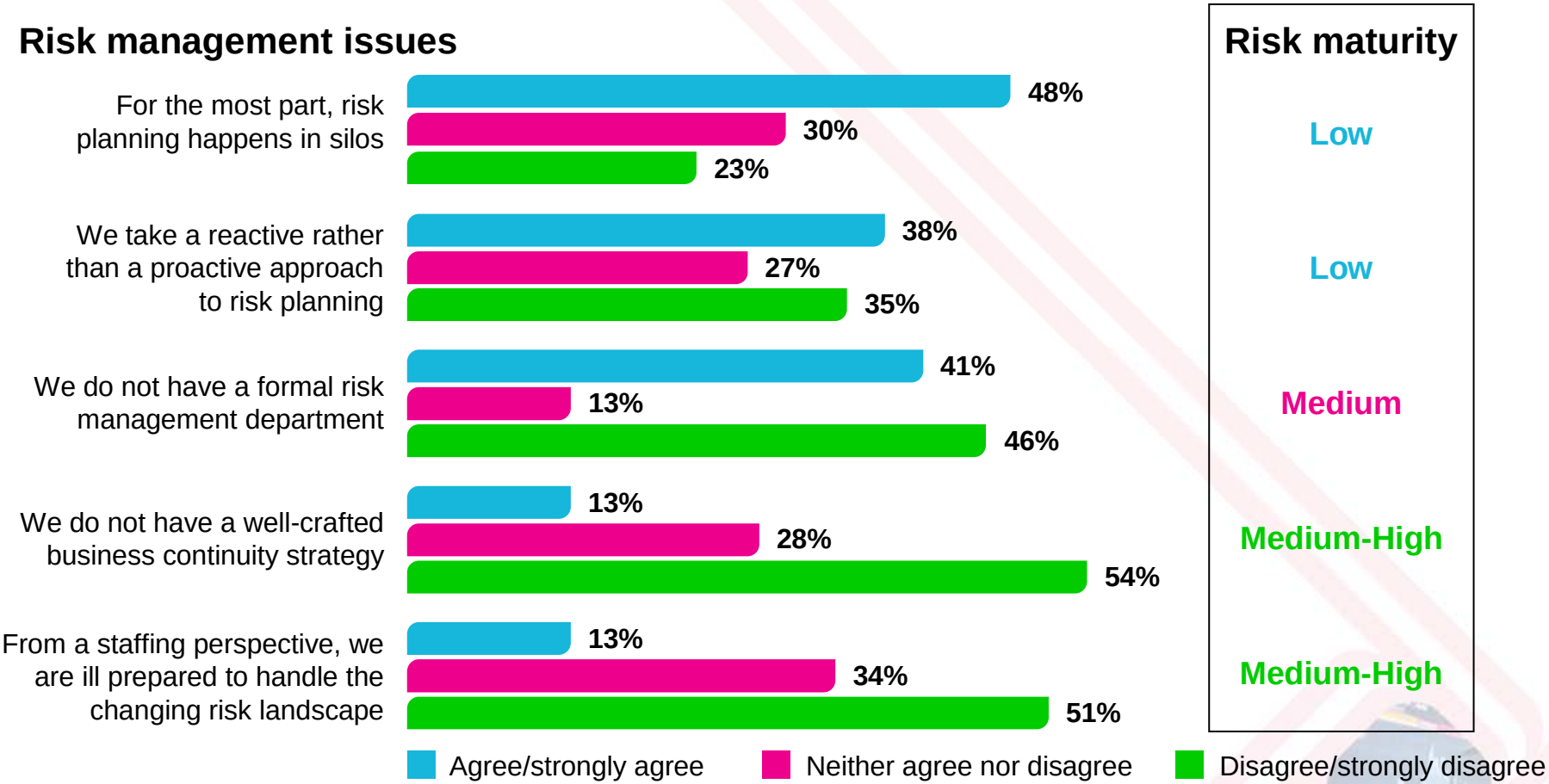
IBM Internal Research

INTELLIGENCE

- Every day, 15 petabytes of new information is being generated. This is 8x more than the information in all U.S. libraries.
- Poor data quality will cost the banking industry $27 billion in operating costs.

IBM Internal Research

Respondents identified three major areas for improvement to attain a higher level of risk maturity



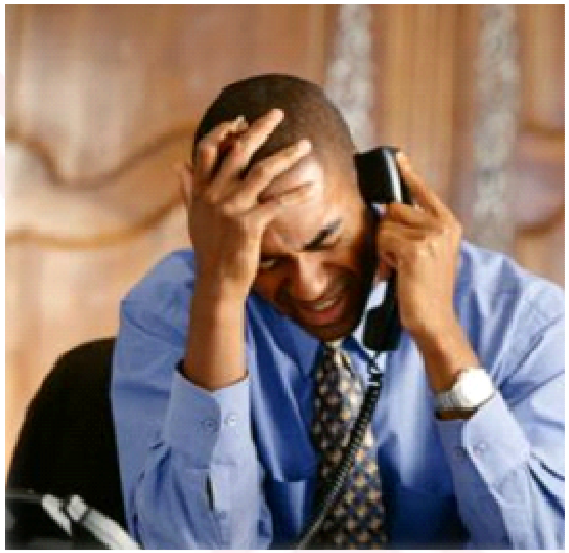
"The environment changes quickly; we react rather than anticipate."

Logistics and distribution, Western Europe

Sources: Q13b,e,f,g (Do you agree or disagree with the following statements?)
Q12 (From a staffing perspective, how prepared is the IT department to handle the changing risk landscape over the next three years?)

... and disruptions have enormous impact on the business

- Downtime ranges from **300–1,200 hours per year**, depending on industry[1]
- In some industries, downtime costs can equal **up to 16 percent of revenue**[1]
- For **32 percent** of organizations, just four hours of downtime could be severely damaging[2]
- Online **security attacks** are accelerating, causing downtime and loss of revenue
- Security is a **top area of concern and spend** for midsize businesses
- Some industries are **enforcing fines** for downtime and inability to meet regulatory compliance



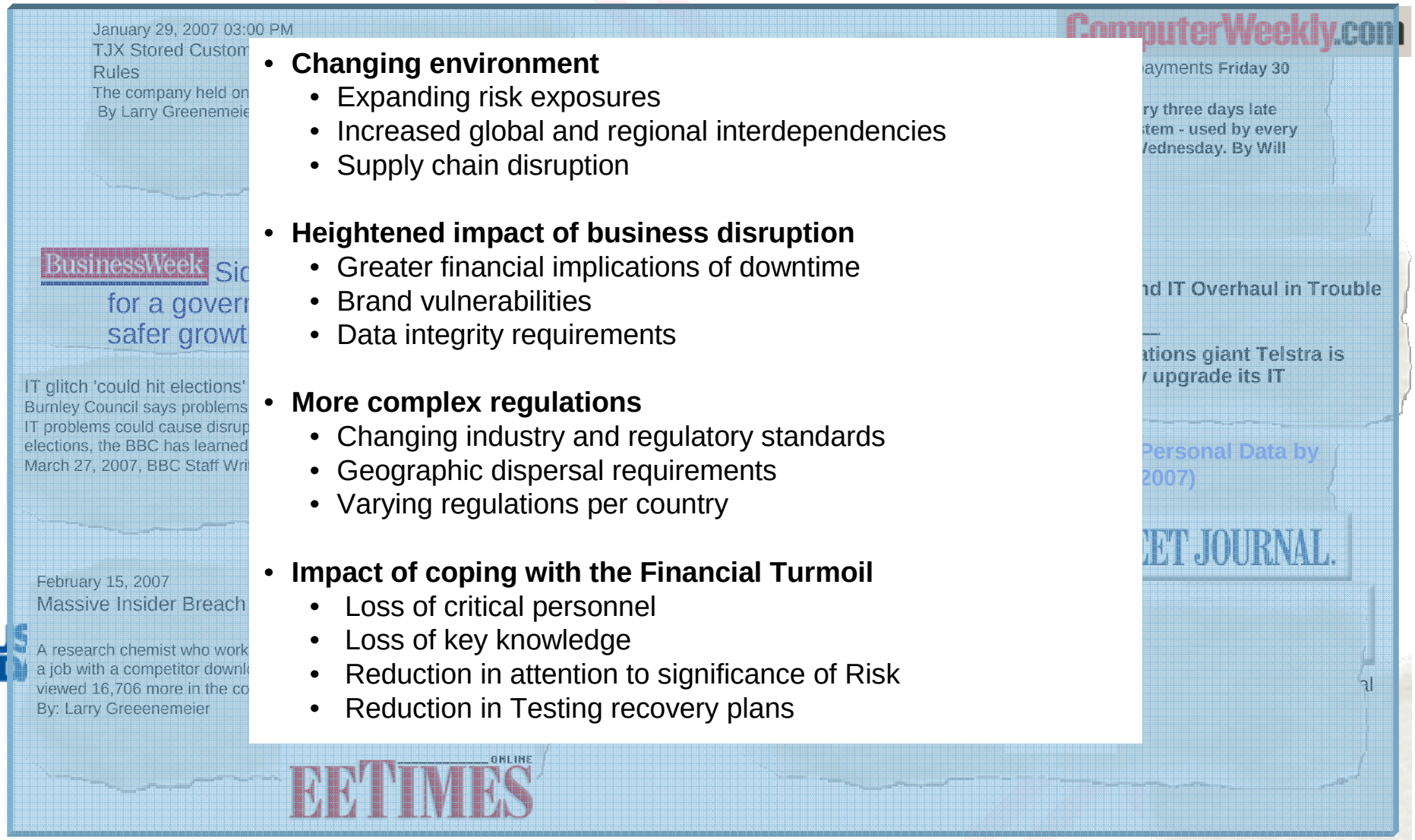
1 Infonetics Research, *The Costs of Enterprise Downtime: North American Vertical Markets 2005*, Rob Dearborn and others, January 2005.

2 Continuity Central, "Business Continuity Unwrapped," 2006, http://www.continuitycentral.com/feature0358.htm

agenda

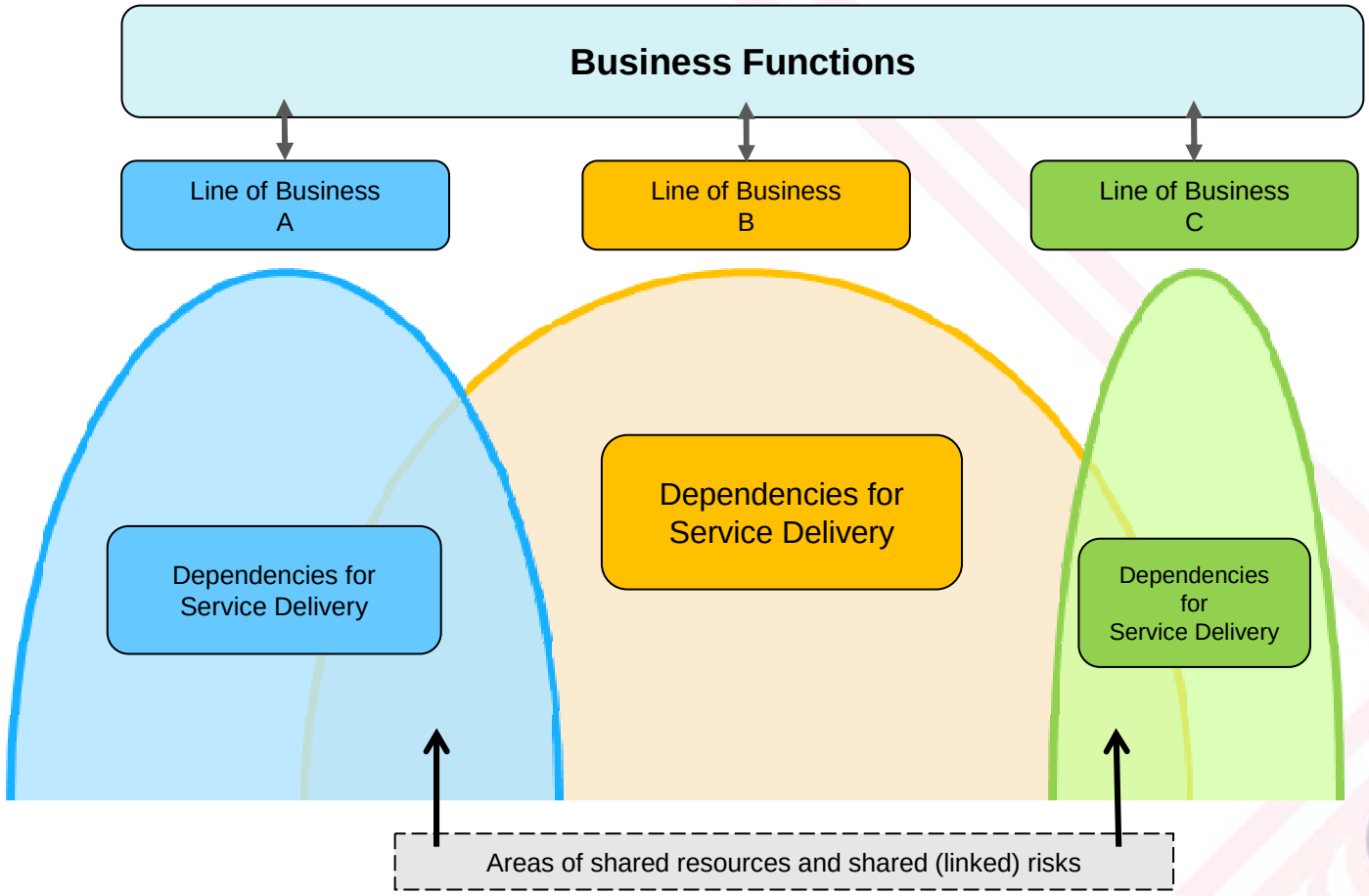
1	Today's risks and the impact to your business
2	Risk management challenges
3	Resilient Enterprise Blueprint - IBM's approach to addressing IT risk

The world is riskier than it used to be…



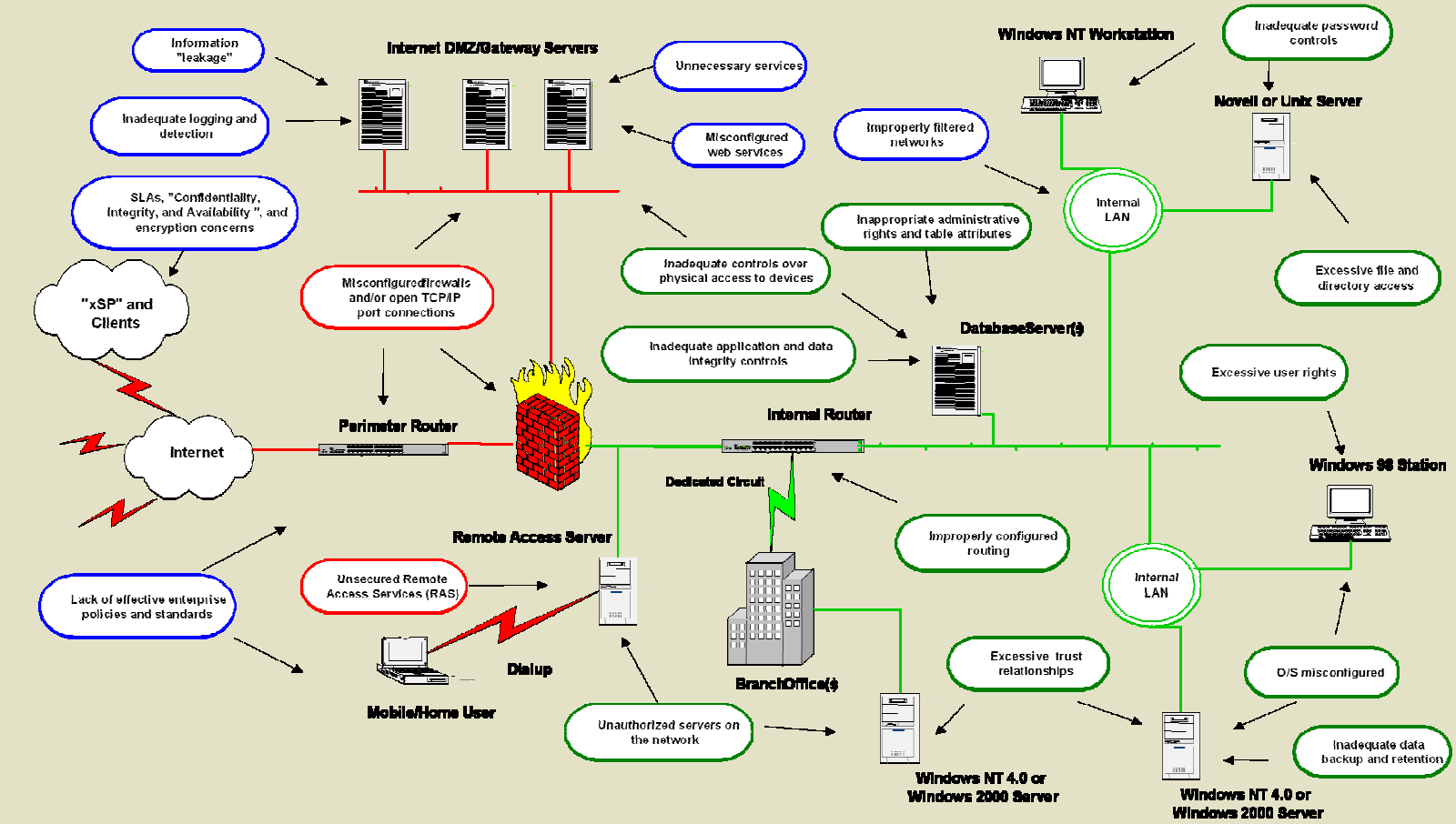
- **Changing environment**
  - Expanding risk exposures
  - Increased global and regional interdependencies
  - Supply chain disruption
- **Heightened impact of business disruption**
  - Greater financial implications of downtime
  - Brand vulnerabilities
  - Data integrity requirements
- **More complex regulations**
  - Changing industry and regulatory standards
  - Geographic dispersal requirements
  - Varying regulations per country
- **Impact of coping with the Financial Turmoil**
  - Loss of critical personnel
  - Loss of key knowledge
  - Reduction in attention to significance of Risk
  - Reduction in Testing recovery plans

The business has gotten more complicated as business functions overlap and have many interdependences

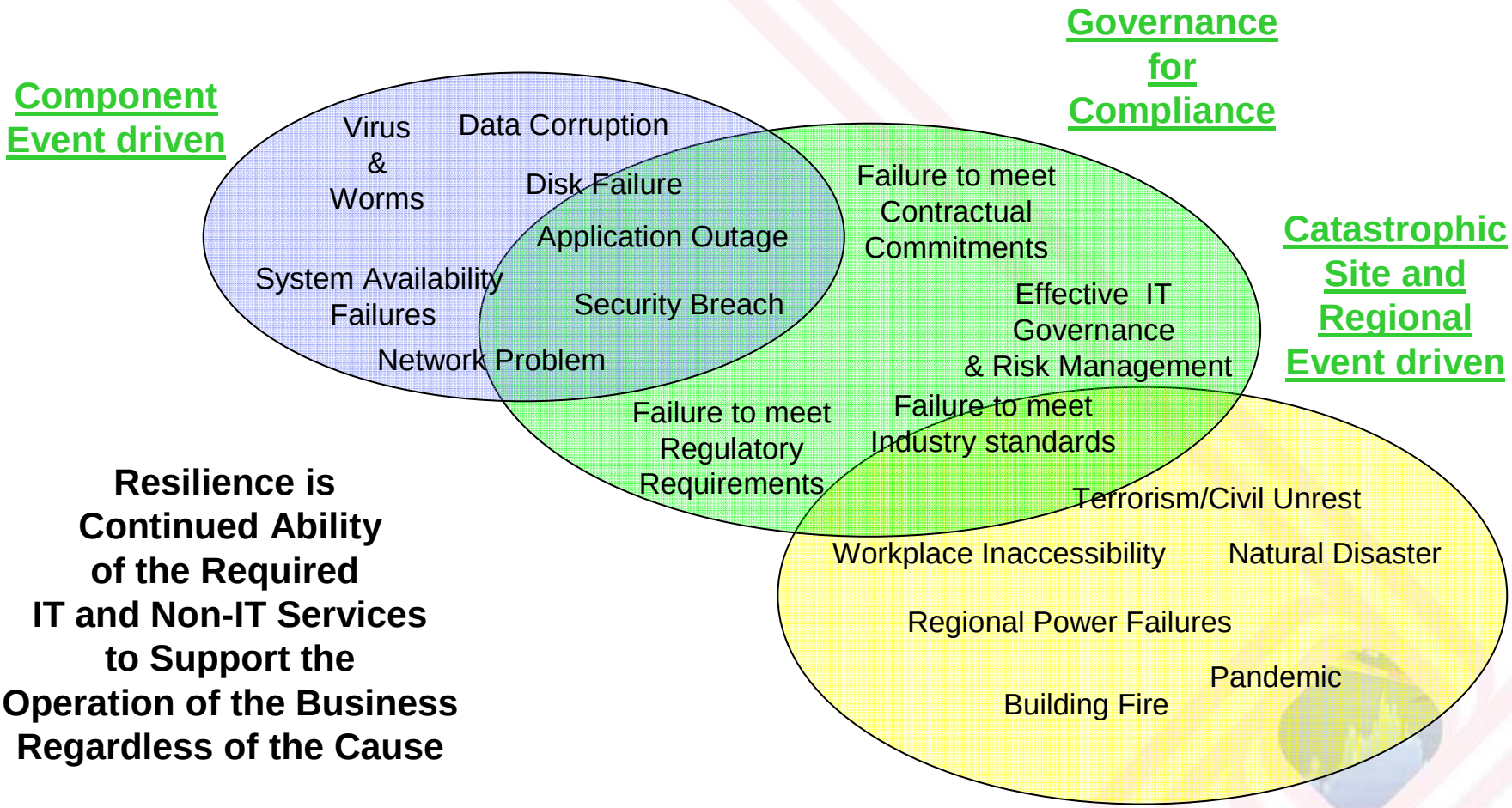


Complexity of Enterprise IT Increases Risk and Vulnerability Exposures

(Threat Colors: Red – External; Green – Internal; Blue – Both)



Today's reliance on IT related service continuance for business operation is changing the view of Business Continuity from an catastrophic event orientation to an outcome perspective Operational Risk Management perspective



Resilience is Continued Ability of the Required IT and Non-IT Services to Support the Operation of the Business Regardless of the Cause

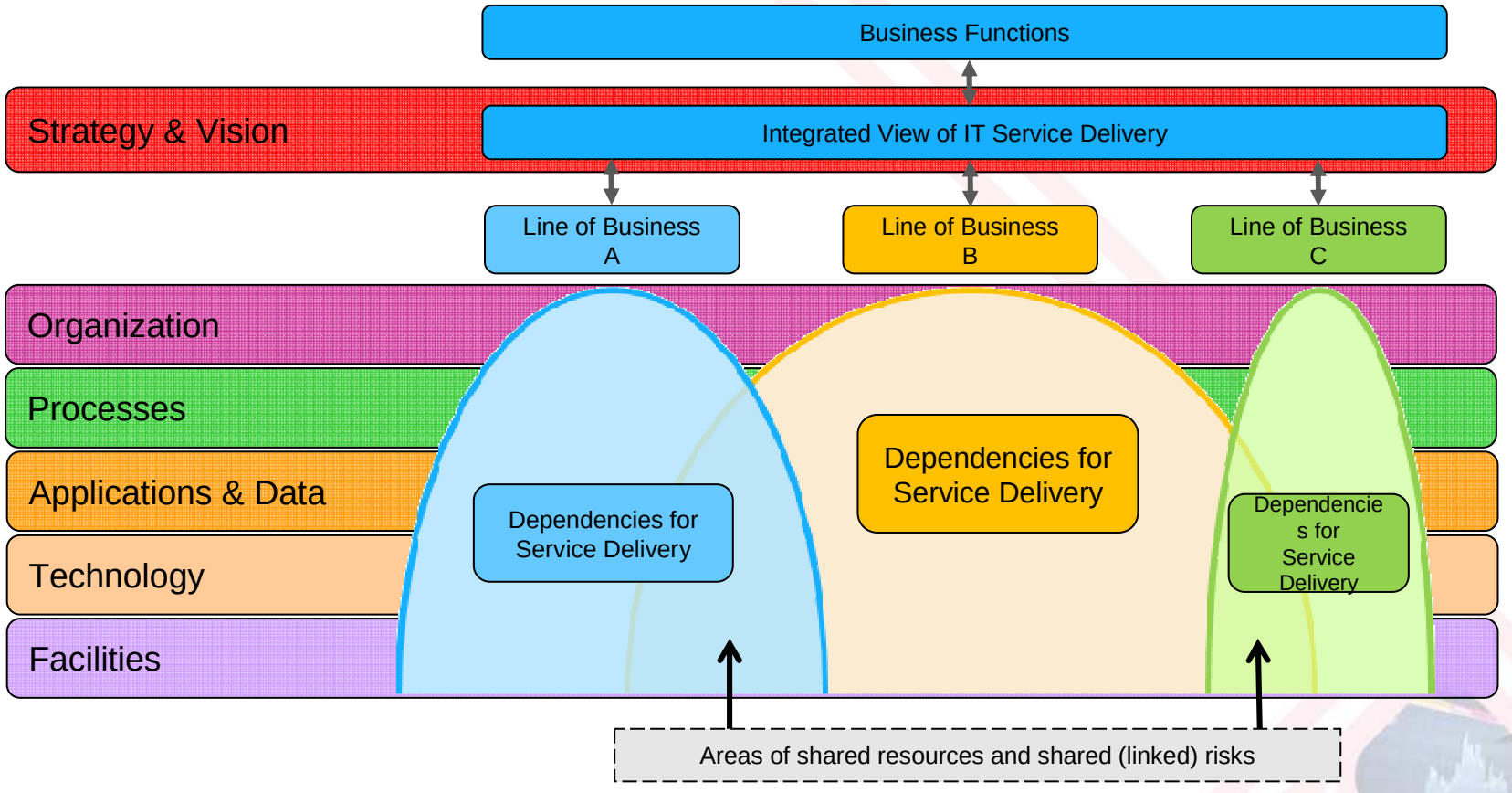
This shift indicates a need for IBM's Resilient Enterprise Blueprint strategy to enable governance and achieve resilience requirements by preventing, protecting and managing IT operational risk.

"The unfortunate truth is our ability to imagine and plan for catastrophic disasters is woefully inadequate." – Dr. Irwin E. Redlener, Director of the National Center for Disaster Preparedness at Columbia University.

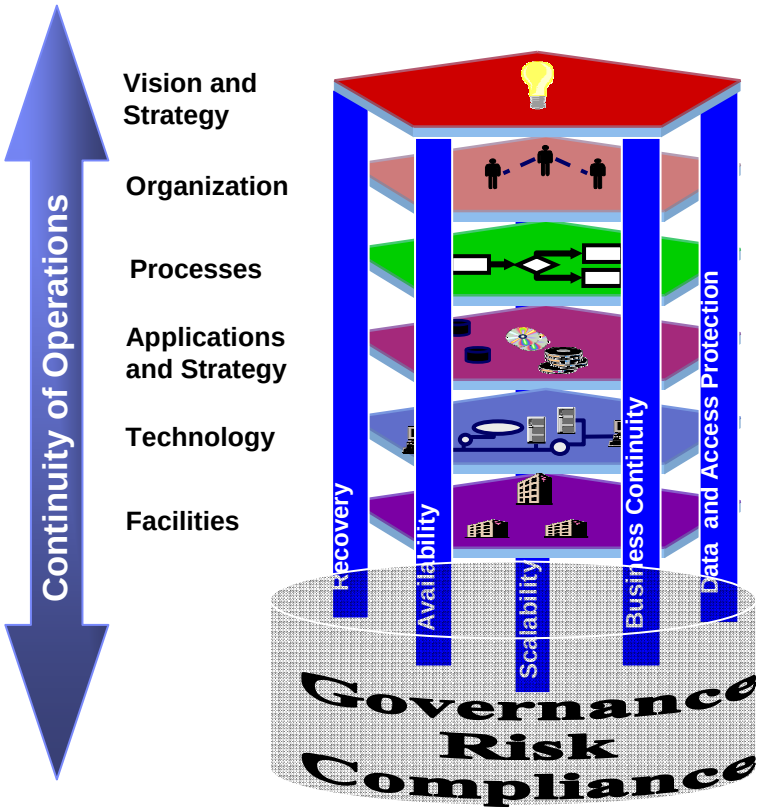
agenda

1	Today's risks and the impact to your business
2	Risk management challenges
3	Resilient Enterprise Blueprint - IBM's approach to addressing IT risk

The Resilient Enterprise Blueprint links the IT Service Delivery Resilience requirements across the enterprise



The IBM Resilient Enterprise Blueprint (REB) takes a holistic view of how risks are mitigated through all the layers of your enterprise



Assets	Identify assets to be secured and controlled from inadvertent and/or intentional misuse.
Governance	Establish policies, procedures, and standards to define behavior.
Profile	Locate and identify all assets across the infrastructure.
Value	Determine business worth of resources.
Vulnerabilities	Identify potential vulnerabilities and the ability to exploit them.
Threats	Identify potential threats and the likelihood of occurrence.
Risk	Calculate level of risk based upon exposures and countermeasures.
Solutions	Eliminate or reduce of likelihood of vulnerabilities.
Metrics	Establish measurements to determine impact and value of security initiatives.
Monitoring	Measure compliance against established policies, procedures, and standards.

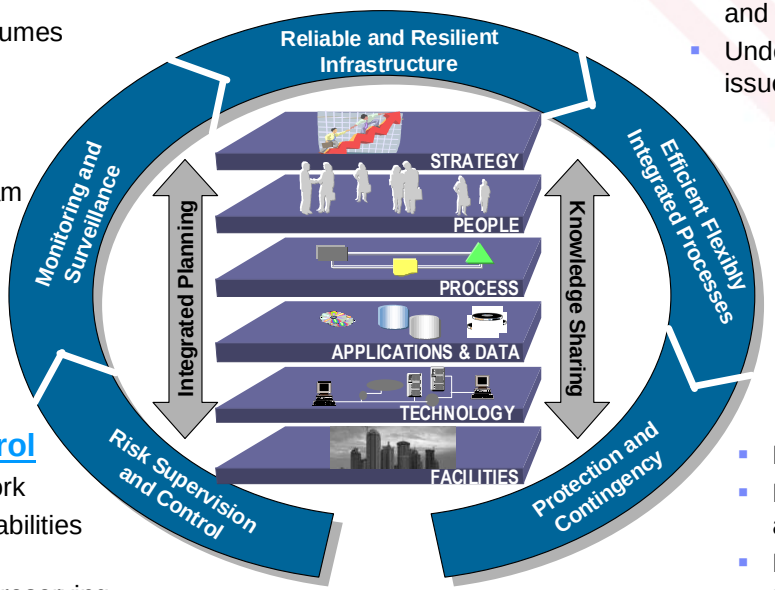
Achieving an optimized IT Operational Risk management environment requires each component must work together across the company

Reliable, Secure and Resilient Infrastructure

- An infrastructure that is resistant to disruption
- Monitoring and self-healing
- Scalability for the unexpected
- Adequate Protection from Threats

Monitoring and Surveillance

- An efficient process control framework
- Extracting meaningful signals from volumes of data
- Monitoring protocols that will alert to perceived threats
- Leading analytical tools into mainstream processing



Efficient & Flexible Integrated Processes

- More reliable and controllable processes
- Transformation opportunities to reduce complexity and standardize
- Understanding organizational communication issues and constraints

Risk Supervision and Control

- An effective risk management framework
- Benchmarking existing or planned capabilities against best practices
- Meeting regulatory requirements and preserving capital

Protection and Contingency

- Policy and recoverability for each process
- Risk and recovery scenarios across business and IT
- Partners process risks and methods for mitigation
- Joint business/IT planning and testing

The Resilient Enterprise Blueprint provides an operating model that balances risks and cost

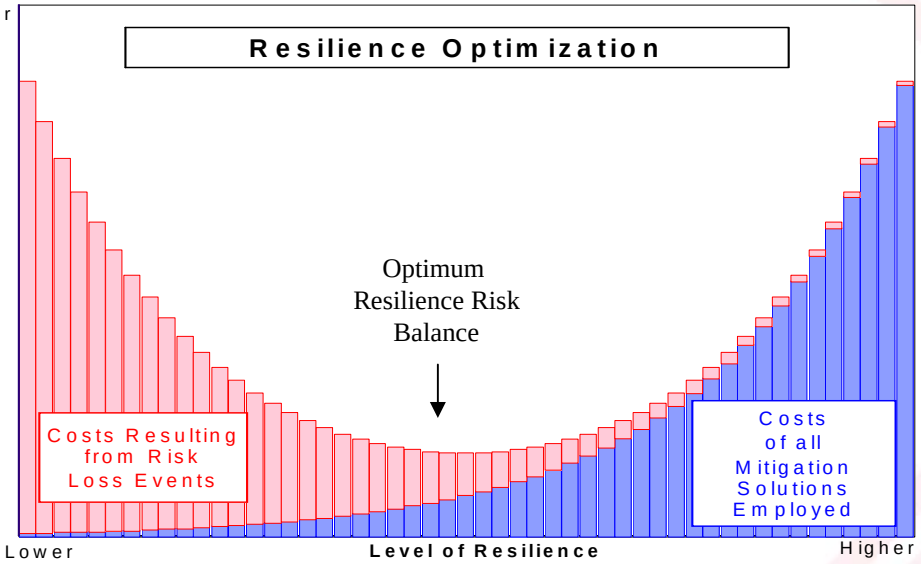
Smart is

"The Right Resilience at the Right Price"

- Understanding the costs associated with the mitigation solutions employed to deal with the selected level of risk
- Understanding the potential loss associated with the level of risk being assumed
- Selecting the mitigation solutions consistent with the level of potential loss
- Selecting the optimum architecture for the mitigation solutions
- Optimized resilience can help reduce costs to the business

Potential Risk Cost Elements

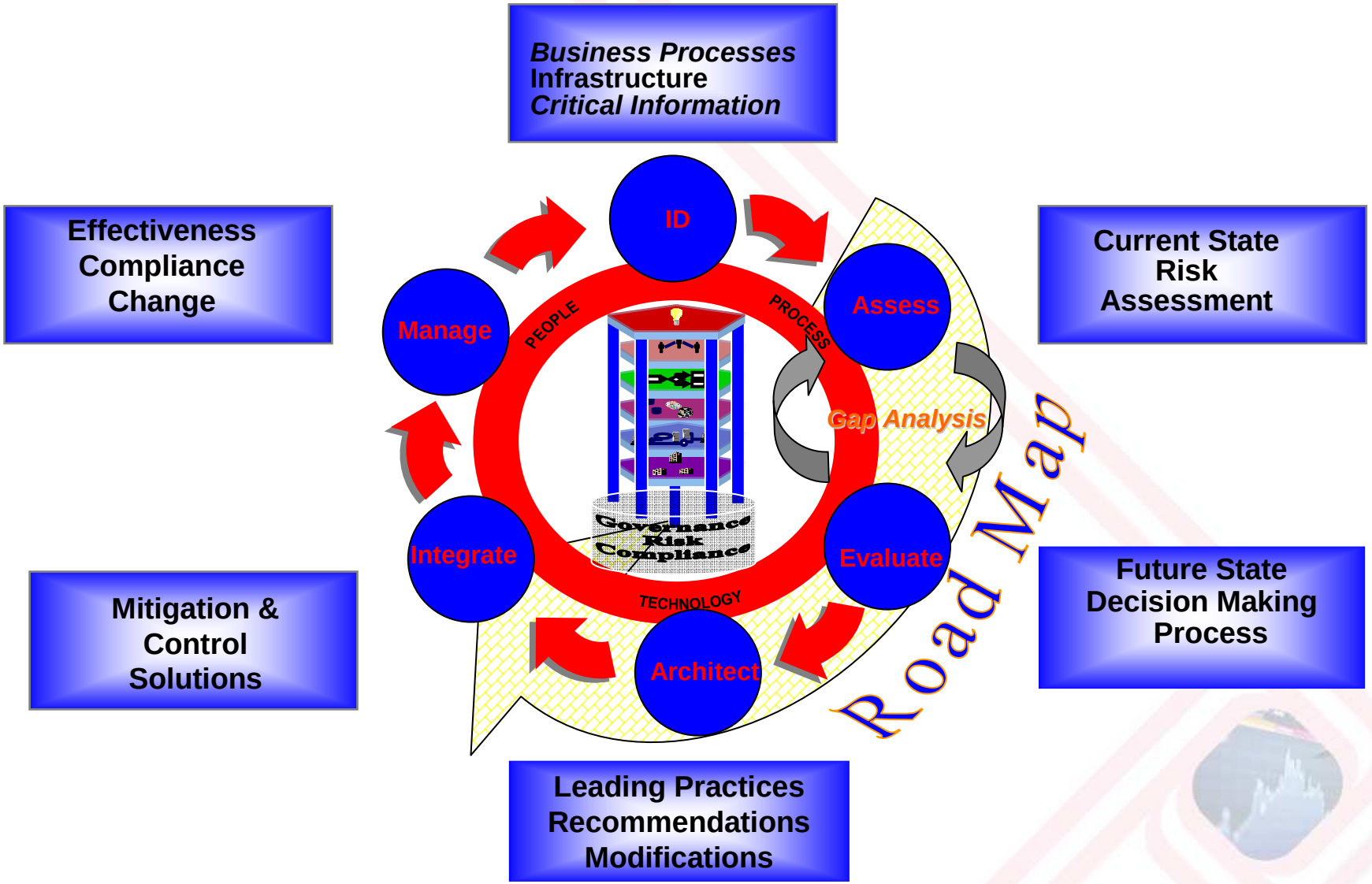
- Loss Avoidance
- High Risk Capital Allocation Position
- Maintain Credit Rating
- Fine and Penalty Avoidance
- Maintenance of Customer Confidence
- Maintain Social Responsibility
- Cost Avoidance



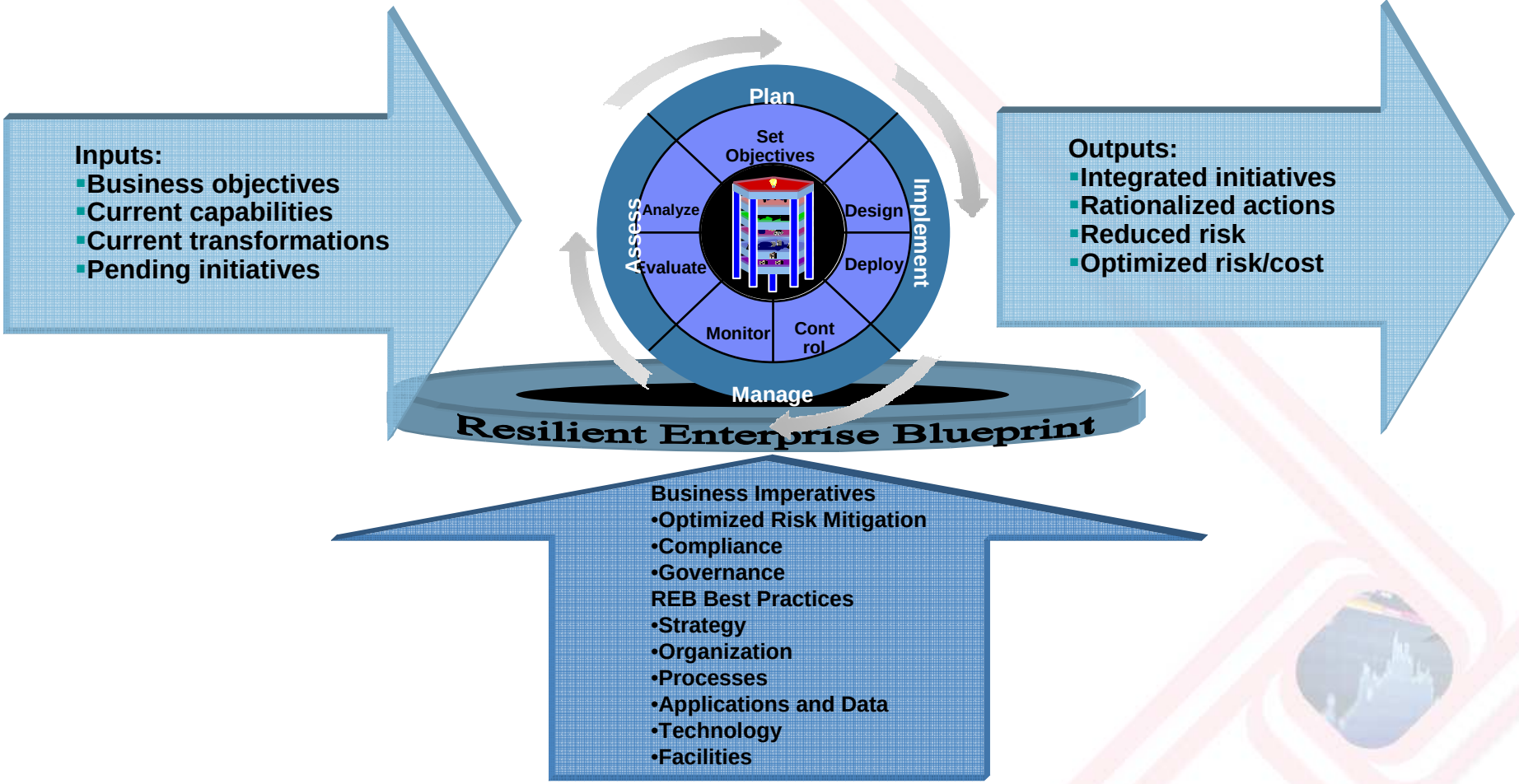
Types of Mitigation Solutions

- IT Resilience Architecture
- IT Service Delivery Topology
- People and Processes
- Work Place Strategy
- Data and Information Protection
- Regulatory Compliance

IT Operational Risk Management Life Cycle



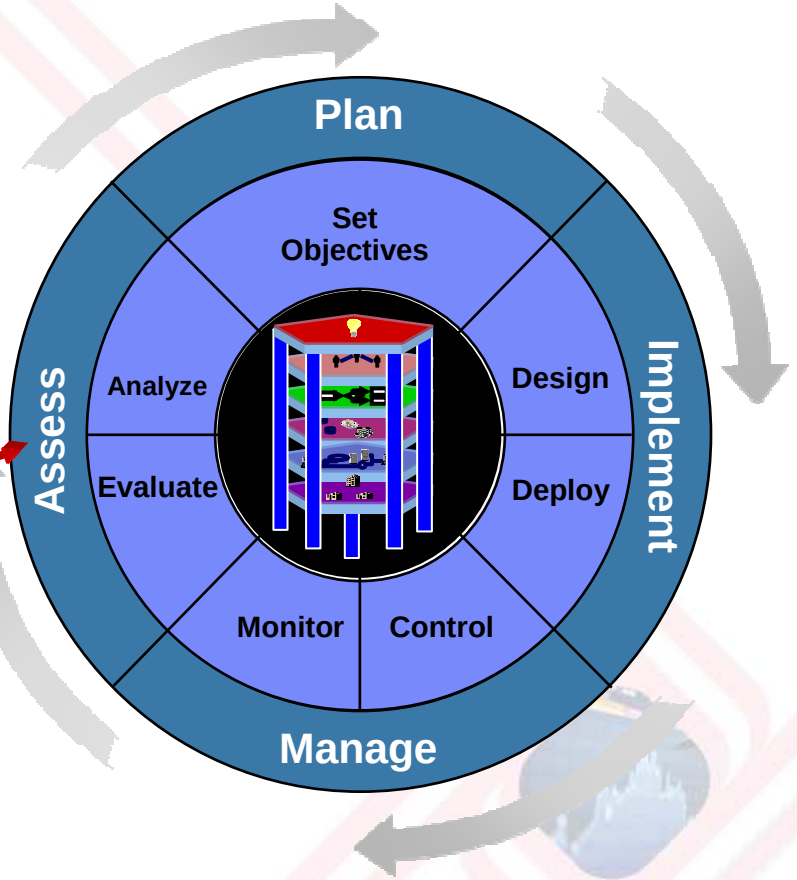
REB provides a continuous improvement governance system that focuses on achieving the Business Objectives by integrating current abilities, initiatives and transformations with best practices to optimize Resilience



To begin, complete a thorough analysis of potential risks and the current ability of the company to mitigate them

Assess

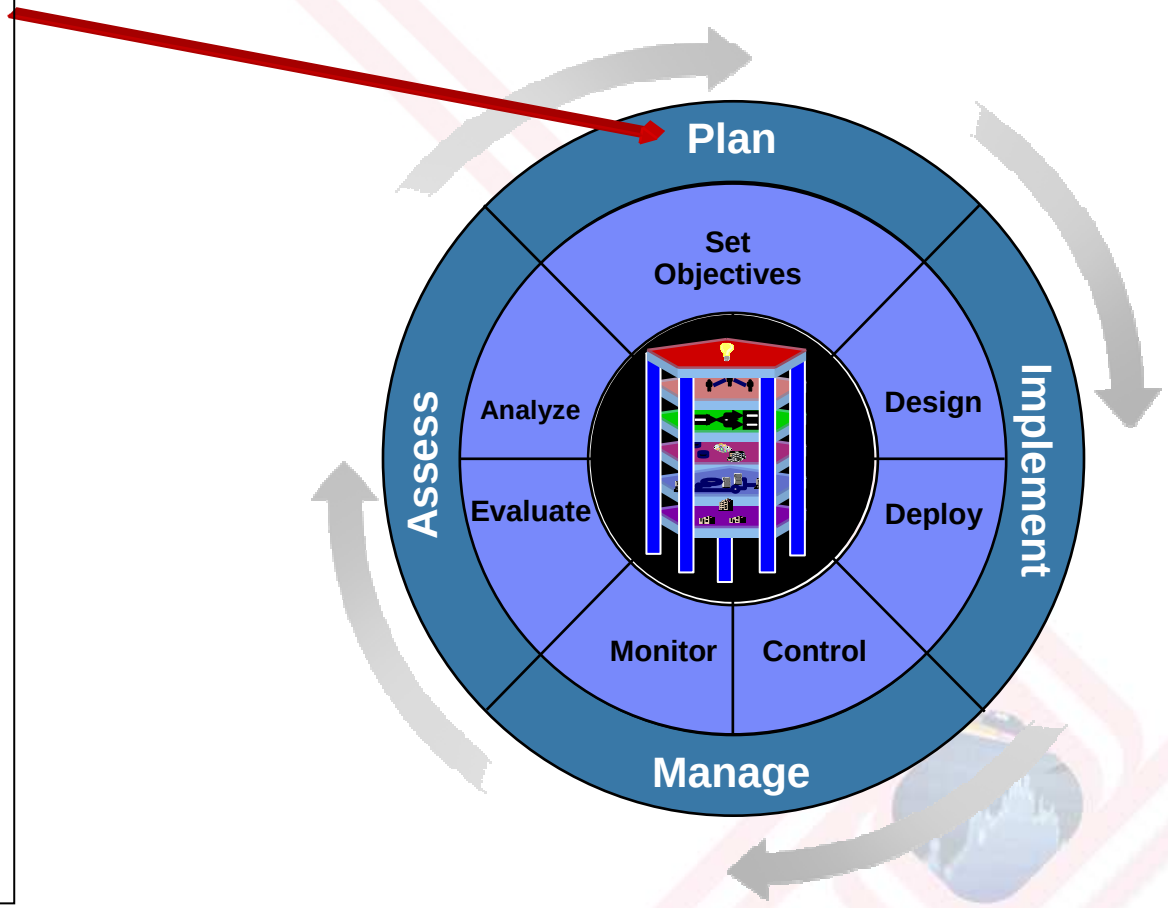
- Analyze current & potential risks
  - Establish a risk profile
    - By business location
    - By line of business function
    - By business process
  - Determine impact of event
    - Financial
    - Opportunity
    - Reputation
- Analyze capabilities for mitigation
  - Define customized risk framework
    - IBM Business Resilience Framework
  - Identify risk areas for further analysis
  - Assess maturity of mitigation capabilities
    - Basic
    - Managed
    - Predictive
    - Adaptive
    - Resilient



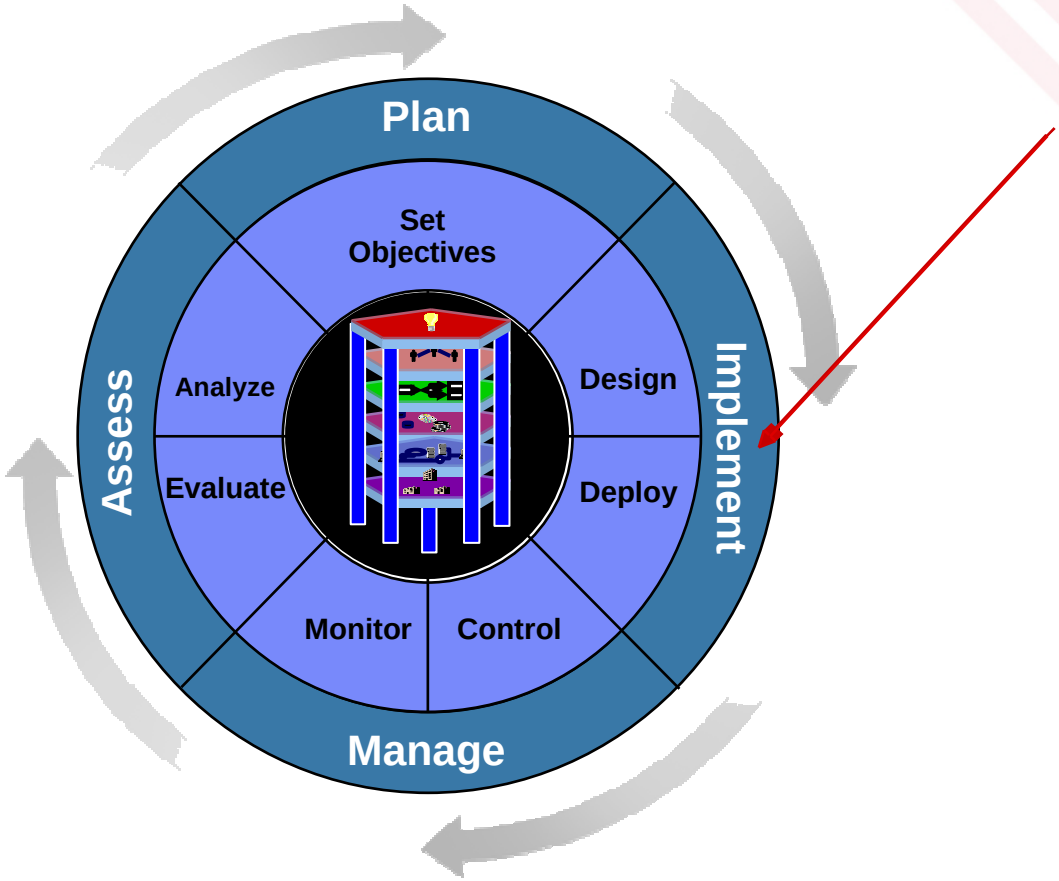
Next, set the objectives for the reach and range of what risks you may need to mitigate.

Plan

- Setting objectives for risk mitigation or enhancement
  - Define the scope for the risk strategy
    - Extended enterprise
    - Enterprise-wide
    - Line of business
    - Business process
    - Business system
  - Select risks to be mitigated or enhanced
    - Procedural
    - Technical
    - Organizational
    - Economical
    - Financial
    - Extra-structural
    - Infra-structural
    - Geological
    - Environmental
    - Societal
    - Governmental



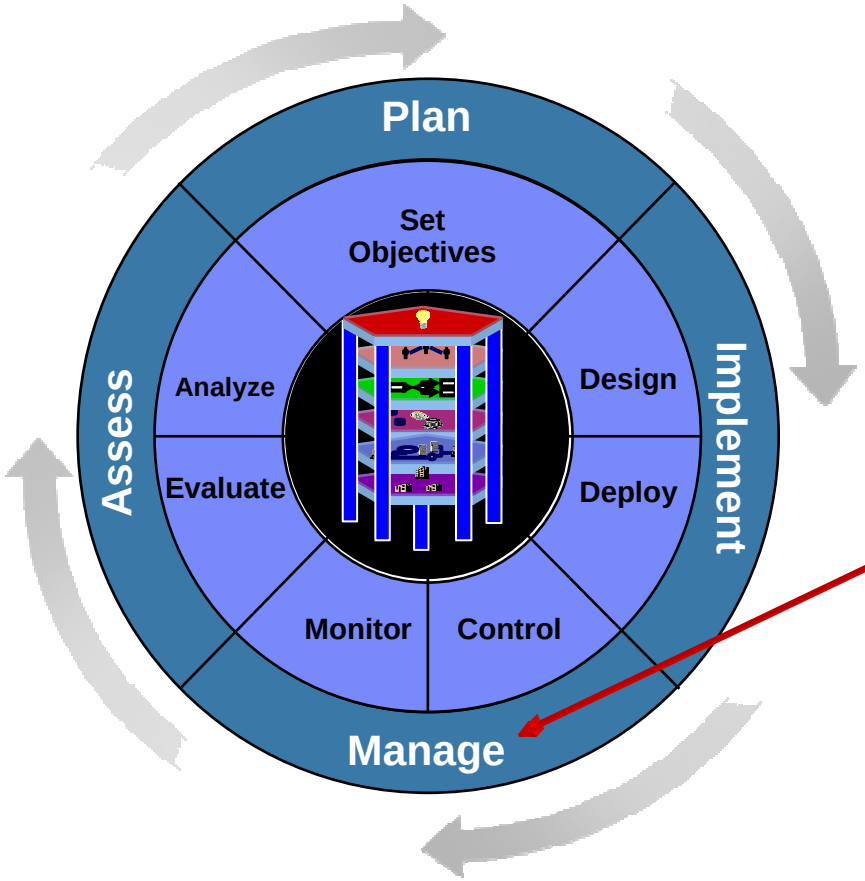
Implement a strategy & architecture that protects critical information and ensures Operational Resilience.



Implement

- Design for Operational Resilience
  - Conceptual design
    - Business and Financial Justification -Concurrence among business executives and explanation to internal and external audit groups
    - Governance / Authority / Policies -Communication, mission, discipline
    - Systems Management Disciplines - Problem, change, configuration, etc.
    - Security- Physical and logical
    - Application & Data - Data protection, backup, restart, synchronization
    - Program Execution - Reporting, roles and responsibilities, public relations, business integration, plan invocation
    - Facilities – Location & management
  - Solution design
    - Goals and guiding principles
    - Functional, logical & technical components
    - Benefits, solution costs & implementation plan
- Deployment of Operational Resilience
  - Protection of critical information
  - Recoverability of business functions

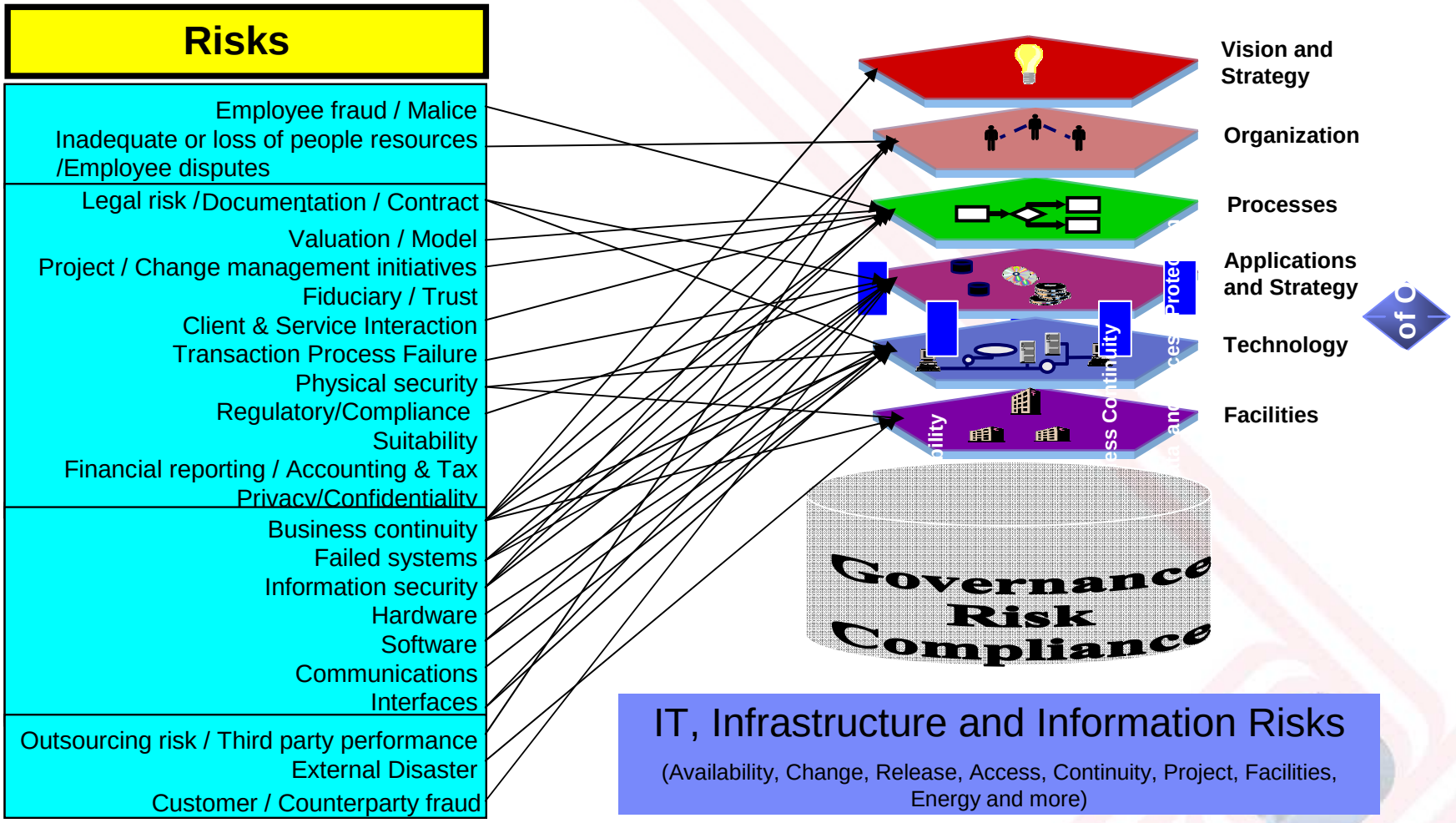
Ongoing management is required to ensure continued operational resilience through control and monitoring



Manage

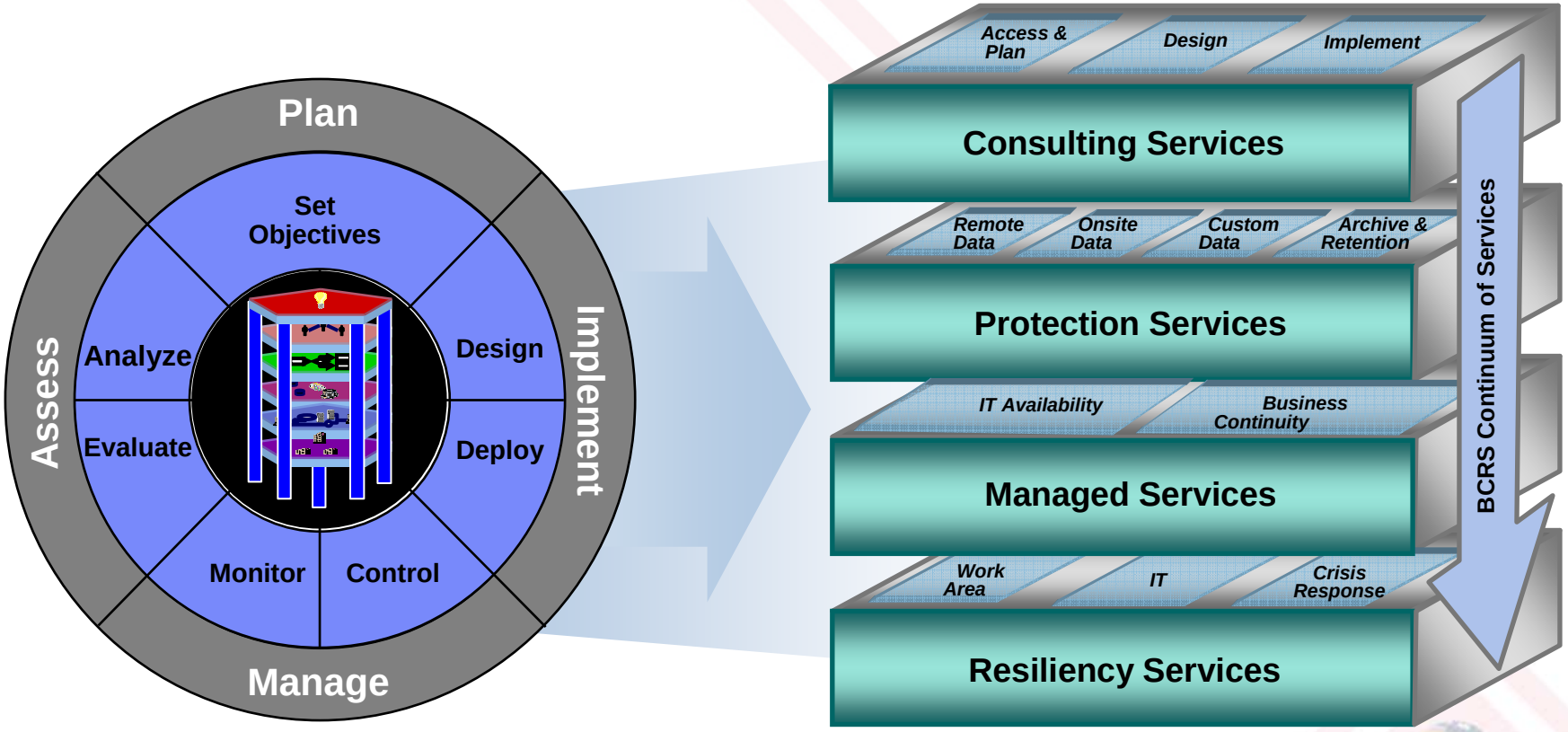
- Control negative risk while enhancing positive risk
  - Ongoing management of risks before, during and after an event
  - Regular testing to ensure preparedness
  - Enforcement of governance policies & procedures
  - Training to ensure all employees understand their roles and responsibilities
  - Proactive information & data protection
  - Accurate communications at all times
  - Access to critical information when needed
- Monitoring current conditions to detect and respond to risks
  - Proactive negative and positive risk response
  - Focus on continuous improvement of risk response strategies
  - Timely reporting of exceptions, measurements and metrics
  - Root cause analysis

IBM's Resilience Enterprise Blueprint Maps Directly to Risk Categories



Sound information is needed to manage each category of risk. Thus, managing information risk well is essential.

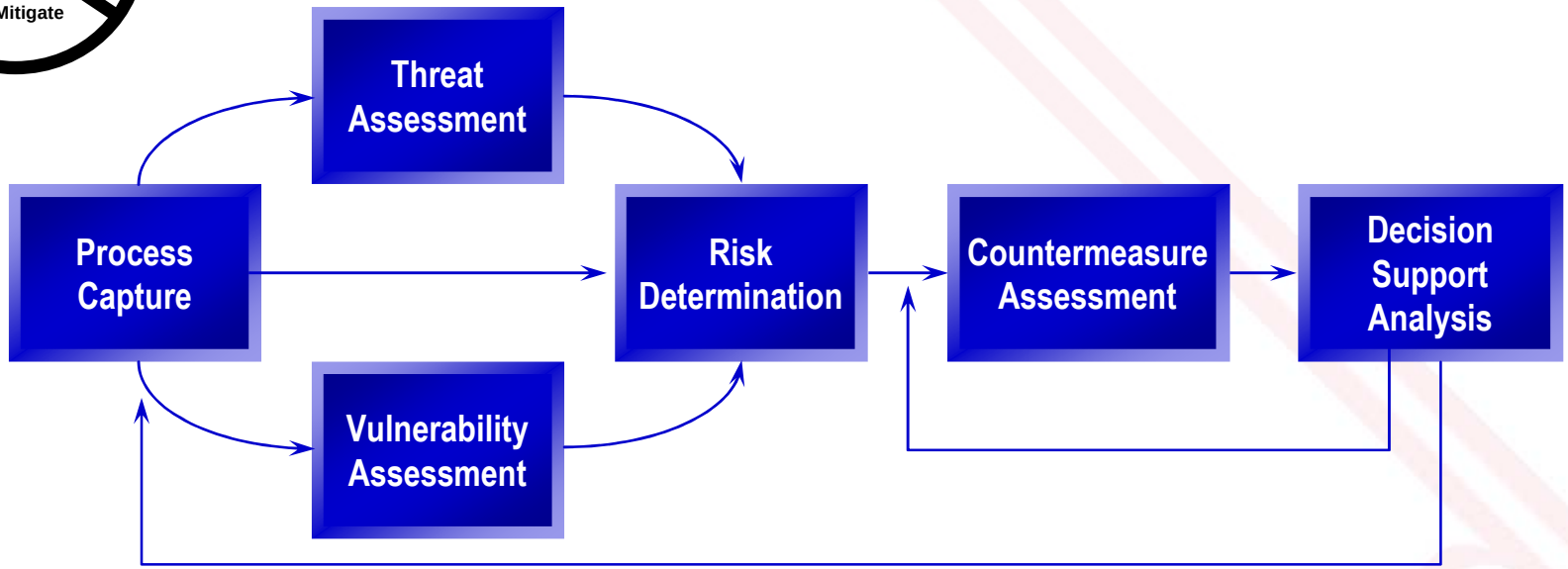
IBM provides services to help realize the strategy and architecture for Operational Resilience



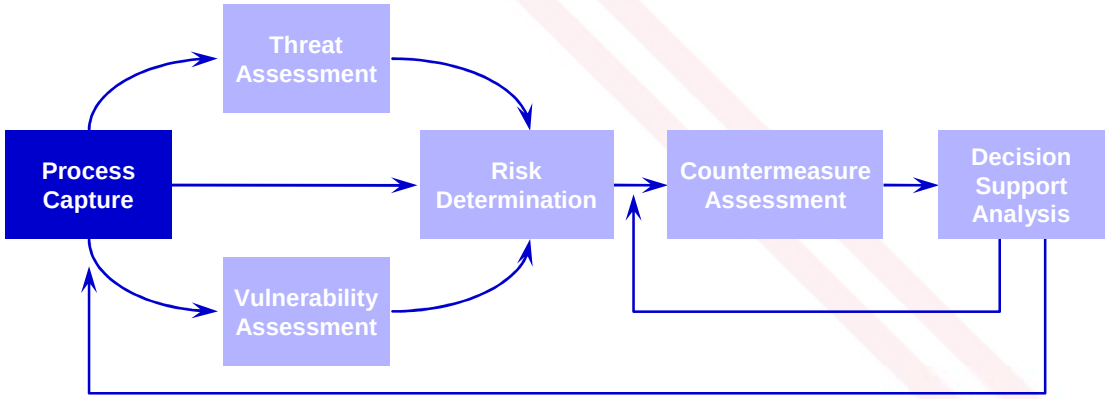
agenda

Risk Assessment Process

Risk Assessment Process



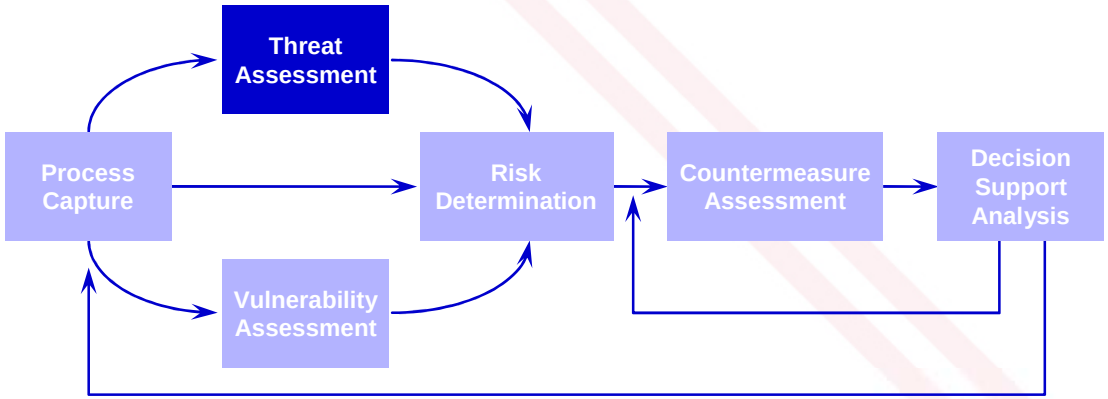
Risk Assessment Process



Process Capture:

- Identify critical/key mega- and major processes (information, physical, and functional) and their dependencies on one another.
- Identify all the infrastructure components that are required to support the various processes. (current and future state)
  - Hardware
  - Software
  - Communications (network protocol, connectivity)
  - Facilities
  - Personnel
- Identify the owners, maintainers, and consumers for the processes and infrastructure components that have been identified.
- Help place both a value (imputed or intrinsic) and importance on critical/key processes/assets.

Risk Assessment Process

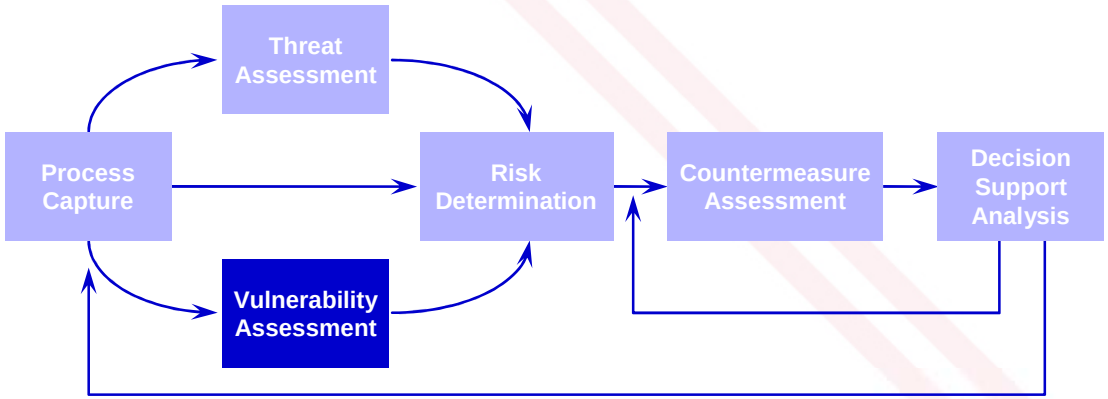


Threat Assessment:

- Identify and rank those threats that apply to the organization.
  - Environmental
  - Man-made
    - External
    - Internal

- Measure the amount of presence a threat has to the organization (physical, electronic, or logical)
- Measure the relative motivation and capability of a threat

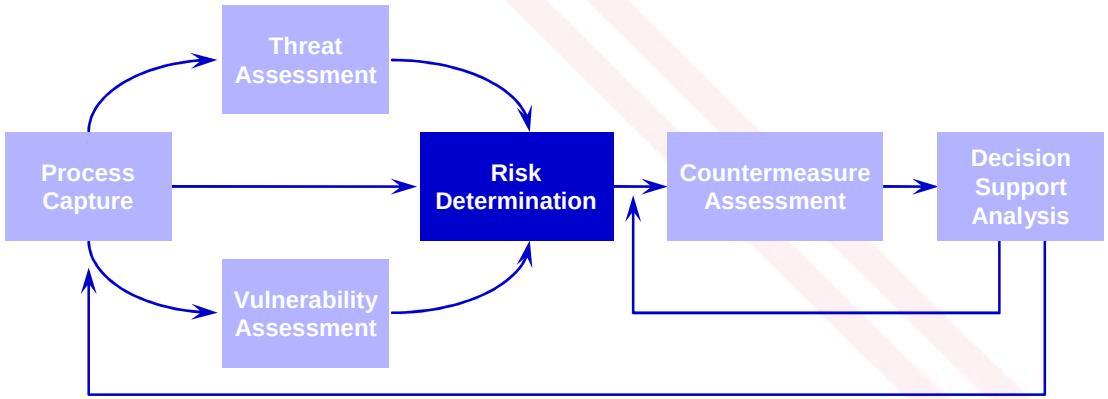
Risk Assessment Process



Vulnerability Assessment:

- Identify and rank the known vulnerabilities associated with the client's specific processes/assets and infrastructure components.
- Vulnerabilities are primarily driven by the system definition completed during process capture.
- Determine if a vulnerability can be exploited via physical or electronic exposure.
- Measure the severity of the vulnerability by measuring:
  - Potential damage caused by exploitation
  - Age of the vulnerability (when it was discovered)
  - Amount of information available for the vulnerability
  - Determine the operational concerns impacted by the vulnerability

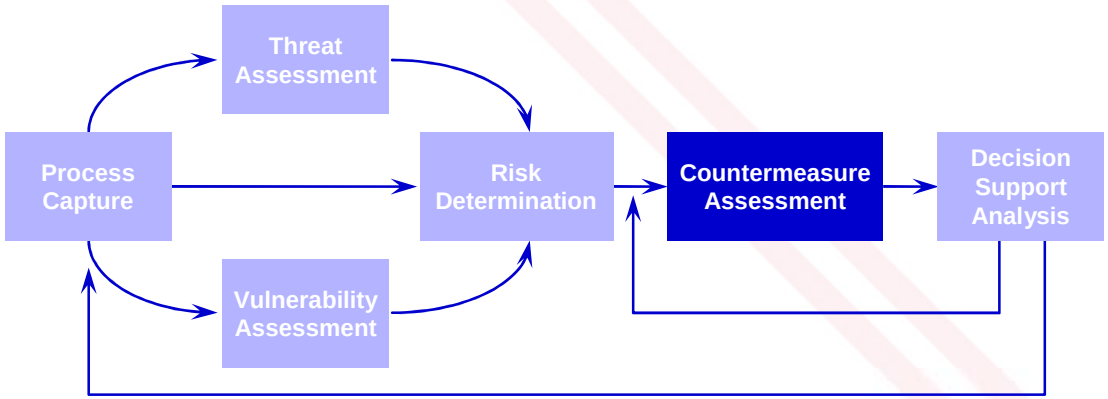
Risk Assessment Process



Risk Determination:

- Risk is the combination of a threat exploiting some vulnerability that could cause harm to some process/asset, based on the threat, vulnerability, and asset measure previously defined.
  - Determine the threats and which processes' or assets' vulnerabilities they can exploit

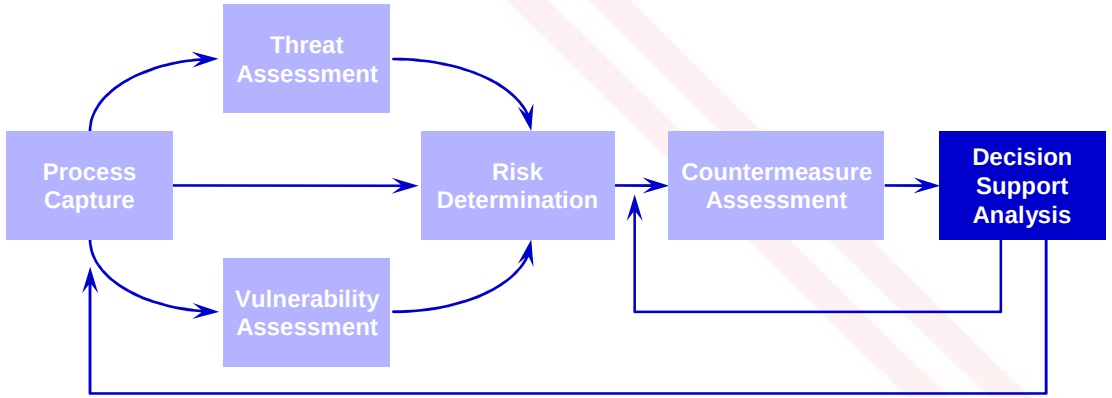
Risk Assessment Process



Countermeasure Assessment

- Identify applicable countermeasures by considering infrastructure-specific threats, vulnerabilities, processes/assets, and components.
- Produce a list of valid countermeasures to support the decision support analysis.
- Countermeasure factors are based on:
  - Process/asset factors: Sensitivity, criticality, perishability, recoverability, quantity, quality, economic value.
  - Threat factors: Physical access, electronic access, capability, motivation.
  - Vulnerability factors: Potential damage, available information.
- Conduct risk mitigation calculations by applying countermeasures to the risk factors they mitigate.

Risk Assessment Process



Decision Support Analysis

- Conduct cost benefit analysis:
  - Identify comparable alternative solution sets
  - Identify the most cost-efficient solution set
  - Consider cost-benefit ratio:
    - Risk delta/cost
    - Highest cost benefit ration implies most cost-effective solution
  - Identify solution leading to the 'biggest bang for the buck'
- For a countermeasure to be considered it must mitigate at lease one factor in the risk measurement.