CIO’s are struggling to address board level requirements that are vastly different from what they were responsible for just 5 years ago.

“I need to manage complexity of compliance across my organization and silos – and be audit-ready all the time.”

“I need to provide access to and recoverability of data at any time.”

“I need to protect against threats – even the ones I’m not prepared for.”

“Lack of resources, expertise and tools to cost effectively manage multi-vendor environments”

How do you…?

• Increase regulatory compliance without increasing capital expenses

• Block potential incoming threats without inhibiting traffic flow, data availability and uptime

• Prepare for the unexpected outage or disaster

Companies face a growing number of growing risks to their IT that continuously stress their ability to deliver service to their customers.

As budgets shrink and service level requirements increase, a company’s business becomes even more vulnerable to IT outages.

The impact of lost data or unplanned downtime can be catastrophic, leading to lost revenue, reputation, and competitive position.

**Finances**

- Lost deals
- Disruption of cash flow
- Lost discounts
- Missed payments
- Drop in stock price

**Revenue**

- Loss of direct revenue
- Loss of future revenues
- Losses due to invoices that cannot be completed
- Losses due to investments not made

**Miscellaneous costs**

- Temporary staff needed
- Travel expenses incurred
- Equipment rental costs incurred

**Productivity**

- Employees who cannot perform their jobs
- Missed deadlines

**Regulatory**

- Inability to meet compliance requirements
At the same time the cost of downtime increases, company’s are inundated with disjointed information.

The amount of information managed by enterprise data centers is expected to increase by at least 50 times over the next decade¹.

The average cost per hour of system downtime is increasing as more business operations become automated².

---

The changing risk landscape will require a shift to a new paradigm that anticipates and integrates daily operations, emergency management & business continuity

- Handle both emergency and non-emergency events, tests and alerts.
- Organize response teams, enabling fast and clear communications between team members.
- Define and provide standard operating procedures for varying situations, with proper assignments, based on legal requirements or historical experience.
- Track the progress and performance of procedures, including the results of the actions for rehearsals and events.
- Locate and manage resources with the required capabilities and skills to handle the events.
- Enable the continuous improvement of the organization’s services and responses.

IBM has seen this shift coming for a while and understands that this is part of the evolution from disaster recovery, business continuity and business resilience into the era of Intelligent IT Risk.

IBM BCRS founded in 1989

---

The definition of IT risk is drawn from several synergistic points.

1. Business results are inextricably reliant on IT service thus IT must support critical business processes and key initiatives by being
   - reliable,
   - predictable,
   - available and
   - secure.

2. “IT” is much broader than “infrastructure” (boxes and network) and includes process, people, data and applications, facilities, and business and IT strategies.

3. “IT” is under intense pressure to execute thus must be:
   - flexible and appropriate,
   - available and recoverable,
   - scalable and ready to perform,
   - secure and protected,
   - accurate and timely.

- Thus, “IT Risk” is “The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.”
Intelligent IT Risk will use predictive risk analytics tied to response capabilities designed to ensure continuous operations.

Predictive risk analysis integrated within the business’ daily operations helps to filter business critical information so they may anticipate problems and opportunities to make the right response faster.

- Leveraging information to make better decisions
  - Large scale situational awareness
  - Mitigate risk across wider risk spectrum
  - Respond to risk and opportunities

- Anticipating problems to resolve them proactively
  - Monitor multiple, diverse inputs
  - Manage key risk indicators
  - Prepare earlier to cut response time

- Coordinating resources and processes to operate effectively
  - Intelligent response integrated with the fabric of the business Continual involvement versus one time training

IBM has created a framework for identifying the risks associated with the use of IT that takes a broad and integrated view starting with an understanding of the core business requirements.

IT risk management requires the analysis of a broadly linked IT Risk Spectrum that goes beyond the traditional view of business continuity.

- **Agility & Appropriateness**: respond in a timely manner with the correct new or modified IT Service in support of changes in business requirements
- **Availability & Recoverability**: keep systems running and, if necessary, recover from interruptions in line with business expectations.
- **Accuracy & Timeliness**: provide accurate data, to the right people, at the right time to make informed business decisions.
- **Security & Data Protection**: provide the appropriate access controls while protecting the business’ information and resources
- **Scalability & Performance**: maintain acceptable performance based on business needs and appropriately accommodate changes in business service volume
- **Process**: How company conducts its core business through business process modeling and IT governance
- **Technology**: Equipment and tools that support the company’s business processes
- **Suppliers**: Businesses and government agencies that provide the critical materials, services and information
- **People**: Human resources with assigned responsibilities within the company and the processes to maintain
- **Infrastructure**: Components under company control that enable operations
- **“Exo-Structure”**: Ecosystem components outside company control (power, water, food, roads, communications and governance

The IBM Risk Spectrum is applied against the company’s business resilience delivery framework and can be “decomposed” for both dependency and parallel analysis.
Our methodology helps a company to understand their strategic business goals and risks to create a real-time IT risk management system.

1. ASCERTAIN and align strategic business goals with value of IT services
2. ASSESS IT risks and capabilities
3. ACT to create an ongoing IT risk management governance system

- Identify Strategic Initiatives against IT service risk treatment and roadmap
- Map strategic initiatives to Organization and IT support processes and services with measurable indicators and potential impact to initiatives
- Categorize IT performance metrics against the IT Risk Spectrum

But KRI’s are only useful if you can combine real-time monitoring and predictive analytics with robust response capabilities.

A effective IT Risk strategy includes defining and measuring Key Risk Indicators (KRI) customized to each company’s unique requirements.

Companies must have access to flexible and dynamic information readily available that can be used to assess the current situation and take appropriate action.

- Event correlation detection
- Executive Dashboard
- Role based views
- Data drill down
- Video Analytics
- 3D modeling

Social interaction
Integrated system monitoring
Click to Action
Progress reporting
The use of predictive analytics and a robust command center allows for improved efficiency, management, collaboration and response to events.

**GOAL:** Collaborate and respond to events.

- **Global Operations**
  - Mega Centers
  - Work Area

**GOAL:** Get the right information to the right people at the right time for rapid problem resolution.

**GOAL:** Effectively manage events and return to a steady state.

**GOAL:** Ensure that the managed environments maintain operational efficiencies.

**Intelligent Response**

- Plans
- Business Rules
- Available Resources

- GOAL: Anticipate to provide real-time response using best practice SOPs, workflows, and resources.

- **Intelligent Operations**
  - The use of predictive analytics and a robust command center allows for improved efficiency, management, collaboration and response to events.

**Example scenario**

**Rapidly respond to emergencies**

- Standard Operating Procedures (SOP) • Extreme Weather Event Preparation • Flash Flood Preparation • Evacuation

**Example Scenario:**

Heavy rains are predicted to cause large scale flooding in the city where the business’ main processing center is located. The center monitors sources that predict the magnitude of the storm and possible outcomes. This will allow the center to start the SOPs that are needed for extreme weather preparation.

As the weather incident continues to affect the city, additional SOPs can be activated to send people home, begin critical backup, move operations, or mobilize additional resources. As these predetermined SOPs execute, constant situational awareness events from the center can be used to ensure the most appropriate response is delivered.

1. Predicted extreme weather
2. Situational awareness engines monitor weather feeds in the center
3. Rules engines will start automated responses via standard procedures (SOPs)
4. The center will manage the most appropriate response based on the situational awareness information and the incident in hand

**Combining predictive analytics and business continuity capabilities into an intelligent command center provides near and long term cost efficiencies.**

The right business resilience strategy can help you:

- **Mitigate risk**
  - Avoid the costs of downtime, brand damage and market share lost to competitors, and reduce the financial impact from business disruptions
- **Protect brand and revenue**
  - Properly assessing the dynamic threats to your IT infrastructure, their potential business impact and your tolerance for risk can help you plan a realistic strategy
- **Protect capital**
  - Analyzing cost tradeoffs can help you avoid unnecessary investments
- **Reduce costs**
  - Creating proactive SOPs with tested response capabilities can help protect you from costs associated with failed recovery and lost data
- **Improve service**
  - You can better align a resilient infrastructure to the needs of your business to maintain service level agreements based on your tolerance for risk

**Thank you**

Richard Cocchiara
IBM Distinguished Engineer
rmcocch@us.ibm.com
1-845-759-2043

ibm.com/services/continuity