

BC46: BC on the Front Line; Product Reliability at Thomson Reuters

Eric Staffin, MBCI, CBRM, CBRA, CBRP
Global Head of Product & Infrastructure
Risk Mgmt., Investment & Advisory
Thomson Reuters
eric.staffin@thomsonreuters.com
917-779-6919



THOMSON REUTERS

Doug Weldon, FBCI, CBRM, CBRA
President, Vigilant Services Group
dnweldon@vsg1.cc
407-492-9676



Presentation Outline

- BC – Beyond Recovery and Continuity
- Gathering Requirements from the Front Line
- Deriving Enterprise Requirements from Stakeholder Requirements
- Components of Competitiveness
 - Utility and Warranty
- How Optimum Warranty is Achieved
 - Reactive Approach
 - Proactive Approach
- “Advanced” Business Resiliency Programs

Thomson Reuters - Overview

Born from two powerful companies, Thomson Reuters is unified by the common goal to provide the world's professional markets with Intelligent Information to create Knowledge to Act.



- Applications used by over half a million professionals globally



- Informs healthcare decisions affecting 150 million lives



- Westlaw is relied upon by 98% of the world's major law firms



- Reuters News reaches over one billion people daily



- Used by more than 20 million researchers worldwide



- Checkpoint is used by 99 of the top 100 U.S. accounting firms

Markets Division (\$7.4bn revenue)

Professional Division (\$5.1bn revenue)



A truly global company...

Thomson Reuters unites the traditional strength of Reuters in Europe and Asia with the strong footprint of Thomson in the US and Canada to serve our customers on a global scale

Business Resiliency Program – Key Drivers

- Thomson Reuters' clients in the Corporate and Financial Industries are the most advanced in the world in terms of managing risk and in the maturity of their business resiliency programs.
- Thomson Reuters operates in highly competitive (and in some cases commoditized) industry segments where market prices cannot always support the most advanced and resilient infrastructure, and where customers often prefer to pay for utility and performance warranties over inter-site resiliency and geographic redundancy.
- Client requests for SLAs are numerous and can be exacting.

Program Objectives

Protect, safeguard, secure, and sustain company assets (people, systems, facilities, and information)

Establish a framework that ensures continuous focus on client retention through product reliability

Elementize and prioritize threats, operational risks and business resiliency in a cost effective manner

Establish a management system that ensures compliance with corporate governance guidelines, contractual commitments, strategic priorities, and legal and regulatory standards and guidelines

Program Requirements

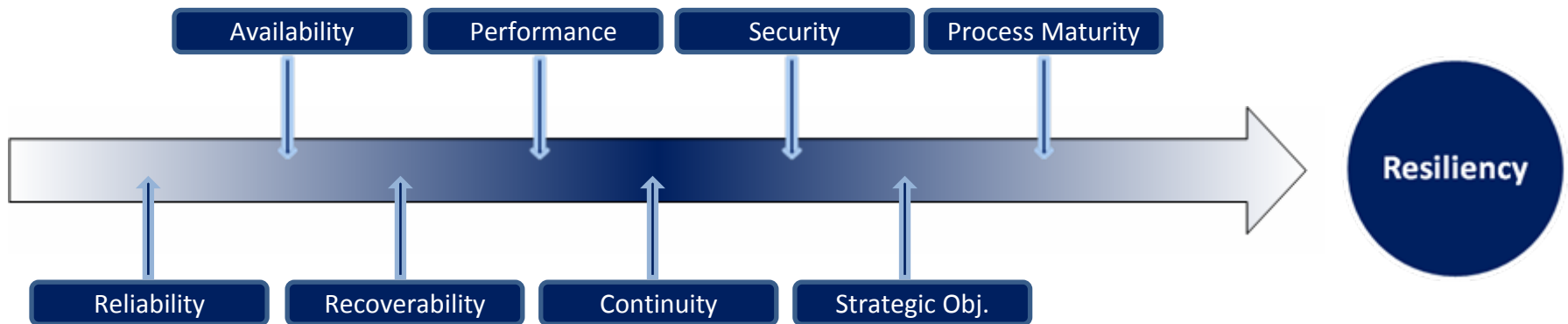
Adherence to Corporate Governance guidelines, client contractual commitments, and all applicable regional legal, regulatory, and exchange requirements.

Continuous alignment with corporate Strategic Planning and Risk Management guidelines.

Help to maximize product competitiveness through the proper application of risk management and resiliency processes and techniques.

Evolution to Resiliency

- Long Maturation Process
- Increased Integration Over Time
- Sustainability & Repeatability
- Becomes Embedded in Enterprise Risk Management Framework



Resiliency Starts at the Front Line

External Stakeholders

- Customers
- Regulators
- Shareholders
- Community Members
- Emergency Responders
- Suppliers
- Local Government Agencies

Internal Stakeholders

- Employees
- Dependent Systems
- Auditors
- Human Resources
- Sales
- Technology
- Finance
- Chief Risk Officer
- Facilities
- Legal

Key Drivers of Product Competitiveness

- ✓ Product Features / Functionality
- ✓ Client Service / Support
- ✓ Reputation
- ✓ Price / Price Elasticity
- ✓ Terms and Conditions
- ✓ Stakeholder Requirements / Demands

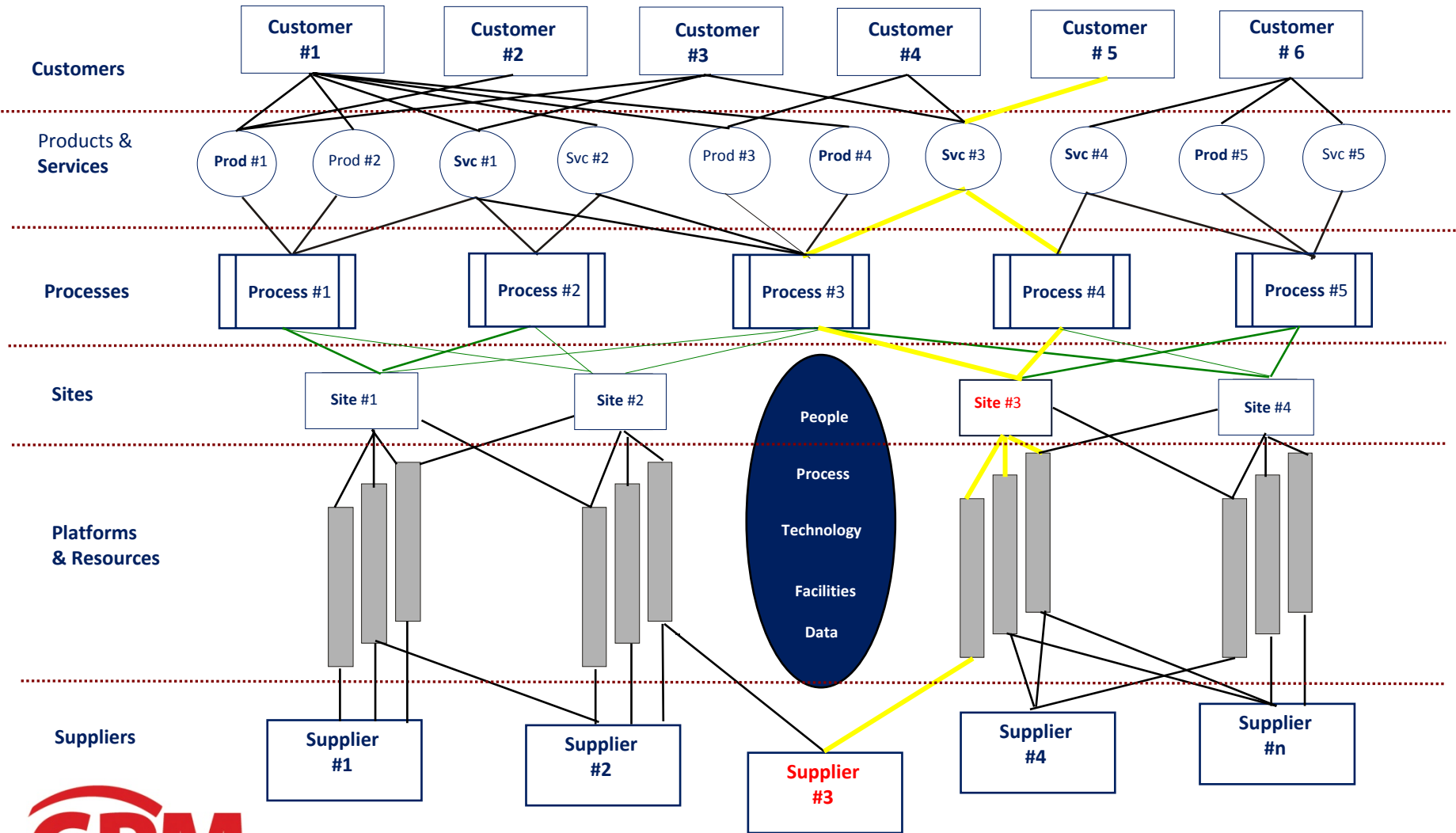
- ✓ **Resiliency**

Resiliency Spending

- Intense competition for resource allocations
- Continuous pull from **Non-Discretionary** spending



Stakeholder Requirements Drive All Other Requirements!



ERM* and Product Risk Management

- Strategic / Market Risk
 - **Product Risk**
- Financial / Credit Risk
 - **Customer SLAs**
- Operational Risk
 - **Product Resiliency**

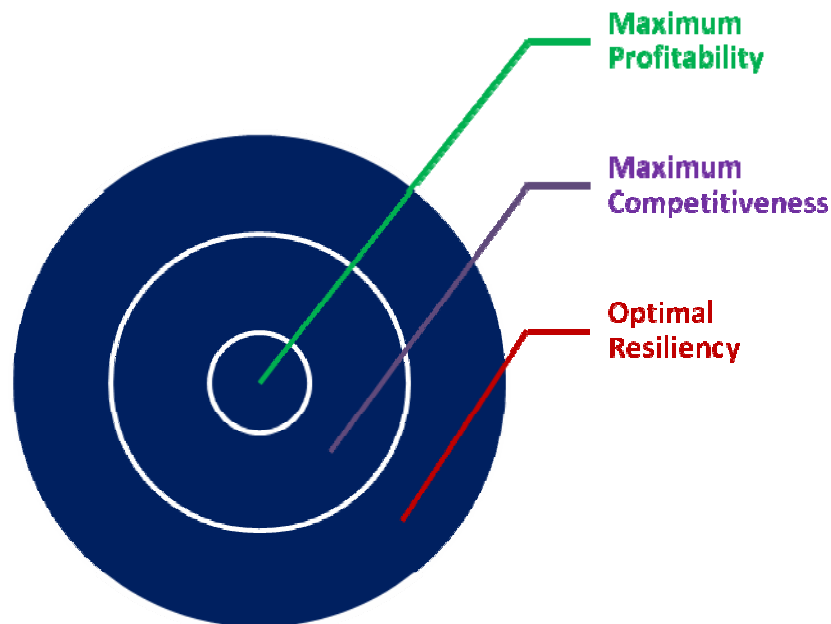


Optimization Strategies

- Optimize
 - Utility *
 - Warranty *



- Optimize
 - Cost **
 - Resiliency **



Typical Story Lines – Reactive / Defensive

- A major product experiences a significant disruption
- One or more significant penalties are assessed based on SLA triggers that have been tripped
- BC and RM people are brought in to try to minimize the damage
- Discovery that SLAs are all different and not consistent with the product infrastructure
- Efforts are made ad hoc to
 - Reduce the penalties
 - Improve product resiliency

Proactive Approach to Customer SLAs

- Customer warranty requirements are part of product design
- Standardize SLAs, as much as possible, in advance
- Match penalties and price to the product infrastructure
- BC/RM people are at the table with the Client and have intervention rights - Gatekeeper!
- Complete transparency to the Client
- Reverse engineer the SLA requirements to dimension the timeline
- Only accept SLAs that match the organizational model and risk / resiliency strategies

Service Level Agreement – Balanced Approach



From

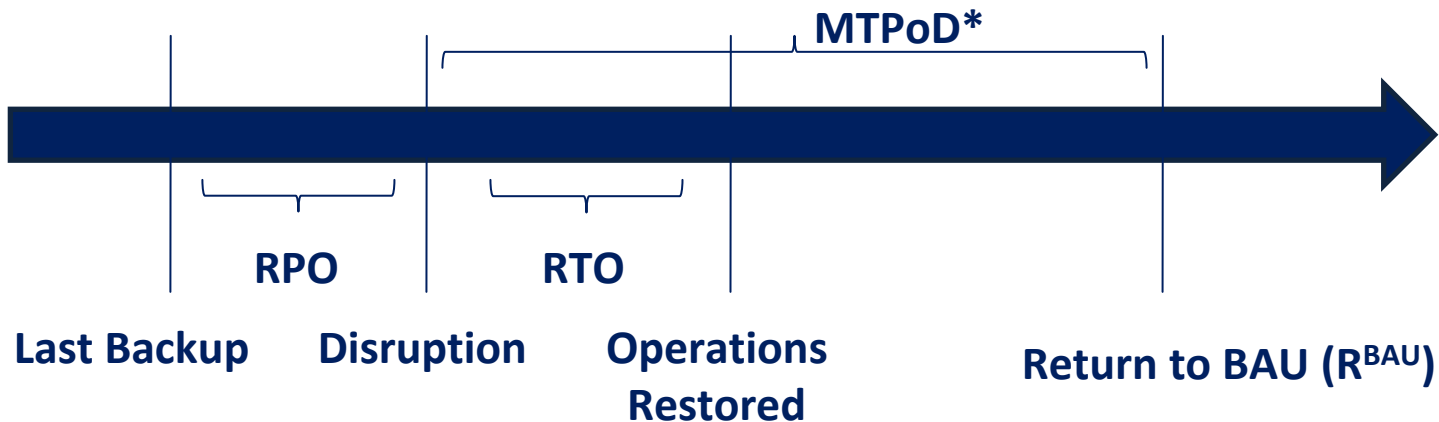
- ✗ Legal Problem
- ✗ Technical Avoidance
- ✗ Owned by Sales
- ✗ Buyer Power
- ✗ Deal-centric
- ✗ Deal Opener
- ✗ Commercial Exposure
- ✗ Enterprise “Headache”
- ✗ Lose - Lose

To

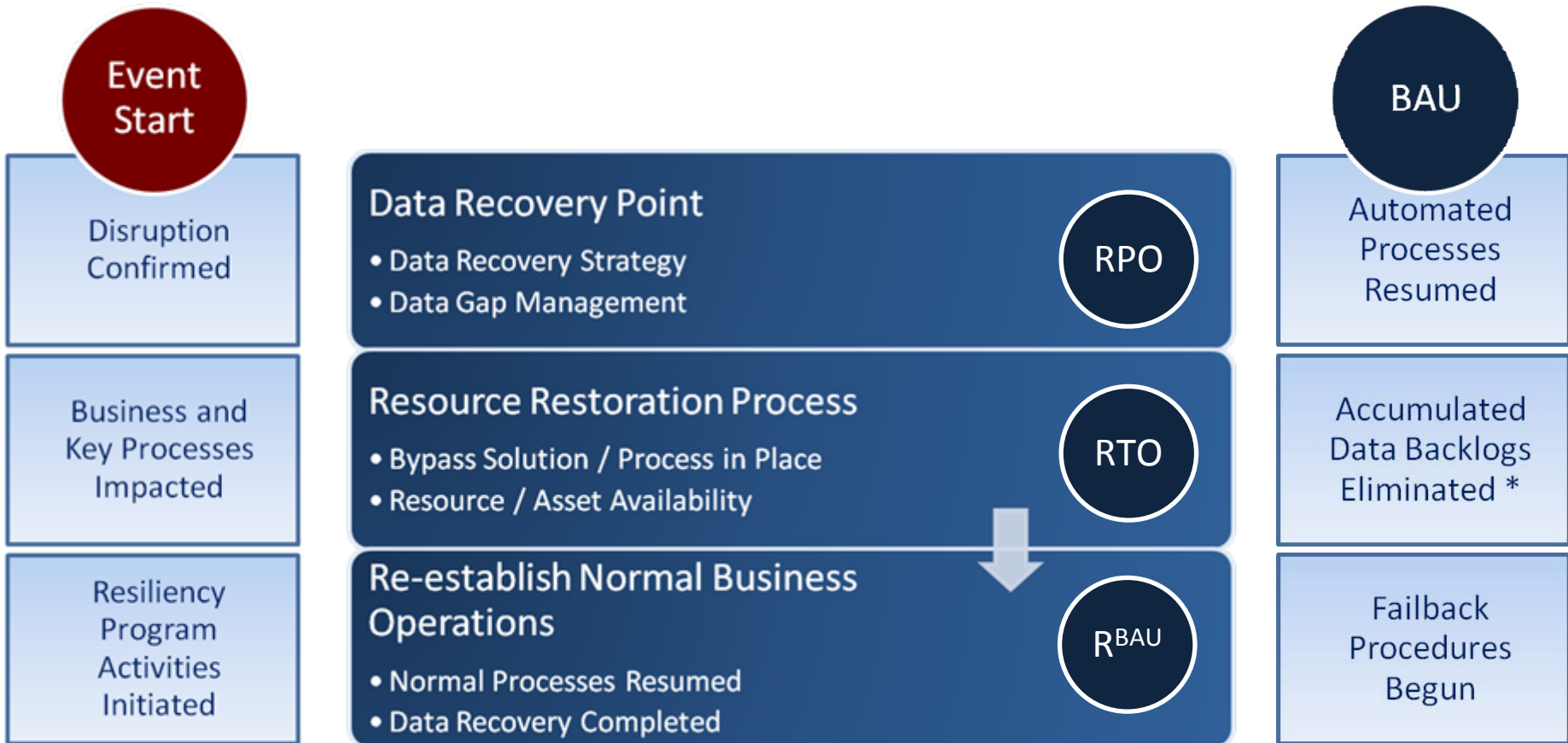
- ✓ Business Concern
- ✓ Organizational Ownership
- ✓ Owned by CRO / BCO
- ✓ Supplier Power
- ✓ Process-centric
- ✓ Deal Closer
- ✓ Managed Risk
- ✓ Enterprise “Survival”
- ✓ Win – Win

Typical Major Disruption

- 12 Hour Disruption
 - 1 Hour Analysis and Escalation
 - 3 Hours Remediation
 - 4 Hours Recovery
 - 4 Hours to Return to Business As Usual (R^{BAU})



Incident / Disruption Lifecycle



* September 14, 2007: According to an IDC report, over 90% of companies fail within one year of a significant data loss.

Incidents / Disruptions ➤ Commercial Exposure

How do we understand, capture, and measure the risk and likelihood of commercial exposure ?

- Ability to Meet Recovery Time Objectives (RTOs)
 - Ability to Meet Recovery Point Objectives (RPOs)
 - Business Impact Analysis (BIA) Data
-
- Client Service Level Agreements (SLAs)
 - Historical Incident Management Data
 - Ability to Return to Business as Usual (R^{BAU})

<u>Incident Duration (Hours)</u>	<u>Commercial Exposure (\$ Millions)</u>
0	0
6	1
12	5
24	10
48	20

MTPoD = \$15MM
Total Product Revenue - \$40MM

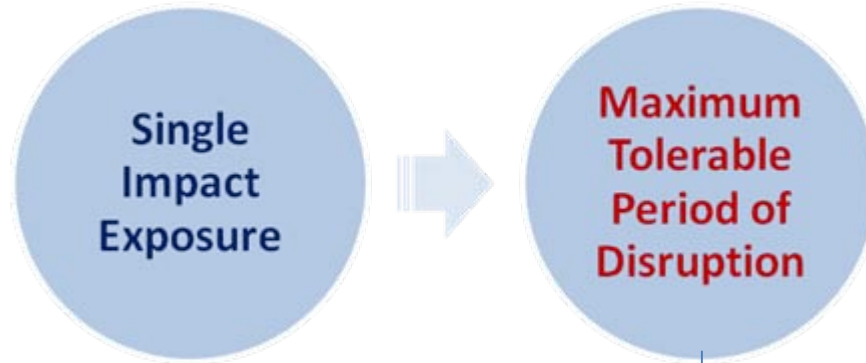
* Maximum Tolerable Period of Disruption (BS25999)

Duration after which an organization's viability will be **irrevocably** threatened if product and service delivery cannot be resumed

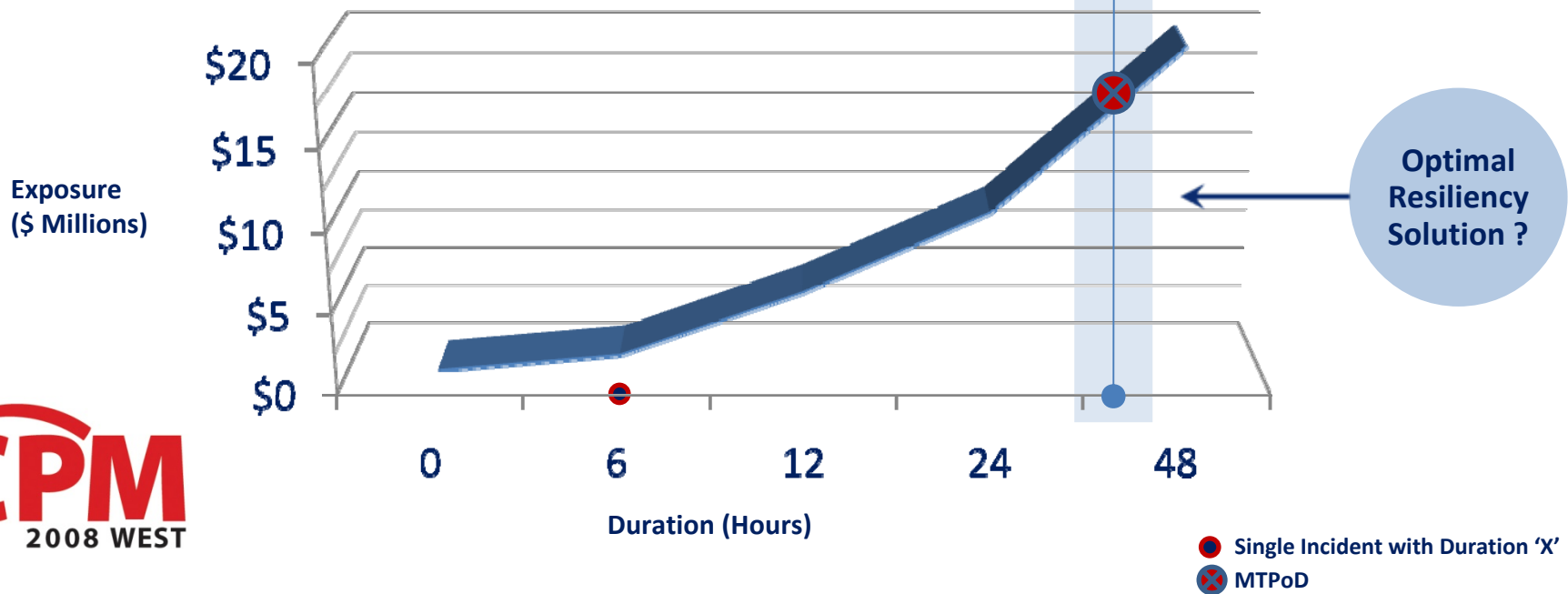
Incidents / Disruptions ➤ Commercial Exposure

Incident Duration (Hours)	Commercial Exposure (\$ Millions)
0	0
6	1
12	5
24	10
48	20

MTPoD = \$15MM
Total Product Revenue - \$40MM



■ Exposure



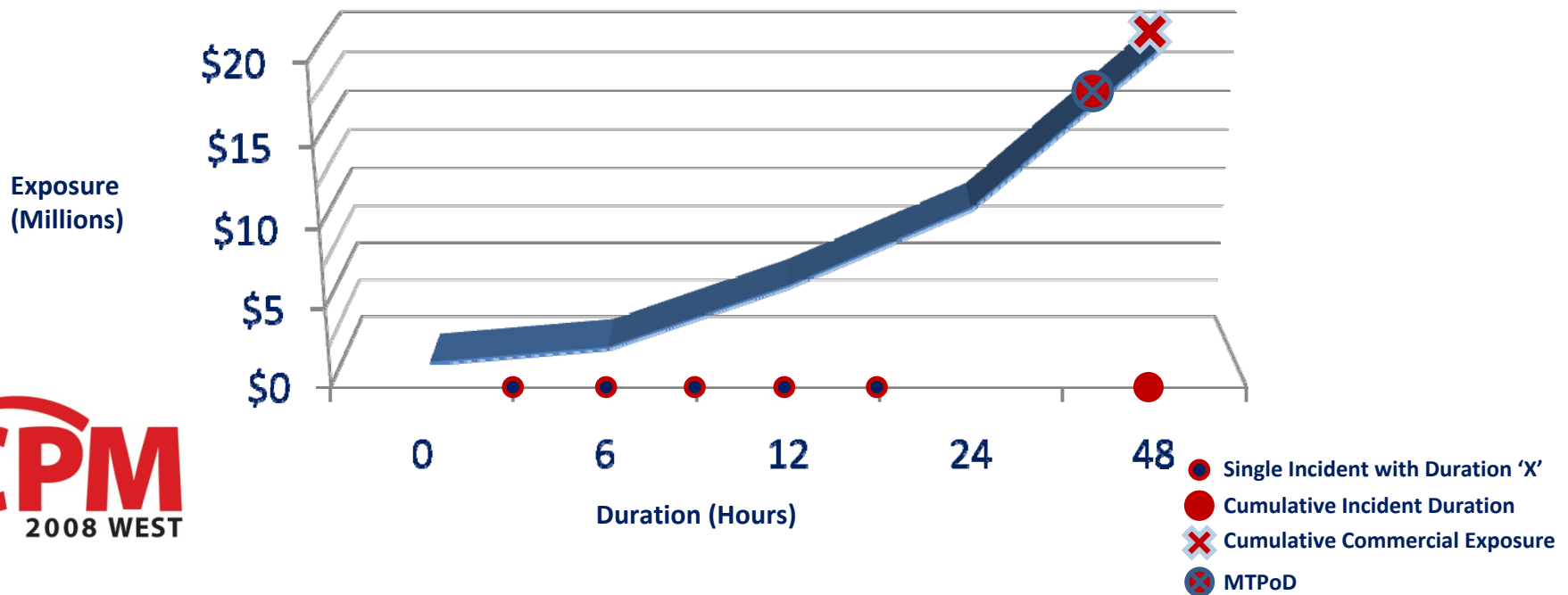
Incidents / Disruptions ➤ Commercial Exposure

Incident Duration (Hours)	Commercial Exposure (\$ Millions)
0	0
6	1
12	5
24	10
48	20

MTPoD = \$15MM
Total Product Revenue - \$40MM



■ Exposure



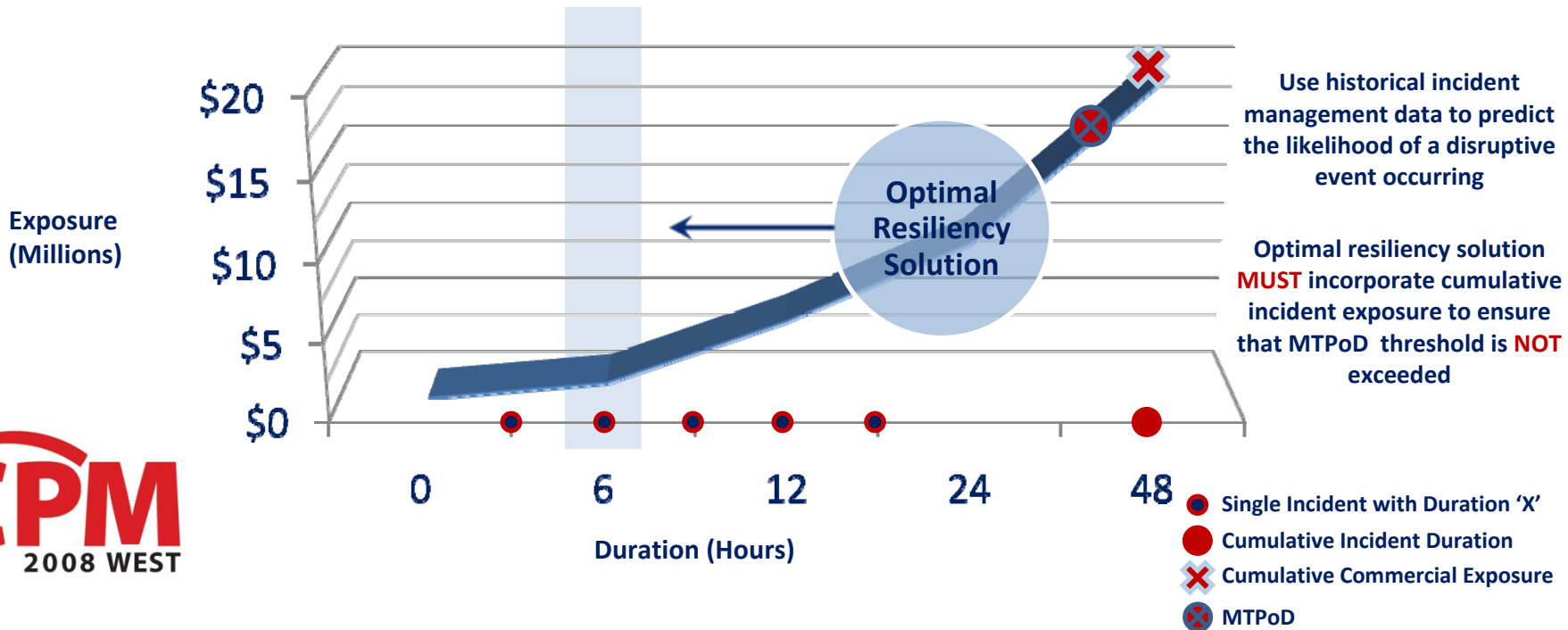
Incidents / Disruptions ➤ Commercial Exposure

Incident Duration (Hours)	Commercial Exposure (\$ Millions)
0	0
6	1
12	5
24	10
48	20

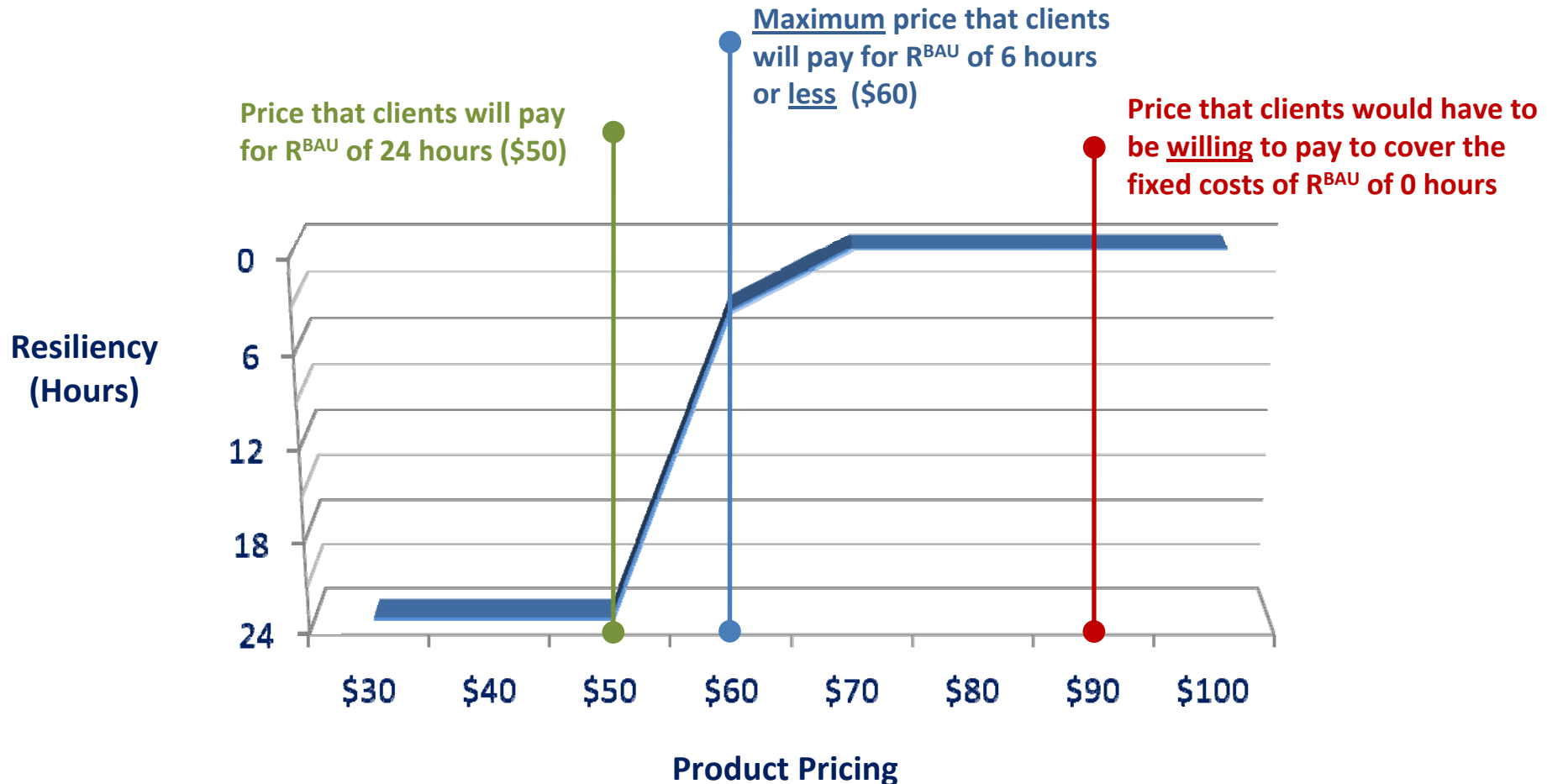
MTPoD = \$15MM
Total Product Revenue - \$40MM



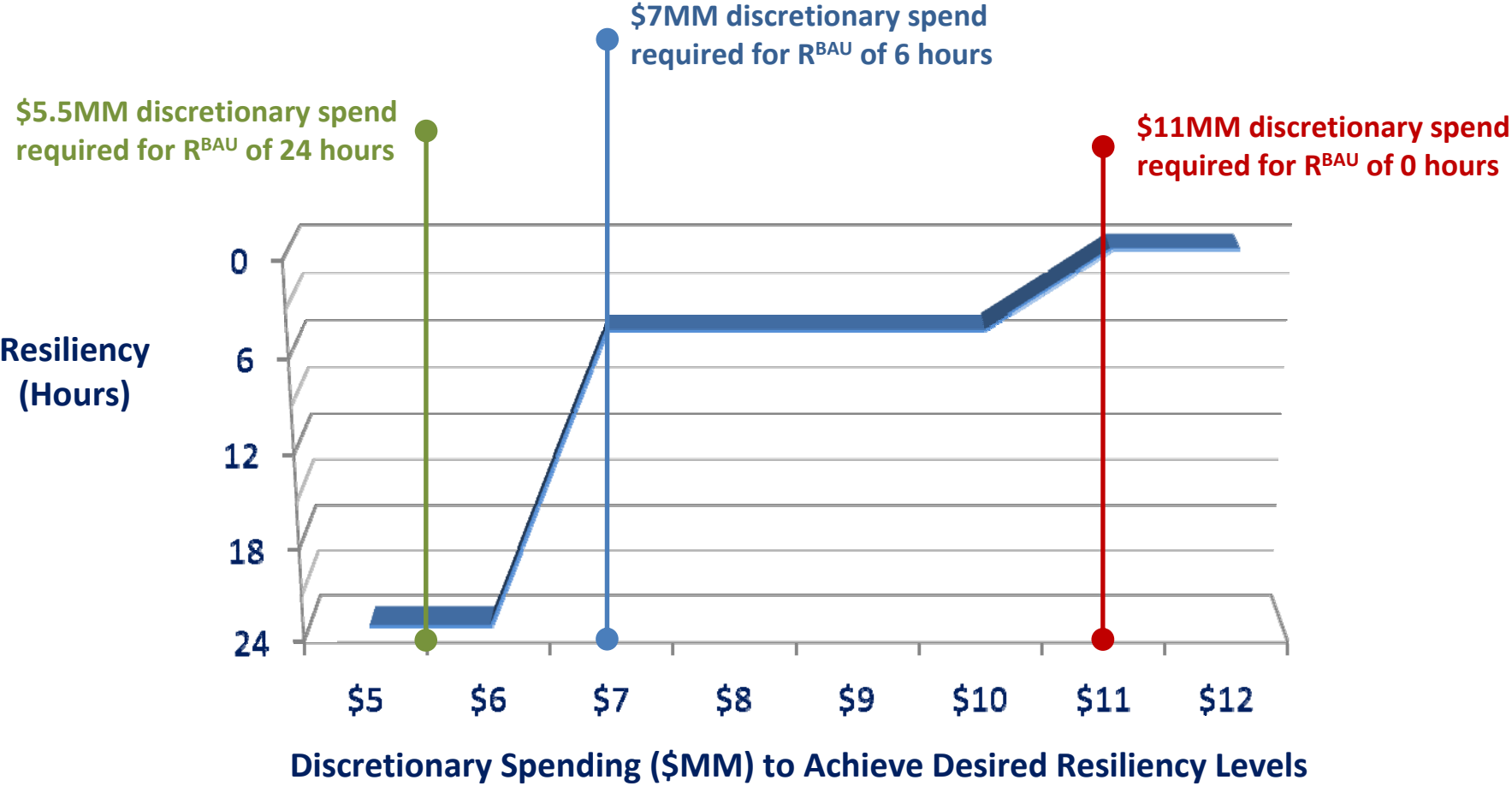
■ Exposure



Margin as a Function of Resiliency and Price



Discretionary Spending as a Function of Resiliency



Business Resiliency Program - Index

Plan	Do	Check	Act	Appendix
<ul style="list-style-type: none"> • Policy Objectives and Requirements • Scope • Assumptions • Program Risks • Definition of Plan-Do-Check-Act • Plan Resource Allocation • Promoting the Program • Records and Documents Repository and Control • Criteria Matrix • Enterprise Incident Management • People and Facilities Continuity • Infrastructure and Content Recoverability and Resiliency • Common Infrastructure Resiliency Documentation • Contract Compliance • Supplier Recoverability • Annual Management Sign-Off for Plans 	<ul style="list-style-type: none"> • Strategy • Operational and Product Risk Management • Risk Analysis • Risk Mitigation • Prioritization • Product Analysis Inputs and Workflow • Product Analysis Reporting • People and Facilities • Plan Audit • Systems and Content Audits • Development and Implementation Testing • Maintenance • Post Incident Review • Remediation Work 	<ul style="list-style-type: none"> • Analyze Results and Trends of Individual: • Plan Walkthroughs • Table Top Testing • Process or Plan Simulations • Full End to End Simulations • Resiliency Documentation Audits • Revalidate Risk Assessment Inputs/Outputs • Revalidation of Planned Production Failover Testing • Analyze Results of Client Audits • Analyze Results of Individual Plan Audits • Program Audit – Stage Consolidation Table 	<ul style="list-style-type: none"> • Program Audit Output – Perform Corrective Actions as Required • Program Audit Output – Perform Preventative Actions as Required • Program Maintenance – Update Policy, Objectives, etc. as Required • Perform Management Reviews at Least Annually 	<ul style="list-style-type: none"> • Policy • References • Kits • Business Resiliency Documents • Business Impact Analysis • Application Impact Analysis • ERM Assessment • Product Resiliency Program - Rolling Four Quarter Plan • Business Continuity Program - Rolling Four Quarter Plan • Reference Documentation • Template Details • BC/DR Common Client Queries • Glossary • Data Center and Pop Site Matrix Plans

Business Resiliency Program – Key Documents

Service Summary

- Summary Description
- Key Contact List
- Billing System Used
- Key Clients
- Client Turnover and Growth Profile
- Client Contractual Requirements

Service Description

- Detailed Description
- IT Work Flows
- Business Operations Work Flows
- Business Operations Dependency Mapping

IT System Description

- Application Flows
- Authentication and Entitlement Flows
- Log Flows
- Systems Dependency Mapping

Data/Content Description

- Sources and Uses of Data
- Data Flows
- Database Schema

Service Infrastructure

- Network Design/Infrastructure
- Network Equipment/Services Inventory/Suppliers

Hardware Infrastructure Configurations

- Hardware Inventory/Suppliers
- Software Inventory/Suppliers
- People/Space Profiles

Service Resiliency Requirements

- Reliability/Availability Requirements
- Performance Requirements
- Recovery/Continuity Requirements

Service Risk Assessment

- Incident History/Statistics
- Security Assessment
- Disaster Recovery/Failover Assessment
- Business Continuity Assessment
- Service Management Assessment
- Service Functionality Assessment
- Resiliency Assessment Rollup

Service Reliability/Resiliency Strategy and Infrastructure

- Strategy Summary
- Network Design/Infrastructure – Firewall and Other Security Infrastructure
- Data Backup and Recovery/Continuity Infrastructure
- Reliability/Availability Infrastructure
- IT Disaster Recovery Infrastructure
- IT Continuity/Failover Infrastructure
- Business Operations Recovery/Continuity Infrastructure

Service Resiliency Procedures

- Incident Management Procedures
- Monitoring (Error Handling/Logging) Criteria for Failure/Troubleshooting Procedures
- Escalation Procedures
- Criteria for Disaster/Declaration Procedures
- Security Procedures
- Data Backup and Recovery/Continuity Procedures
- IT Disaster Recovery Procedures
- IT Continuity/Failover Procedures
- Business Operations Recovery/Continuity Procedures
- Restoration Procedures
- Service Resiliency Testing and Maintenance
- Change Management Process
- Code Repository (Source Control)
- Resiliency Testing Plan/Schedule
- Resiliency Maintenance Process and Schedule
- Training and Awareness Plan
- Common Infrastructure Resiliency Documentation
- WAN Network
- LAN Networks
- Data Centers
- Data Bunkering
- Common Office Space Recovery

Resiliency Planning & Prioritization

- ✓ Prioritization of initiatives is determined by a number of inputs that highlight commercial and reputation risk.
 - Products that have had significant down time during a specific measurement period
 - High calculated risk based on product infrastructure and surroundings
 - Products where commercial exposure exists due to Client contractual warranties and commitments (SLAs)
- ✓ Inputs and drivers should be updated on a near real-time basis, prioritization is reviewed monthly, and the process is formally reviewed annually.

Product		Resiliency			Projects	BIA / SLA Exposure				Historical Outages Details				
Product Name	Prior Year Revenues	Geographic Redundancy	Tested	MTPoD	Target Remediation	0	2	24	72	Maximum Outage Duration (minutes)	Number of Outages	Total Outage Dur. in Previous 6 Months	Average Duration	Max Severity

Organizational Design

- Design, develop, enhance, and implement a global program to identify critical performance, reliability, and disaster recovery gaps.
- Drive the implementation, validation, operationalization, and auditability of sanctioned disaster recovery, stabilization, and client-facing product resiliency initiatives.
- Negotiate, monitor, and manage client Service Level Agreements (SLAs).
- Drive improvement in underlying component/infrastructure reliability, improve client perception of product reliability, and reduce the risk of technical SLA-related penalties.
- Drive the analysis, recognition, prioritization, recovery, and application infrastructure remediation efforts to improve product speed, stability, and reliability, and minimize commercial exposure on system outages.

Summary and Conclusion



- Establish a preventive approach to identify, assess and measure operational and product risk factors
- Understand, measure, and capture commercial risk and exposure
- Selectively control the factors which could lead to any negative impact on revenue, profitability, and/or structural assets
- Programmatically follow an operational risk management framework in order to assess threats and vulnerabilities, and the likelihood of these vulnerabilities being exposed
- Produce a qualitative and quantitative risk management summary for the corporation and provide recommendations for resiliency planning initiatives.
- **Drive execution!**