sia partners
Pioneer of Consulting 4.0

Operational Resilience

Marketing Presentation

June 2020

Eric Blackman
John Gustav

Scott Arden
Wayne Hu
William Palumbo
Joseph Willing
Robert Rowland
Greg Angelopoulos

Operational Resilience: The World – and Your Business - Interrupted

Earlier this year, very few predicted the unprecedented lockdowns and workplace disruptions that have resulted from COVID-19. Seemingly overnight, businesses are facing challenges across the enterprise that are testing even well-prepared teams.

Businesses today must anticipate any and all contingencies that could dramatically interrupt operations for a significant period of time.

Operational Resilience: The World – and Your Business – Interrupted

Operational Resilience is "the ability to prepare for and adapt to changing conditions and disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." (FFIEC Handbook)

Working across five critical areas – Business Continuity, Technology Disaster Recovery, Threat / Risk Assessment, Cyber Resilience, and Third-Party Risk – Sia Partners can support your business in becoming operationally resilient by preparing for, responding to and remediating disruptive events.

BUSINESS CONTINUITY

A system of prevention, mitigation, and recovery from potential threats to a company. It ensures that personnel and assets are protected and able to function and recover quickly in the event of a disaster.

THREAT/ RISK ASSESSMENT

The Threat/Risk Assessment identifies and prioritizes potential threats using historical and forecast data and assesses their financial and operational impacts on mission critical business functions.

TECH DISASTER RECOVERY

The recovery of enterprise information technology applications and business supporting infrastructure. Addresses guidelines for returning operations to a normalized state with minimum disruption.

CYBER RESILIENCE

The ongoing protection of technology assets and infrastructure from nefarious activity and disruption. Enables organizations to respond and recover from incidents and limit the severity of future attacks.

THIRD PARTY RISK

Addresses a firm's dependence on outside parties to perform activities and services. It is measured against the likelihood that an outside party is unable to provide the services required to support a firm's needs.

SIA PARTNERS SOLUTIONS

- Governance
- Technology Assessment
- Crisis Management Framework
- Peer Review
- Audit and Reg Remediation
- Second Line of Defense
- Ad Hoc Solutions

- Business Impact Analysis
- Threat Identification & Analysis
- Stress Testing
- Legal & Regulatory Assessment
- Vendor Assessment & Selection
- Comparison & Benchmarking

- Technology & Infrastructure Assessment
- Disaster Recovery Plan
- Plan Testing & Change Management
- Response & Recovery Strategies
- System Implementation

- Cybersecurity Awareness & Training
- Network Security Assessment
- Data Protection & Cloud Security
- Vulnerability Assessment & Penetration Testing
- Incident Response Framework

- Third Party Risk Reviews
- Service Level Agreement (SLA) Analysis
- Ongoing Third-Party Performance Monitoring
- Process Design & Procedures
- Data Management
- Vendor Continuity Management

COMMUNICATION STRATEGY

PROCESS RE-ENGINEERING

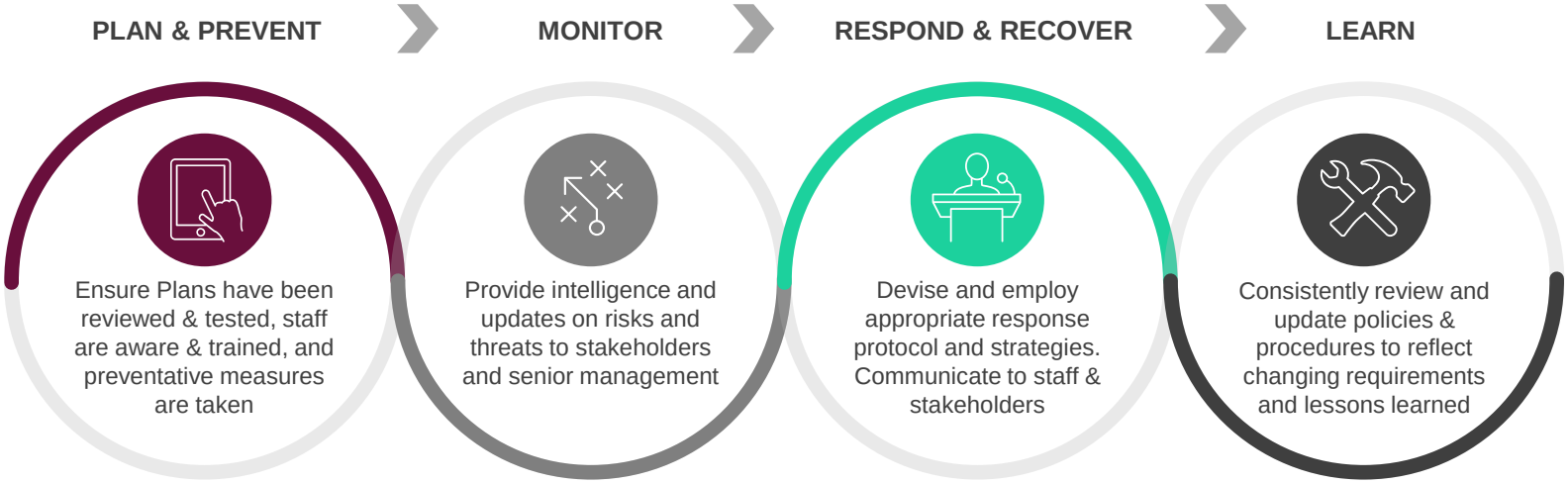
POLICIES & PROCEDURES

STRATEGY & PLANNING

REPORTING

Business Continuity

Business Continuity ('BC') is a system of prevention, mitigation, and recovery from potential threats to an organization's people, infrastructure, process, and assets. Business Continuity Management ensures that the organization is prepared to quickly respond to and recover from business disruptive events.



BC PLANNING

- Business Continuity Plan Template/Structure
- Business Unit Hierarchy
- Recovery Strategies
- Process Taxonomy
- Business Impact Analysis
- Risk Assessment
- Reporting & Dashboards

BC TESTING

- Test Scripts and Forms
- Testing Strategy
- Testing Coordination
- Roles and Responsibilities
- Workflows / Approval
- Masking / Access Restriction
- Results / Feedback Process

CRISIS MANAGEMENT

- Incident Management
- Response Coordination (Internal / External)
- Communication Strategy (Management / Staff)
- Alerts/Banners / Rapid Notification / Hotlines
- Event Logging
- Training (Internal / External)
- Contact Information (Internal / External)

Technology Disaster Recovery

When a company's IT systems and data are compromised by outside threats such as natural disasters, global pandemics, technology failures, cyber-attacks, it is crucial to have a developed recovery plan to restore and maintain core business functions. Disaster recovery focuses on developing a strategy that will help clients businesses return to normal while minimizing interruptions or loss when an unforeseen hardship occurs. Disaster Recovery strategies should be flexible to cover events of varying impacts to the business and should provide leadership with confidence when navigating uncharted waters.

Fault Tolerance

Despite system or hardware failure, it is imperative for normal operations to keep functioning. Cloud computing allows for business systems to continue operating regardless of technological failure.

Data Loss

Data loss management is crucial as more companies rely on data as part of their core products and services. Many customers trust companies in the handling of personal information. Protecting data is critical to keeping the business running and customers happy.

Network Integration

A challenge faced in the transition to a DR system is minimizing latency between internal and offsite / cloud-based servers. Network optimization tools can be utilized to monitor and manage movement of data.

Sustainability

An effective Disaster Recovery Plan must consider the firm's broader strategy and include future growth plans (locations strategy, third party vendors, organization structure, etc.).

Change Management

A disaster recovery plan needs to be assessed and updated regularly to ensure the recovery model is up to date with new business products, services, and IT systems. Employees should be trained on the plan on an ongoing basis.

Recovery Approach

A disaster recovery plan must be able to support a seamless transition back to a normalized state of business. Businesses should continually test the efficacy of their plan in a variety of scenarios, time periods, and as new threats emerge.

Threat/Risk Assessment

Threat and Risk Assessments identify and prioritize potential threats using historical and forecast data and assesses their financial and operational impacts on mission critical business functions.

The four steps below make up the Risk Assessment process. Risk Assessments are conducted annually and conclude when the gaps identified in the existing business contingency plan have been identified.

- Conducted enterprise wide
- Operational (process) and Financial
- Recovery Time Objectives
- Industry impact analysis
- Customer impact analysis
- Supplier impact analysis
- Infrastructure analysis

- **Threat Identification:** Known historical events, predictable (weather), non-predictable/ black swan (e.g. pandemic, terrorism, etc.)
- **Threat Analysis:** Assignment of probabilities/ likelihoods based on historical and actuarial data
- Prioritization of threats taking into account potential financial, operational, and reputational impacts

- Development of stress test scenarios
- Test business readiness against various selected threat scenarios
- Revise assumptions across BIA and Risk and Threat Assessment

- Impact assumption testing and re-assessment
- Gap Analysis against existing BCP
- Update existing contingency plan

Cyber Resilience

Threats - Cybercrime, natural disasters, infrastructure or technology failures, or staff unavailability are all examples of key business threats.
Defense - In an event, infrastructure, data and operations are compromised it is imperative that defensive measures exist to sustain critical enterprise functions.
Response - Prevention roadmaps must outline risk mitigating response mechanisms for restoring disruptions to a normalized state preventing future threats.

	STRATEGY	OPERATIONS	REGULATORY
Are you Resilient?	• Is your company's Cyber Security program resilient, enough? • Are you aware of the current Cyber Threats and their impacts? • Is your organization prepared to respond to Cyber Crime incidents?	• Are all devices connected to your system secure? • Do your systems have adequate and safe backup and recovery? • Do you have data encryption standards in place? • Do your systems have business continuity planning / governance?	• Do you understand Information Security Regulations across business lines? • How do you assess Regulatory Compliance with regards to business continuity in the IT space? • Does your Cyber Security program meet Regulatory Standards?
Sia Partners Solutions:	• Organization Governance plan • Cyber Security / IT Risk assessment • Third-Party Security assessment • Vendor Selection advisory • Software Asset management • Access Rights management • Target Operating Model • Cybersecurity training & awareness	• Vulnerability Assessment & Penetration Testing • Cyber-Attack Simulation (Blue Team / Red Team) • Incident Response Preparation & Testing • Software Development • Data Classification / Loss Prevention	• Cybersecurity Regulatory Framework • NYS DFS - Part 500 Gap Analysis & Remediation • SWIFT Customer Security Program Gap Analysis Review & Remediation • Data Privacy Review & Remediation (GDPR/CCPA Compliance) • Industry Best Practices (FFIEC, COBIT, NIST, CIS)

Third Party Risk

Third Party Risk arises from a firm's dependence on outside parties to perform activities or provide services on its behalf. Third party risk is measured against the likelihood that an outside party is unable to provide the activities and/or services required to support a firm's business needs.

Common risks posed by third parties:

Operational

Operational risk is a firm's risk of business process / function failure due to a third party service outage or the unavailability of a third party's services.

Concentration

Concentration risk is the risk of a third party failure when the business has formed a dependence on such vendor for numerous functions and uses many of the vendor's services throughout the organization.

Reputational

Reputational risk includes the risk of monetary loss, legal action, and any associated press related to these events resulting from third party actions or performance.

Information Security

Information Security risk is the risk that a third party with access to confidential or internal business data misuses such data.

Compliance/Legal

Compliance and legal risk includes the firm's risk of exposure to potential legal penalties or fines if a third party does not meet certain regulatory requirements.

Data Privacy

Data Privacy risk is the risk that a third party with access to a firm's employee or customer Personally Identifiable Information (PII) misuses such data.

AML/OFAC

AML/OFAC risk is the risk that a third party has vulnerabilities of being non-compliant with BSA/AML requirements or OFAC sanctions regulations.

Financial Health

Financial Health risk is the risk that a vendor is unable to provide services due to its current financial situation.

Through unparalleled industry expertise, we deliver superior value and tangible results for our clients

14 BU working in an integrated manner across **25** offices

SECTORS

Banking
Consumer Goods & Retail
Energy, Resources & Utilities
Government
Healthcare
Insurance
Manufacturing
Pharmaceuticals
Real Estate
Tech
Telecommunications & Media
Transportation & Logistics

SERVICES

Actuarial Sciences
CFO Advisory
Change Management
CIO Advisory
Compliance
Corporate Strategy
Marketing & Customer Experience
Data Science
Digital Transformation
Human Resources
Operational Excellence
Pricing & Revenue Management
Procurement & Sourcing

Consulting 4.0, Our Innovation Ecosystem

DATA SCIENCE EXCELLENCE CENTER

EMERGING TECH LAB

RPA
IoT
Data Management
Cybersecurity
Blockchain
DevOps
Serverless PaaS
Quantum Computing
Volumetric Displays

Voice Recognition/Virtual Assistants
Taxonomy & Ontology
Augmented/Virtual Reality
Drones
Conversational User Interfaces

BIM
Autonomous Vehicles
Connected Home

STUDIO

E-commerce
AI
Startup trends

DIGITAL PLATFORM

Productivity Tools
Collaborative Tools
Design Thinking Lab
MOOCs
DataSets & DataLab
Data Science Showroom
APIs & Consulting Bots

APIFICATOR by sqapartners

DIGITAL TRANSFORMATION OFFERINGS

Digital Due Diligence
Innovative Ecosystems
Digital Trends Observatory
Digital Assessment & Strategy
Data Monetization
Transformation Hub
New ways of working
POC to industrialization

FOVE Digital marketing agency

IDEATION

Learning Expeditions
Students Contests | Hackathon
Sia Ideas
Open Source Thought Leadership

siapartners

Pioneer of Consulting 4.0

Sia Partners is a next generation consulting firm focused on delivering superior value and tangible results to its clients as they navigate the digital revolution. Our global footprint and our expertise in more than 30 sectors and services allow us to enhance our clients' businesses worldwide. We guide their projects and initiatives in strategy, business transformation, IT & digital strategy, and Data Science. As the pioneer of Consulting 4.0, we develop consulting bots and integrate AI in our solutions.

Follow us on **LinkedIn** and **Twitter @SiaPartners**

For more information, visit:

www.sia-partners.com

**Sia Partners Panama, a Sia Partners member firm*

Abu Dhabi
Amsterdam
Baltimore
Brussels
Casablanca
Charlotte
Chicago
Denver
Doha
Dubai
Frankfurt
Greater Bay Area
Hamburg
Hong Kong
Houston
London
Luxembourg
Lyon
Milan
Montreal
New York
Panama City*
Paris
Riyadh
Rome
Seattle
Singapore