sia partners

Pioneer of Consulting 4.0

Operational Resilience

Capabilities Offering

June 2020

Eric Blackman
John Gustav

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

Table of Contents

Operational Resilience 3

Business Continuity Management 6

Technology Disaster Recovery 12

Threat and Risk Assessment 20

Cyber Resilience 28

Third Party Risk Management 34

Appendix 40

- Governance Framework
- Key Regulatory Rules and Guidance
- Industry News and Hot Topics
- Glossary of Key Terms
- Selected Sia Operational Resilience Credentials

1

Operational Resilience

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.

PANDEMICS

NATURAL DISASTER

SEVERE WEATHER

EMPLOYEE VANDALISM

CYBER ATTACKS

TERRORIST ATTACKS

WORKFORCE STOPPAGES

POLITICAL UNREST

Operational Resilience: Managing Disruptive Events

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

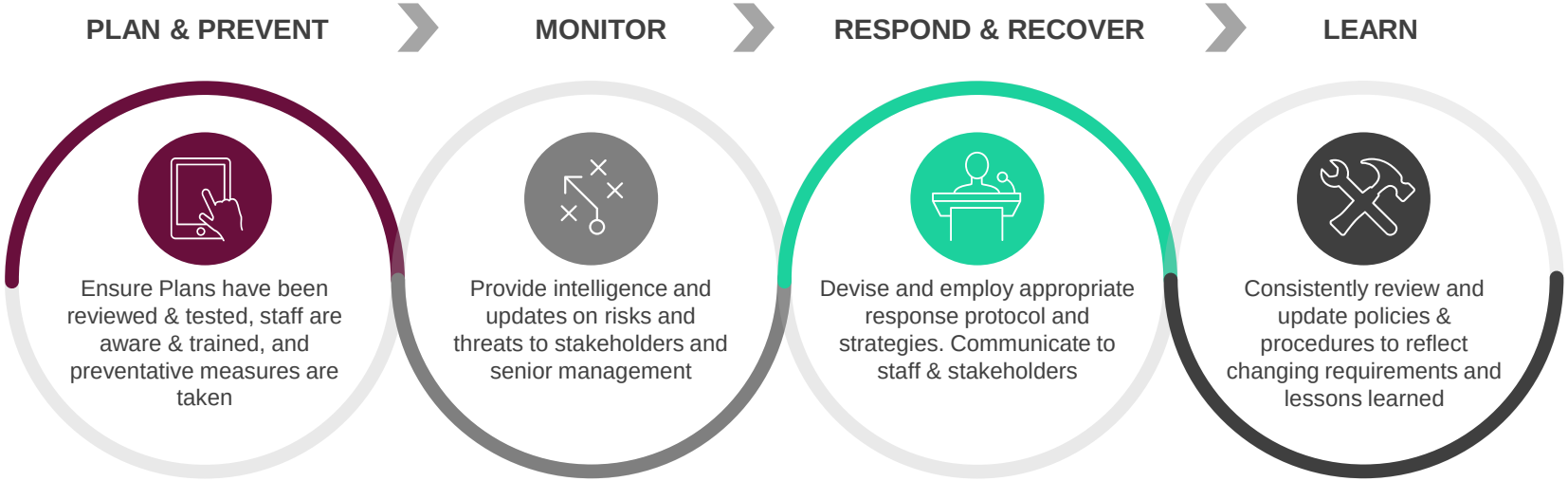
REPORTING

2

Business Continuity Management

Business Continuity Management: Overview

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)

Business Continuity Management: Key Client Concerns

ARE YOU PREPARED TO HANDLE A BUSINESS CONTINUITY EVENT?

Developing a robust Business Continuity framework pre-event that incorporates both annual business continuity plan reviews and scheduled testing is key to an effective response. Business Continuity requires Executive Buy-In, dedicated BCM staff, and up-to-date technology infrastructure (including BCM-focused applications). Prioritizing key / critical functions and performing Business Impact Analysis across your enterprise will further assist your team in understanding vulnerabilities and tolerances.

DO YOU HAVE AN APPROPRIATE CRISIS AND DISASTE MANAGEMENT RESPONSE?

Proper preparation for any business continuity event starts before an event occurs. Developing formal business continuity plans, testing of those plans, and creating effective response plans covering both business processes and technology can help mitigate the impact of any event. Crisis managers would oversee communication to employees and other stakeholders once business continuity plans are activated. Post-mortem exercises are conducted after recovery of a disaster.

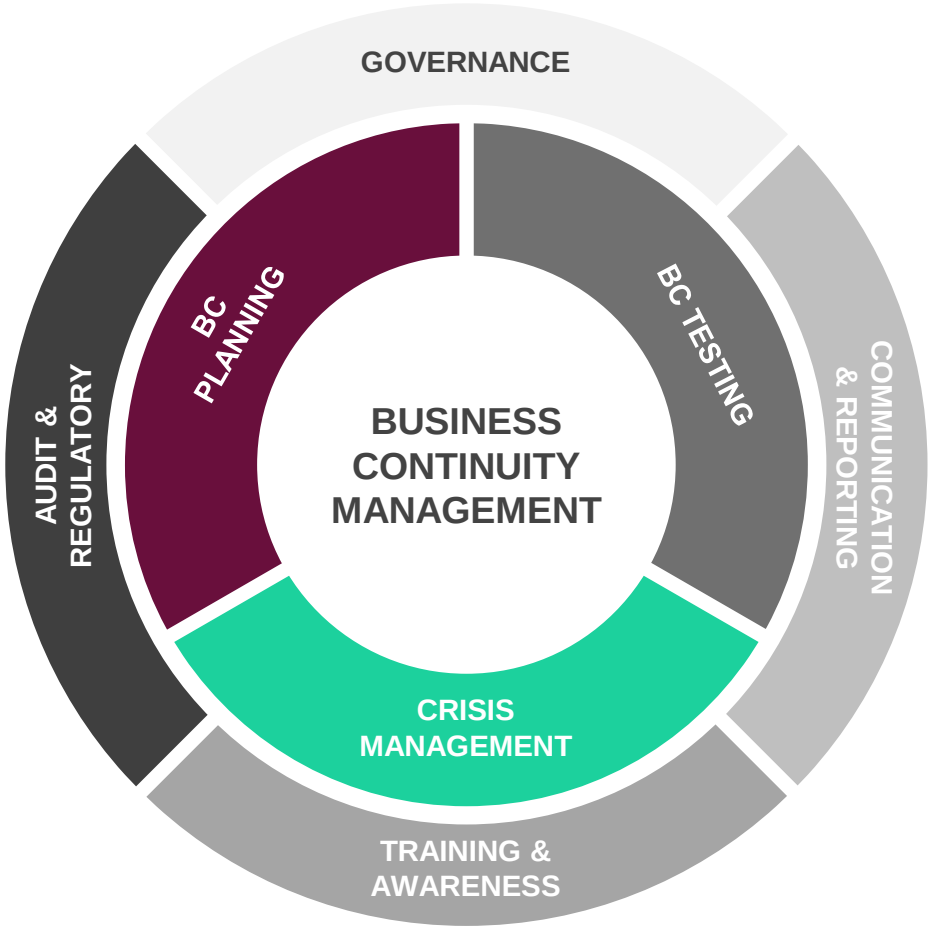
HAVE YOU ESTABLISHED A PROPER GOVERNANCE FRAMEWORK FOR BUSINESS CONTINUITY?

A formal **Governance** structure should be established to oversee your firm's business continuity effort. Senior Management buy-in will be crucial in your efforts to build a resilient organization. Bringing together the right parts of an organization (i.e. Business, Technology, Legal, Regulatory) will be instrumental in ensuring a coherent framework and will lay the groundwork for consistent and effective reporting.

HOW CAN YOU DESIGN EFFECTIVE TRAINING AND AWARENESS FOR STAFF?

Designing and implementing an effective training program for staff remains a challenge. Engagement is imperative across all levels to ensure a proactive response to a business continuity event. Simulations, table-top exercises, and plan reviews are just some of the ways to increase staff awareness in preparation for an event.

Business Continuity Management: Roles and Responsibilities



BC PLANNING

BC Planning includes the setting of BC Planning Standards, publishing procedures for the firm, providing plan standards, reviewing BC Plans,, and monitoring plan testing. To help reduce the impact of business continuity events, teams must conduct a Business Impact Analysis (“BIA”). The BCM Team develops and maintains plans and tests Recovery Strategies documented in said Plans at least annually.

BC TESTING

BC Testing is the process where designated members verify the viability of their Recovery Strategies. Specifically, BC Plan Testing involves Recovery Essential Personnel perform their designated critical business processes using Recovery Strategies documented in their BC Plans. The BC Plan Test objective is to confirm that the strategies can be deployed and provide a reasonable expectation that they will continue operation during a business continuity event.

CRISIS MANAGEMENT

Crisis Management is the process of managing the Firm’s response during a business continuity event. The BC Team will coordinate among key partners such as Technology, Corporate Security, and Corporate Services, as well as with Human Resources, Legal and Compliance, and Corporate Communications, as appropriate, to assess event impact for proper escalation within the firm, including escalation to senior management.

Business Continuity Management: Approach

Sia Partners' comprehensive approach to Business Continuity helps our clients to prepare for and recover from disruptions to an organization's people, infrastructure, and mission critical processes. Sia Partners can assist your organization with subject matter expertise in all key facets of Business Continuity, including planning, testing, training, technology, and crisis management.

Strategic Planning

- Identify key client stakeholders
- Establish deliverable timelines (interim and final)
- Establish status reporting frequency and methodology
- Develop feedback mechanism for all updates, revisions, enhancements and additions
- Create final deliverable approval/sign-off model
- Identify project team and budget

Current State Review

- Review Policies & Procedures
- Identify team roles & responsibilities
- Assess existing technology solutions
- Evaluate existing training programs
- Review governance framework
- Identify applicable regulations

Stakeholder Working Sessions

- Understand and document team functions (global and regional)
- Understand and document individual roles / responsibilities (global and regional)
- Receive system demos and assess user / system interactions
- Document technology and governance enhancements and assist in their implementation

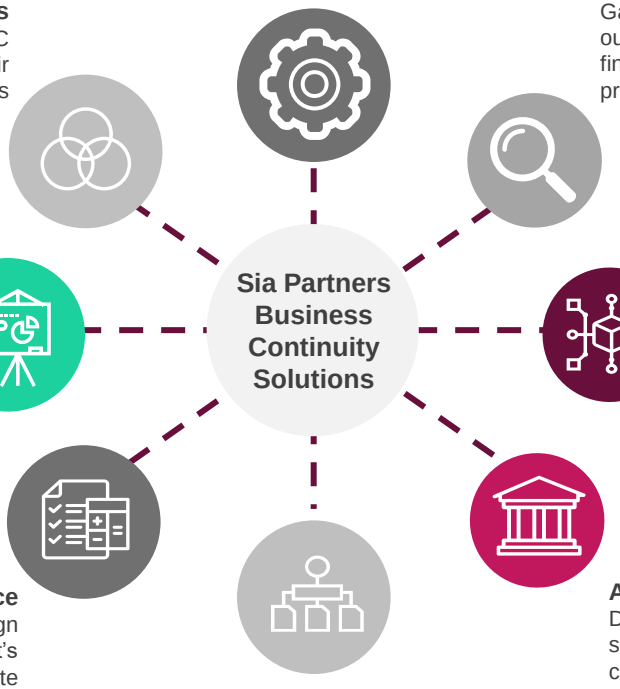
Future State Design

- Establish governance framework
- Create / Amend BC Plan Template and Structure
- Design Recovery Strategy
- Develop process taxonomy
- Establish roles & responsibilities
- Enhance Business Impact Analysis (BIA)
- Design risk assessment
- Develop analytics
- Establish testing strategy & logic
- Design incident management framework
- Implement communication strategy
- Enhance training program
- Design technology solution

Finalize & Implement

- Review Future State Design with key stakeholders
- Implement Future State Solutions
- Review and make adjustments (as needed)
- Receive client approval

Business Continuity Management: Solutions



Policies and Procedures
Assist BCM to write or enhance its policies and procedures

Ad Hoc Solutions
Optimize our client's unique BC practices based on their specific requirements

Peer Review
Gather relevant information from our clients and summarize our findings to determine best practices and industry standards

Crisis Management Framework
Create, decommission or revise the CM Framework, which includes policies / procedures and system functionality

Technology Assessment
Help our clients to enhance their current in-house system or identify the appropriate vendor solution to meet their requirements

Governance
Support the development, design and enhancement of our client's BC Governance Model to create an effective environment for management decision making

Audit and Regulatory Remediation
Design, implement and execute solutions to ensure our clients are compliant with audits and regulations

Second Line of Defense
Guide the transition of our client's BC team from a primarily tactical and administrative function to a more proactive "Second Line of Defense" Model

3

Technology Disaster Recovery

Technology Disaster Recovery: Overview

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. Technology 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. Technology 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 production 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.

Technology Disaster Recovery: Key Client Concerns

01

HOW CAN THE SCOPE OF A DISASTER RECOVERY PLAN ENSURE BUSINESS CONTINUITY?

Prioritizing key / critical functions and conducting a business impact analysis across your enterprise will further assist your team in understanding vulnerabilities and tolerances and will help to determine what recovery point and time objectives must be met for mission-critical objectives.

02

HOW CAN DATA LOSS AND NETWORK LATENCY BE PREVENTED IN THE TRANSITION TO A RECOVERY SYSTEM?

It is imperative to back up critical systems at regular intervals in order for systems to continue normal operations despite points of failure. For mission-critical operations, Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) must be clearly planned and defined to minimize down time.

03

WHAT TYPE OF DISASTER RECOVERY SOLUTION IS RIGHT FOR YOUR COMPANY?

There are a wide variety of disaster recovery systems available such as physical sites, cloud, hybrid-cloud and AI enhanced solutions. The decision should be made based upon an assessment of the desired RTOs and RPOs i.e., how much downtime and data loss is acceptable or affordable.

04

HOW OFTEN MUST A DISASTER RECOVERY PLAN BE TESTED AND UPDATED?

A disaster recovery plan should be constantly evolving and routinely updated to account for changes to your infrastructure, technology updates, and the many other factors that affect your IT environment. Testing will help to ensure there are no points of failure in your plan and that your plan will be effective and sustainable in the long term.

Technology Disaster Recovery: Roles and Responsibilities

The disaster recovery planning and response team should include representatives from departments that will be most heavily affected by system failure. These include representatives from:

Disaster Management Team / Administration

Disaster Management Team/ Administration: The management team is responsible for assessing damage and risk to business and to direct and monitor recovery efforts. Management must also allocate sufficient resources and well-trained staff to ensure the development and execution of the DRP.

Operations Team

Operations Team: The Operations Team is responsible for recovering assets like data centers and other important computer locations and providing technical support.

Network Team

Network Team: The Network Team manages all computer communications and networking protocols during a period of outage or disaster.

Facilities Management

Facilities Management: In the event that facilities have been compromised, facilities managers must help ensure building is safe and aid in any required work to build and to help coordinate a sustained recovery effort.

Human Resources

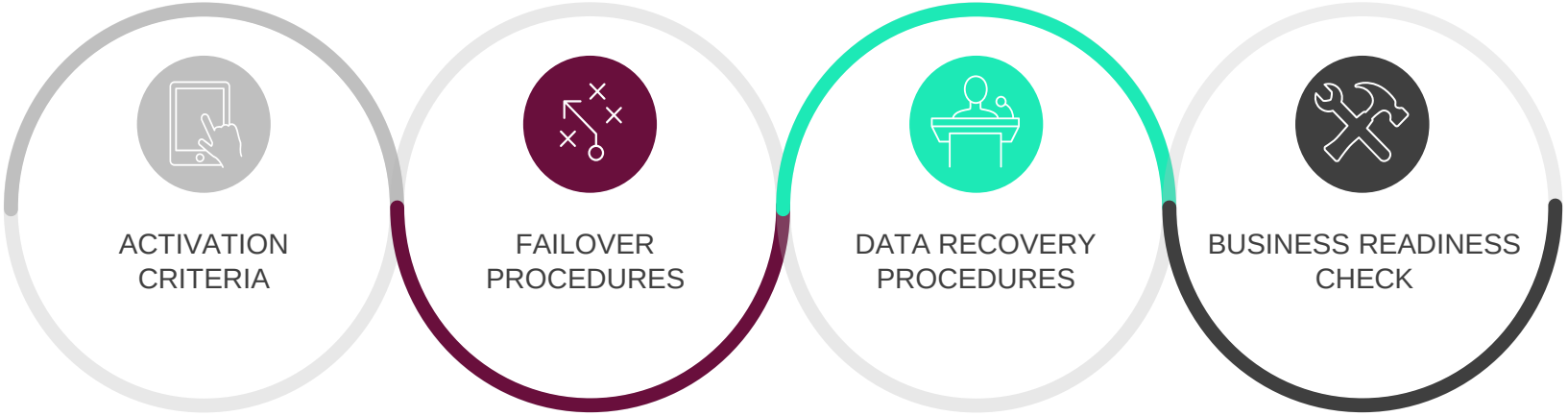
Human Resources (and/or designated Crisis Communication Coordinator): To initiate call trees or other communication procedures to general staff and contact staff necessary to fully evaluate disaster, and frame necessary internal and external communications.

Third Party Institutions

External Vendors / Third Parties: Roles of outside vendors include providing IT backup and support, and may be integral in the functioning of an institution. Third parties should also submit their own DRP for review and consideration for the event that their systems are compromised.

Technology Disaster Recovery: Plan

A disaster recovery plan (DRP) is a highly detailed step-by-step plan that takes into account a variety of scenarios with specific actions to minimize the effects of the disaster. The DRP is a comprehensive document that outlines specific policies and procedures that must be followed in order to restore essential business functions such as:



Activation Criteria is the primary input that triggers the shift to a disaster recovery system.

Failover Procedures are detailed steps that must be followed to transition to recovery sites.

Data Recovery Procedures support the backup and recovery of data in the event of an adverse event.

Business Readiness Check is procedural evaluation of readiness of a disaster recovery system for production use.

Technology Disaster Recovery: Testing

Ongoing testing of a DRP is a necessity, because the effectiveness of the plan can inevitably be impacted by changes to personnel, skill levels, and hardware and software architectures within an organization. The main objective of Disaster Recovery Test is to ensure that, in the case that a disaster does happen, the DRP will be sound. The most commonly run tests of the DRP are as follows:

Paper Test

In a paper test, members of the DR team review and annotate recovery plan documents such as DR policies, procedures, timelines, benchmarks, and checklists which are kept both as hard copies on site and digital copies in the cloud.

Walk Through Test

In a walk through test, the DR team engages in a group walk through of the DRP to identify potential issues or blind spots and any modifications that should be made to the disaster recovery environment.

Scenario Simulation

Scenario Simulation involves executing the DRP in a test environment with no disruption to the production workflow. The simulation is run according to specific recovery scenarios.

Parallel Test

In a parallel test, failover recovery systems are tested to make sure that, in case of disaster, they can perform real business transactions supporting key processes and applications. Meanwhile, primary systems continue to run the full production workload.

Cutover Test

A cutover test assesses failover recovery systems built to take over the full production workload in case of disaster. Primary systems are disconnected during the test.

Technology Disaster Recovery: Approach

The steps outlined below represent the Sia Partners approach to Tech Disaster Recovery. Following a comprehensive assessment leveraging a business impact analysis, the client's core processes and technical architecture are assessed against business and regulatory requirements. A comprehensive Disaster Recovery Plan is then developed and tested thoroughly.

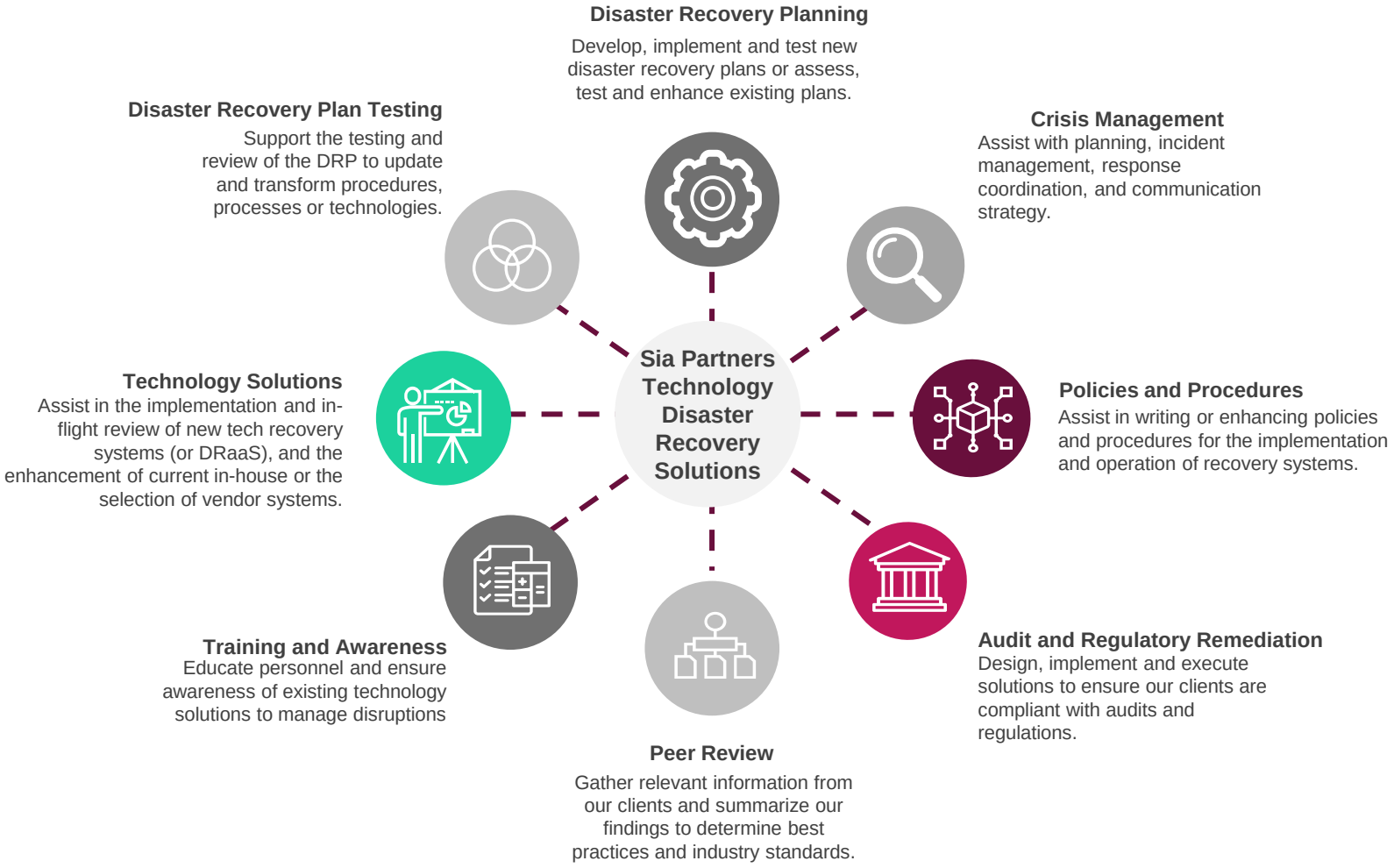
- Business Impact Analysis: assessment of the probability of forecasted and unforecast events
- Determination of what IT services and data processes support mission-critical business activities in order to develop recovery point and time objectives

- Client's Business Model & Production Landscape: Assess current core processes and technical architecture
- Regulatory and industry standards and requirements

- Development of a written plan to determine a complete response in the event of system failure
- Procedures for restoring backlogged activity or lost transactions to identify how transaction records will be brought current within expected recovery time frames

- Test recovery readiness against various selected disaster scenarios
- Revise plan based on technological development and a pass / fail logic in testing
- Develop a plan maintenance plan to monitor change management

Technology Disaster Recovery: Solutions



4

Threat and Risk Assessment

Threat and Risk Assessment: Overview

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.

Business Impact Analysis
A systematic process to determine and evaluate the potential effects of an interruption to critical business operations resulting from a disruption.

Threat Identification and Analysis
Threats are assessed on the basis of their likelihood of occurrence, and prioritized based on expected potential impact on business operations.

Stress Testing
Threat scenarios are chosen and simulated to test business readiness. Deficiencies in existing business continuity plans are identified for remediation.

During the Threat/Risk Assessment, the business is primarily concerned with answering the following three key questions:

- Have all the potentially disruptive threats to the business been considered and analyzed?
- What is the current ability of the business to continue to function if one or more of the threats materializes?
- What are the financial and operational implications of a disruption?

Threat and Risk Assessment: Approach

These four steps represent Sia's approach to 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

Threat and Risk Assessment: Roles and Responsibilities

The Roles & Responsibilities identified below are typical for each phase the Risk Assessment, although individual organizations may differ depending on the maturity of their program and unique business needs.

Assessment Team (Risk Group)

Business Impact Analysis	Risk Assessment	Stress Testing	Review and Refresh
• Lead analysis and documentation of critical business processes • Develop questionnaire for business units • Conduct interviews with key stakeholders • Assess impact of disruptions.	• Identify all potential risks • Determine likelihood • Prioritize threats based on potential impact	• Choose and develop stress test scenarios • Revise Risk Assessment assumptions	• Based on results of stress test and using the updated assumption, complete a gap analysis against existing BCP plan • Update contingency plans based on impact assumption testing and re-assessment

Assessment Team (Counterparts)

Business Units	Professional Forecaster	Business Units	BCP Team
• Assist in the identification of processes, systems, equipment, personnel, etc.	• A third party professional forecaster/statistician may be used to augment probabilistic threat analysis	• Simulate impact of threat and assess readiness based on current BCP • Revise BIA assumptions	• Develop roadmap to revising BCP plan

Threat and Risk Assessment: Business Impact Analysis

Step 1: Operational Analysis
- Process Taxonomy Questionnaire: Inventory and analysis of key functions and associated personnel, facilities, communication, systems, technology, equipment, suppliers, process dependencies etc. at the BU level
- Interviews with key personnel in each BU

Step 2: Potential Impacts: Financial and Operational
- Disruptions, downtime and associated costs (and other resultant risks)
- Recovery time objectives (RTOs), methods, and protocols
- Scoring disruptions based on financial, reputational, and operational costs

Step 3: Legal and Regulatory
- Legal and regulatory implications should also be analyzed during the business impact analysis.
- Impact on Third Party SLAs in event of disruption

BUSINESS IMPACT ANALYSIS

- Process Taxonomy: Identify and analyze mission critical processes, systems, equipment, records etc.
- Conducted enterprise wide to ensure that all business and process interconnectivity is assessed.
- Some organizations must additionally consider industry-wide impacts (interconnectivity with industry, suppliers, and customers), as well as regulatory requirements.
- The output of the BIA should include a prioritization or tiering of critical process, systems, etc.

SAMPLE BIA OUTPUT

Process	Total Dependencies	Customer Impact	Financial Impact	Resources Impact	Legal Impact	Recovery Point Objective	Recovery Time Objective	Max Allowable Downtime	Overall Priority
Fixed Income Trading	26	Extreme	High	High	Extreme	2 Hrs	4 Hrs	2 Hrs	1
Taxation	12	Medium	Medium	High	High	8 Hrs	16 Hrs	8 Hrs	2
Budgeting	4	Low	Medium	Low	Medium	24 Hrs	32 Hrs	24 Hrs	3

Threat and Risk Assessment: Threat Identification and Analysis

Threat Identification

The Risk Assessment begins by identifying and assesses sing all potentially disruptive threats to the business.

- Who/what is taken into consideration when scoping risks and prioritizing threats?
- How accurate are the estimates, and what if they're wrong?

Natural

- Extreme weather
- Climate disruptions

Environmental

- HVAC
- Security
- Conditions limiting access to facilities, equipment, systems

Man-made

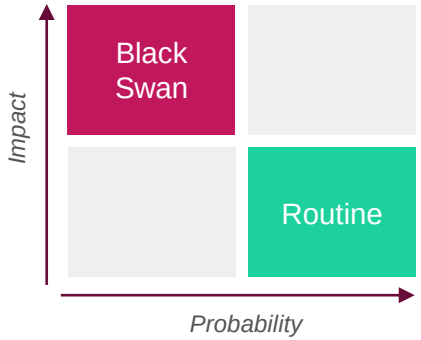
- Civil disturbance
- Terrorism
- Electrical failure
- Crime
- Key staff departures

Threat Analysis

The Threat Analysis assesses and assigns risk likelihood, and estimates impact.

- Threat Model
- Financial and Operational Impacts

Threat Analysis Matrix



Particular emphasis should be given to low probability, high impact events (catastrophic), and highly probably, low impact events (predictable).

Threat and Risk Assessment: Stress Testing

"[T]he most difficult threats to address are those that have a high impact on the institution but a low probability of occurrence. Using a risk assessment, BCPs may be more flexible and adaptable to specific types of disruptions that may not be initially considered."
- FFIEC Handbook

Threat Scenario Estimated Cost Analysis

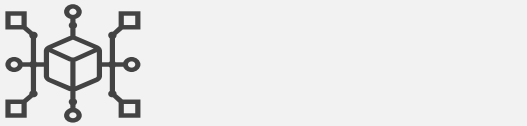
Threat	Likelihood	Impact	Cost Estimate	Priority
Power Outage	High	Low	$	1
Pandemic	Low	High	$$$$$	1
Hurricane	Moderate	Moderate	$$$	2

Threat and Risk Assessment: Solutions

Sia Partners offers a comprehensive set of solutions to ensure that the Risk Assessment is thorough and in line with best practices and the highest industry standards.

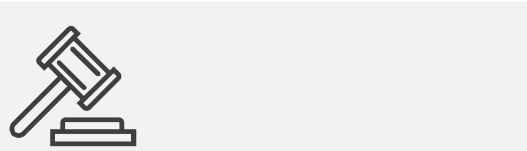
Design a Business Impact Analysis

- Process Taxonomy: Questionnaire and Inventory
- Impact Assessment: Potential impact of disruptions operationally and financially
- Metrics: RTOs, RPOs, and MAD



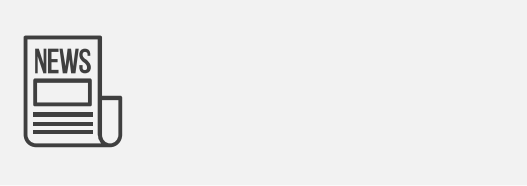
Regulatory and legal requirement and impact analysis

- Identification of key regulator and legislation pertinent to industry
- Alignment of risk/threat assessment and BIAs to applicable regulations and laws



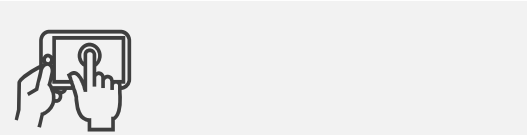
Comparison and Benchmarking against:

- Relevant peers
- Best practices
- Open source intelligence (OSINT)
- Industry trends



Vendor Selection

- Identify and vet software vendors to assist in the identification and assessment of risks/threats (RFPs)
- Facilitate the implementation of vendor solution and ensure proper capture of BIA and risks



Cyber Resilience

Cyber Resilience: Overview

Cybersecurity is the practices associated with protecting systems, networks, and programs from digital attacks and/or damage. In a corporate context, cyber-attacks aim to access, remove, alter, and/or destroy sensitive information; this may include extorting money from users and/or interrupting normal business processes. Implementing effective cybersecurity measures can be challenging because there are more devices and users than ever creating a wider surface area to be exploited by potential attackers. Furthermore, as attackers are becoming more innovative, an ever increasing number of people are working remotely with sensitive and/or confidential customer and firm data.

ACCESS AND PERMISSION
What must be scoped, planned, and managed to ensure users and customers have appropriate levels of access?

GOVERNANCE
How can a business ensure that its Cybersecurity Program(s) and/or functions are reasonably governed, controlled, and overseen? How are Cybersecurity roles and responsibilities defined?

DATA PROTECTION AND PRIVACY
How do you protect private and/or proprietary data? What are the overarching legal requirements and obligations an entity has in protecting its data and/or the privacy of customers?

UPGRADE AND PATCH MANAGEMENT
How often do critical network security systems and infrastructure get tested, maintained and upgraded? How are these changes documented and managed?

NETWORK SECURITY
How can network security between internal, external, and third party networks be ensured? How are breaches of network security managed?

DATA RECOVERY AND REDUNDANCY
To what extent do network security efforts ensure data is backed-up and/or recoverable in the event of a Cybersecurity incident?

Cyber Resilience: Key Client Concerns

Most entities use passive Cybersecurity measures to protect their information often utilizing security infrastructure such as firewalls. While passive security measures are a vital starting point, there is often a need to augment passive measures with an active cybersecurity approach such as the deployment of Cybersecurity analysts and Red Team exercises. Balancing both active and passive measures can be a key to meaningful Cybersecurity.

1 DEFENSE
(Ongoing Passive Measures)

- Network Security: Is your network secure enough to protect you from an attack?
- Encryption: Is your external communication encrypted?
- User Awareness: Are your employees trained for cyber-attacks?
- Patching: Do you have adequate processes in place for software upgrade and patch management?
- Data Redundancy: Do you have solid processes in place for data back-up? are your back-ups safe?
- Cloud Security: Is your data protected on the Cloud?
- Access Management: Is there a strong Identity and Access Management process in place?
- Oversight and Standards: Do you conduct regular audits for third-parties? Do they follow the same cybersecurity standards as your company?

2 RESPONSE
(Reacting to Cyber Incidents)

- Operational Resilience: Are you cyber resilient?
- Secure Response: How do you securely respond to an incident?
- Insurance: Do you have a cyber insurance in place?
- Incident Detection: Are you able to properly identify an incident?
- SOPs: What are your Standard Operating Procedures for containing and eradicating an incident?
- Reporting: Is there a clear reporting procedure for cyber-attacks and other incidents to coordinate with law enforcement and third-parties?
- Recovery: Do you have a process for recovering and restoring your applications into operations?

Sia Partners implemented innovative solutions to support our clients' defense and response frameworks and ultimately support their organization in addressing any types of disruptions that have an impact on systems and data, not only from cyber-attacks.

Cyber Resilience: Roles and Responsibilities

1 DEFENSE *(in BAU)*

Governance

Define a strong governance frameworks, including the roles of the Board of Directors and Chief Information Security Officer.

Risk Assessment

Conduct effective identification, analysis, evaluation and management of cybersecurity risks and review, test and enhance Security Controls.

Threat Analysis

Assess threats and vulnerabilities through penetration testing and vulnerability assessments such as staff awareness, third-party risk, access controls on remote access, and cloud-hosted systems..

Third Parties

Ensure that third party entities have robust controls in place with respect to internal Cybersecurity practices. Conduct due diligence prior to their onboarding and regular Third-Party audits and risk assessments.

2 RESPONSE *(in the context of an attack)*

Incident Response

Review and test the preparedness of the company to a cyber-attack (incident response plan/procedure).

Training

Continuously train staff and develop cultural awareness to manage and address risks.

Table Top

Conduct regular simulation tests (Table Top / Hybrid exercises) to assess how your teams interact in the context of an attack. Ensure your organization is ready to identify, protect, detect, respond and recover from various attack scenarios.

Red/Blue Teams

Run effective simulation of cyber-attacks with Red Teams that are external entities brought in to test the effectiveness of a security program; the Blue Team is the internal security team that is charged with stopping these simulated attacks.

Cyber Resilience: Approach

Our Objective is to assess the Cybersecurity Maturity of your organization and achieve a target state in compliance with cybersecurity regulations and guidelines relevant to your organization. Our solution is tailored to your needs, readiness and organization culture. Sia Partners services also include the selection of vendors which help to mitigate cyber risks.

Assessment

Implementation

Project Governance, Socialization and Scoping

- Kick Off Meeting / Determine Scope and Set Objectives
- Regulatory Context Assessment
- AGILE Transformation
- Rapid Assessment and TOM Design
- List Policies and Procedures
- Documentation Needs
- Survey and Initial Assessment of Vendors

Current State and Gap Analysis

- Apply the “Sia Partners Operational Resiliency Framework”*
- Design the Risk Control Matrix (‘RCM’)
- Analyze Current Infrastructure
- Interview key stakeholders
- Review Policy and Procedures
- Review Contract Agreements and SLAs
- Identify Cyber Risks
- Perform an IT / IS Risk Assessment, including a Vendor Risk Assessment
- Complete a Gap Analysis against the recent regulations and best practices

Findings and Recommendations

- Define Mitigating Controls
- Select and Test Security Controls
- Present Gaps and Mitigation Actions (Risk Heat Map)
- Discuss with Management the Gaps to be accepted (Risk Acceptance)
- Obtain Final Approval for the Remediation Plan
- Propose Software Development or Third-Parties to help mitigate the risks

Remediation Plan and Roadmap

- Build the Remediation Plan and Implementation Roadmap
- Obtain Sign-off from Management
- Define KPIs
- Define Reporting and Escalation Mechanisms
- Select Vendors and Initiate RFP Process for the selected solutions (Penetration Testing, Software Patching, IAM…)
- Prepare Communication Plan

Desired Cybersecurity End-State (Go-Live)

- Implement the Remediation Plan
- Test the Remediation Plan
- Deploy new Software and Test Security Controls
- Communicate to Staff and Provide Ongoing Trainings
- Prepare BAU Handoff
- Conduct Additional Exercise to Assess the Cyber Resilience (Red Team / Blue Team)
- Follow Progress (RAID Log)

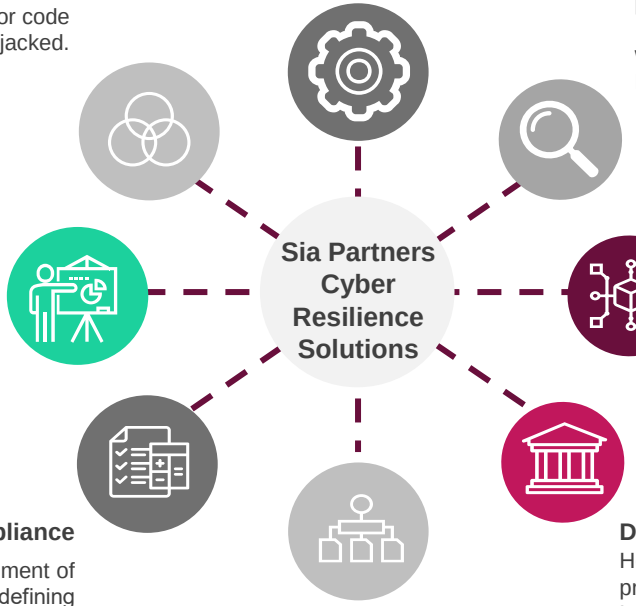
Cyber Resilience: Solutions

Sia Partners can help you improve your firm's Cybersecurity program and select vendors to help you mitigate cyber risks with regards to the following solutions:

Policies and Procedures
Assist Information Security stakeholders to write or enhance policies and procedures including performing gap analysis and updating Cybersecurity concerns in the master BCP.

Web and Application Security
Implement security measures for websites, web applications and web services as well as at the application level that aim to prevent data or code within the application from being stolen or hijacked.

Cybersecurity Awareness & Training
Gather relevant information from our clients and summarize our findings to determine best practices and industry standards – deploy local IT trainings and raise employees' awareness with regards to Phishing, Spoofing, and Social Engineering.



Incident Response Framework
Define and implement best practices in responding to Cybersecurity incidents. Define an incident response plan to help IT staff detect, respond to, and recover from network security incidents and address issues like cybercrime, data loss, and service outages that threaten daily work.

Network Security Assessment
Help our clients to enhance their current in-house network security infrastructure or identify the appropriate vendor solutions to meet your Cybersecurity challenges regarding Advanced Threat Prevention, Network Access Control, DDoS Protection, Domain Name Security and Firewalls.

Governance, Risk & Regulatory Compliance
Support the development, design and enhancement of our client's Cybersecurity programs including defining roles and responsibilities, policy and procedural support, and compliance with the current regulations (such as State and Data Privacy regulations) and industry best practices (FFIEC, COBIT, NIST…).

Data Protection & Cloud Security
Help our clients in implementing protective digital privacy measures (such as Data Encryption, Data Loss Prevention and Data Privacy measures) and Cloud Security controls (using trusted software, managing assets lifecycles, considering portability or continuous monitoring).

Vulnerability Assessment & Penetration Testing
Help define, scope and guide of our client's red teams and or external penetration testers in order to identify Cybersecurity vulnerabilities and deficiencies to be patched and/or repaired.

6

Third Party Risk Management

Third Party Risk Management: Overview

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 / 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.

Third Party Risk Management: Key Client Concerns

01

DO YOU HAVE AN ADEQUATE TPRM PROGRAM IN PLACE?

Develop a robust TPRM program that allows the firm to effectively analyze the risks of engaging with a Third Party. This program should enable staff to effectively record and track risk scores of new and legacy services. It is also important to ensure that the program has written procedures governing the program and that these procedures are successfully being operationalized.

02

DO YOU HAVE SMES THAT CAN EFFECTIVELY ASSESS SPECIFIC THIRD PARTY RISKS?

In order to properly assess the various risks involved in onboarding a third party, **engage with subject matter experts** and ensure their participation in the TPRM program. TPRM must be supported by SMEs spanning multiple disciplines in order to effectively address all types of third party risk.

03

HOW CAN YOU INCREASE TRAINING AND AWARENESS FOR STAFF?

Contract Owners and Subject Matter Experts serve essential roles within a TPRM program, however, third party risk is not their main function within a bank. Therefore, firms must ensure that these teams have a clear understanding of their roles and responsibilities within a TPRM program to effectively participate.

Third Party Risk Management: Roles and Responsibilities

Roles and responsibilities within a third party risk management (TPRM) program can be described using the three Lines of Defense (LOD) model, shown below. Sia Partners offers solutions for teams within both 1st LOD and 2nd LOD.

Third Party Risk Management: Approach

Define Scope and Objective

- Remediation of Third Party Risk Management Program
  - Third party risk reviews
  - Enhancements to current TPRM program and processes

Current State Review

- Determine the following with TPRM Management and ORO Management:
  - Define process for completing the end to end third party reviews
  - Frequency and method for status reporting on progress of reviews
  - Estimated timeline for completion of respective milestones / deliverables to stakeholders
  - Areas for enhancements within the current TPRM program and processes

Develop Plan and Roadmap

- Identify key personnel and resources necessary for completing risk reviews of third parties
- Identify business lines / departments who could play a role in the third party risk management review process
- Determine target milestones (e.g. complete all reviews of high risk vendors by a date)

Execute and Develop Deliverables

- Oversee the completion of risk assessments to evaluate the inherent risks associated with the goods and/or services provided by the third party at an arrangement
- Oversee the completion of control assessments to assess the residual risk associated with the third party
- In overseeing the remediation program, identify process improvements and enhance policies and procedures

Monitor and Control Project

- Document current state trackers and report against targeted deadlines to stakeholders

Finalize

- Reach “Closed” status for all remediation reviews with an enhanced process on how to handle all BAU reviews going forward

Third Party Risk Management: Solutions

Sia Partners can help improve your firm's Third Party Risk Management program and/or processes in the following ways:

Data Management

- Design and implement a database to track third party services used by an organization and ensure data integrity among the dataset
- Maintain records of third party vendors used by a business for reporting and tracking purposes
- Provide visualized reporting and dashboard solutions on a regularly scheduled basis

Policies & Procedures

- Define and document current state processes
- Conduct a gap analysis on current processes and identify solutions to resolve gaps
- Facilitate change management process to implement enhanced procedures

Contract Management (SLAs)

- Service Level Agreements (SLAs) are important because they set boundaries and expectations between the businesses and vendors. Our SMEs can assist to:
  - Design a process for SLA review
  - Provide an analysis on high and critical risk vendors that require SLAs

Third Party Risk Framework

- Perform evaluation of the risks associated with the goods and/or services provided by the third party
- Assess the onboarding of new vendors process
- Provide project management solution to help the firm implement a robust TPRM program

Third Party Performance Monitoring

- Risks posed by third parties are not static, and require ongoing evaluation. Our SMEs can assist in the ongoing evaluation of third parties to:
  - Ensure they are meeting contractual and regulatory requirements
  - Confirm risks are appropriately managed

7

Appendix

Operational Resilience: Governance Framework

The table below reflects an approach to governance of Operational Resilience teams that will suit many firms. Communication flows from bottom-up and top-down. Depending on the size and needs of an organization, specific governance models will vary. Sia Partners can help to design the right structure for your organization's needs.

Key Stakeholders	Roles & Responsibilities
EXECUTIVE STEERING COMMITTEE	▪ Creates and maintains an organization's Operational Resilience Mandate ▪ Allocates Program Funding ▪ Outlines the organization's mission critical functions ▪ Validates the program's strategy, output, and timelines ▪ Visibly supports the mission across the organization
ENTERPRISE RISK COMMITTEE	▪ Provides strategic guidance across divisions ▪ Communicates program compliance to the executive team ▪ Evaluates and approves recommendations made by the Operational Resilience Governance Committee ▪ Designs program pillars for successful delivery
OPERATIONAL RESILIENCE GOVERNANCE COMMITTEE	▪ Provides strategic direction across the Operational Resilience Teams ▪ Develops proactive ownership to track and enable delivery ▪ Consolidates reporting and raises issues to the Enterprise Risk Committee ▪ Optimizes allocation of resources ▪ Creates workstreams and monitors the progress of the Ops Resilience Teams
OPERATIONAL RESILIENCE TEAMS	▪ Acts as the primary focus for delivery of the Operational Resilience program ▪ Involves key stakeholders across groups and divisions ▪ Takes ownership of Operational Resilience Plans, Testing & Crisis Response ▪ Implements globally consistent standards ▪ Tracks and reports metrics, analytics, and issues to the Governance Committee

Key Regulatory Rules & Guidance (1/2)

Regulator	Applicable Rule / Guidance
FFIEC (FRB, FDIC, NCUA, OCC, CFPB)	Business Continuity Management IT Handbook
CFTC	Final Rule part 23, Subpart J - Duties of Swap Dealers and Major Swap Participants - 23 603 Business Continuity and Disaster Recovery
CME	Rule 983 - Disaster Recovery and Business Continuity
NFA	9052 - NFA COMPLIANCE RULE 2-38: BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN
NFA	RULE 2-38. BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN.
ISO	ISO/IEC 24762:2008:Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services
FINRA	Regulatory Notice 18-09:FINRA Updates Designation Criteria to Require Firms Reporting U.S. Treasury Securities to TRACE to Participate in FINRA's Business Continuity/Disaster Recovery Testing
FINRA	Regulatory Notice 15-43:FINRA Files Rule with SEC for Authority to Designate Firms for Mandatory Participation in FINRA's Business Continuity/Disaster Recovery Testing, As Required by Regulation SCI
SEC	Rule 1001(a)(2)(v) of SEC Regulation SCI
FEMA	Disaster Recovery Reform Act of 2018
BASEL	BASEL II, BASEL Committee on Banking Supervision 2003:Requires that banks put in place BC?DR plans to

Key Regulatory Rules & Guidance (2/2)

Regulator	Applicable Rule / Guidance
Specific to Third Party Risk Management	
FFIEC	Outsourcing Technology Services IT Examination Handbook
FINRA	Regulatory Notice 05-48: Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers
FRB	SR 13-19 Guidance on Managing Outsourcing Risk
OCC	Third Party Relationships: Risk Management Guidance
FDIC	Financial Institution Letters: Guidance for Managing Third-Party Risk
NY DFS	23 NYCRR 500: Section 500.11 Third Party Service Provider Security Policy
Specific to Cyber Resilience	
National Institute of Standards and Technology	NIST 4.1
Center for Internet Security	CIS 7.1
NYSDFS	NYSDFS Part 500
SWIFT Customer Security Program	SWIFT (Quasi Regulatory)
COBIT 5.1	ISACA (Information Systems Audit and Control Association)
GDPR (General Data Protection Requirement)	European Parliament & Country Regulators
Payment Services Directive II – EU	European Central Bank
California State Statute	California Consumer Privacy Act - CCPA
Payment Services Directive II – EU	FTC

Industry News and Hot Topics

Organizations are vulnerable to a variety of threats, from impacts to their people and physical property, to disruptions that affect operations, essential functions, and supply chains. Top threats to operational resilience include unplanned IT outages, cyberattacks, adverse weather, and health & safety incidents. Although it is impossible to predict the next incident, businesses should closely follow trends to identify areas of vulnerability, and fortify accordingly.

	Highlighted Event Details
Disruptive Events	**COVID-19:** Pandemic has interrupted global supply chains, travel, and forced half the world into conditions of shutdown, shuttering businesses and requiring billions to work remotely.
	California Wildfires: Widespread fires across the state displaced thousands and bankrupted the power utility PG&E.
	Iranian aggression in Strait of Hormuz: Iranian warships regularly threaten commercial vessels, including oil tanks, disrupting supply chains in this strategically vital part of the world.
Industry Hot Topics	**Migration to Cloud:** Hybrid cloud models and AI are currently the two dominant forces driving digital transformation. Projections are that companies must "become AI companies" in order to remain competitive.
	Zoom's problems: Security breaches in online meeting platform have resulted in meeting being 'hi-jacked' by third parties.
	Working from Home: With COVID-19 causing lockdown internationally, a historic number of people are working remotely. This has introduced another layer of security requirements for firms already grappling with complex cyber security threats.
	AI: AI is being utilized to automate how enterprises self-detect, diagnose, and respond to anomalies in real time.

Glossary of Key Terms (1/5)

Term	Definition
BC Event	An interruption with potential impact to normal business activity of the Firm's Personnel, operations, technology, suppliers, and/or facilities.
BC Threat Assessments	Exercise undertaken by BUs in partnership with BCM to determine threats and vulnerabilities to BUs' Critical Business Processes and locations and the impacts that could arise
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.
Business Continuity Management ("BCM")	A Firm-wide risk and control organization dedicated to providing guidance on industry standards and best practices for Business Continuity Recovery Strategies and solutions across the Firm, as required.
Business Continuity Planning	Preparation for the recovery, resumption, and maintenance of Critical Business Processes and for returning to normal business operations following a BC Event.
Business Impact Analysis ("BIA")	The process of identifying and assessing the potential impact of non-specific threats that may significantly disrupt the business operations of the Firm.
Contingency Plan	A written and BU-focused operational response and recovery plan to maintain or resume business in the event that a supplier's services are no longer available to the Firm.
Crisis Management	The process of managing a Firm's operations in response to a BC Event that threatens Business Continuity. Crisis Management focuses on leadership and delegation, communication, and people accountability responsibilities. This includes determining who communicates what to whom, and who is responsible for approving those communications.
Critical Business Processes	Firm business activities and functions that, if interrupted due to a BC Event, must be prioritized (tiered) for restoration to protect the Firm's assets, meet essential and time-sensitive organizational needs, and/or satisfy regulations.
Disaster Recovery as a Service (DRaaS)	Disaster recovery as a service (DRaaS) is a cloud computing and backup service model that uses cloud resources to protect applications and data from disruption caused by disaster. It gives an organization a total system backup that allows for business continuity in the event of system failure.

Glossary of Key Terms (2/5)

Term	Definition
Extended Outage	A BC Event, the impact of which lasts more than five days, potentially up to several months.
Impact Tolerance	The maximum tolerable level of disruption to an important business service, including the maximum tolerable duration of a disruption
Interdependency	The reliance of two or more BUs, processes, functions, or third-party providers on each other in the execution of a business process.
Maximum Allowable Downtime ("MAD")	The total time for Critical Business Processes and the acceptable losses before a BU must have the process restored.
Pandemic	An infectious disease outbreak that can have a significant impact on Firm operations.
Personally Identifiable Information (PII)	any information that could potentially be used to identify a specific person.
Recovery Point Objectives (RPO)	The age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure.
Recovery Strategies	Options documented in a BC Plan for the Firm or a BU to respond to a crisis depending on its anticipated severity and duration.
Recovery Time Objective (RTO)	The targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity
Relocation	Type of Recovery Strategy that enables the physical movement of impacted Personnel to resume business operations in alternate, non-impacted locations.
Scenario testing	Is the testing of a firm's ability to remain within its impact tolerance for each of its important business services in the event of a severe (or in the case of FMIs, extreme) but plausible disruption of its operations. In carrying out the scenario testing, a firm must identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile, and consider the risks to delivery of the firm or FMI's important business services in those circumstances

Glossary of Key Terms (3/5)

Term	Definition
Service Level Agreement (SLA)	A contract between a service provider and a client that establishes and describes the deliverables to be provided to the client.
Third Party Risk Management (TPRM)	The process of assessing, managing, and controlling risks that are associated with outsourcing certain business functions to third parties.
Transference	Type of Recovery Strategy that moves a business process from an impacted area to an alternate, non-impacted area staffed with Personnel that the BU has trained and provisioned to conduct that process.

Glossary of Key Terms: Specific to Cyber Resilience (4/5)

Term	Definition
Cross-site scripting (XSS) attack	It is a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.
Cyber Alert Metrics	A notification that a specific attack has been detected or directed at an organization's information systems is a 'cyber security alert' - counting the frequency and typologies of alerts is a critical aspect of cybersecurity metrics. If alert metrics are robust they can allow an organization to more readily identify breaches and/or other compromises of their IT environment.
Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks	It is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic
Drive-by download attack	In a drive-by download attack, criminals compromise a website, often a legitimate one, by embedding or injecting malicious objects inside the web pages.
Eavesdropping attack	Also called a sniffing or snooping attack, it is a theft of information as it is transmitted over a network by a computer, smartphone, or another connected device. The attack takes advantage of unsecured network communications to access data as it is being sent or received by its user.
Malware attack	When cybercriminals create malicious software that's installed on someone else's device without their knowledge to gain access to personal information or to damage the device, usually for financial gain. Different types of malware include viruses, spyware, ransomware, and Trojan horses.
Man-in-the-middle (MitM) attack	It is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other - for example, an attacker within reception range of an unencrypted Wi-Fi access point could insert themselves as a man-in-the-middle.
Password attack	Password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system. A common approach (brute-force attack) is to repeatedly try guesses for the password and to check them against an available cryptographic hash of the password.

Glossary of Key Terms: Specific to Cyber Resilience (5/5)

Term	Definition
Penetration Testing	Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit by simulating a perspective cyber-attacker's methodology and/or techniques as possible.
Phishing and spear phishing attacks	There are very common forms of email attack designed to you into performing a specific action—typically clicking on a malicious link or attachment, and are carefully designed to get a single recipient to respond.
Red Team / Blue Team	Red teams are offensive security professionals who are experts in attacking systems and breaking into defenses. Blue teams are defensive security professionals responsible for maintaining internal network defenses against all cyber-attacks and threats.
Social Engineering	Social Engineering in the context of information security is the psychological manipulation of people into performing actions or divulging confidential information.
Spoofing Attack	A situation in which a person or program successfully masquerades as another by falsifying data, to gain an illegitimate access or permission. This may include websites and apps which are faked or 'spoofed' which collect credentials from unsuspecting users.
SQL injection attack	It is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.
Tabletop / Hybrid Exercise	A security incident preparedness activity, taking participants through the process of dealing with a simulated incident scenario and providing hands-on training for participants that can then highlight flaws in incident response planning.
Windows of Vulnerability (WoV)	The time from when a software exploit first becomes active to the time when the number of vulnerable systems shrinks to insignificance is known as the Window of Vulnerability (WoV). The time-line for each software vulnerability is defined by the following main events:
Zero Day	A zero-day vulnerability is a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw. Said flaw has the potential to be exploited by cybercriminals and hackers can write code to target a specific security weakness.

Select Operational Resilience Credentials (1/3)

Client	Selected Projects
Global Contract Development and Manufacturing Organization	**Business Continuity assessment to support COVID-19 response** ▪ Provided detailed analysis of COVID-19 related activities with identification of gaps compared to best practices in BC domain. The client is now able to address gaps in order to mitigate risks. ▪ Provided risk and issue management tools to increase efficiency and quality in their crisis response processes.
Tier 1 Global Investment Bank	**Business Continuity and Crisis Management Vendor Technology Assessment** ▪ Documented the global Business Continuity Management (BCM) team's business requirements and enhancement requests, and conducted both a high level and deep-dive analysis of the Business Continuity (BC) and Crisis Management (CM) solutions in the marketplace that best fit client's requirements and requests ▪ Completed a high-level BC & CM peer review (Organizational Alignment and System Usage) and performed a high-level review of the client's existing technology solution ▪ Delivered a vendor selection and a go-forward recommendation book based on various factors - such as culture, estimated pricing and implementation timelines, technical concerns, etc.
Tier 1 Global Investment Bank	**Business Continuity Management Policies and Procedures** ▪ Worked with senior members of the Business Continuity Management (BCM) team to develop a plan that summarizes the project scope, key business areas, critical functions, and primary stakeholders ▪ Determined the preferred policy and procedure structure preferred by BCM ▪ Interviewed key personnel ▪ Wrote Business Continuity Planning and Crisis Management policy and procedure documents that clarify BCM roles and responsibilities and communicate BCM's role as the second line of defense ▪ Helped BCM to obtain formal approval of the BCM policy and procedure documents ▪ Assisted with the preparation of a training plan and supported the training for new roles and responsibilities

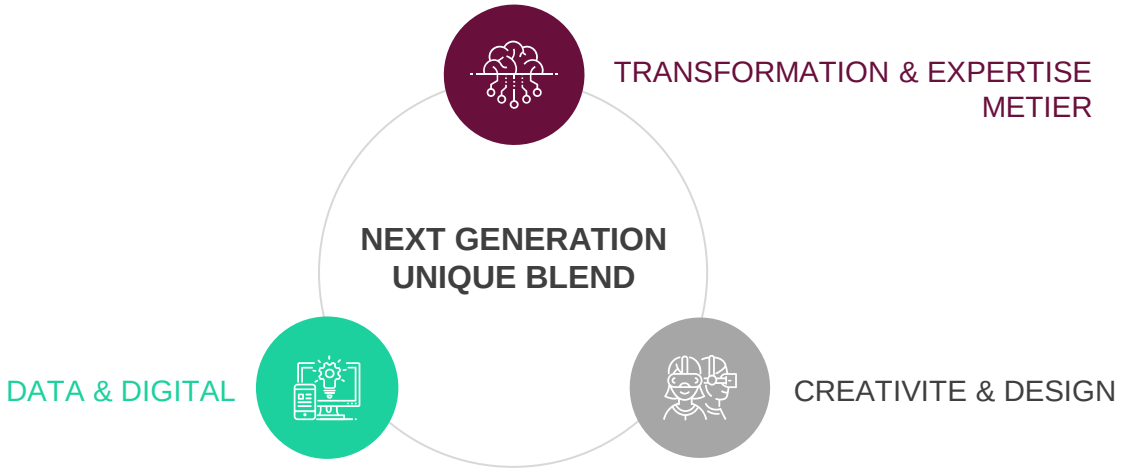
Select Operational Resilience Credentials (2/3)

Client	Selected Projects
French Global Investment Bank	**IT Risk Assessment – FFIEC Management Booklet Examination Procedures Review** • Reviewed the existing IT Risk Assessment program based on the FFIEC Management Handbook guidelines • Conducted an IT Risk assessment inventory including interview with stakeholders • Provided recommendations (if applicable) identification of any potential gaps • Participated and reviewed the bank's own RCSA (Risk Control Self Assessments) for ITEC • Provided recommendations on potential risks identified
French Global Bank	**Information Technology, New York, NY – Information Security Incident Response** • Developed a table-top incident response exercise to evaluate the bank's literacy and awareness about appropriate incident responses, including a complex incident scenario and multiple scenarios tailored to the Bank. • Scheduled and facilitated the formal Information Security incident tabletop exercise involving key members of the IS and IT departments • Delivered an assessment of the bank's response and recommendations on enhancements for the bank's Policy and processes, and a flow chart that references relevant areas of the bank's Information Security Incident Response Policy and Procedures to make use of the document more efficiently during an actual incident.
Indian Global Bank	**Perform simulated cyber-attack scenarios and evaluate the effectiveness of the Bank's incident response plan** • Designed simulated cyber-attack scenarios with supporting evidence that is commonly seen in the industry • Presented the simulated scenarios with the bank's Incident Response Team and observed their responses and actions • Performed a debrief with the client team after the completion of simulated testing and made recommendations • Documented the analysis in a final report

Select Operational Resilience Credentials (3/3)

Client	Selected Projects
French Global Bank	**Perform branch wide IT Risk Assessment for critical applications in NYC** • Assessed Business Continuity Plans for critical applications • Updated Technology Policies and Procedures to meet FFIEC requirements • Remediated Internal Audit issues and provided evidence of the remediation to Internal Audit • Created a Quantitative Threat & Vulnerability Matrix • Streamlined and automated Information Security Officer tasks
German Global Investment Bank	**Gap Analysis, Policy Review and Policy Framework Creation** • Performed a gap analysis of Reg SCI readiness • Partnered with external vendors to ensure appropriate controls were in place • Drafted the full compliment of related policies and procedures to meet SEC Regulation Systems Compliance Integrity ("SCI") requirements • Worked with the client's Business, Legal, Operations and IT departments to identify and educate impacted parties across diverse business units
German Global Investment Bank	**Alternative Trading Systems (ATS) Regulatory/ Compliance - Reg SCI Annual Assessment** • Developed a quantitative model and methodology for evaluating SCI System compliance • Worked with the client's Business, Legal, Operations and IT departments to Identify shortfalls in their business process, controls, and reporting • Analyzed internal and third-party systems policies, corporate policies, internal risk assessments, control procedures

Sia Partners is a next generation consulting firm and a pioneer of Consulting 4.0



25 offices in **16 countries**

$280M Revenue for FY19/20

CAGR of **22% over the last** 3 years

35 bots **3** AI centers

1,400 Consultants

500 clients **92%** returning clients

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

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

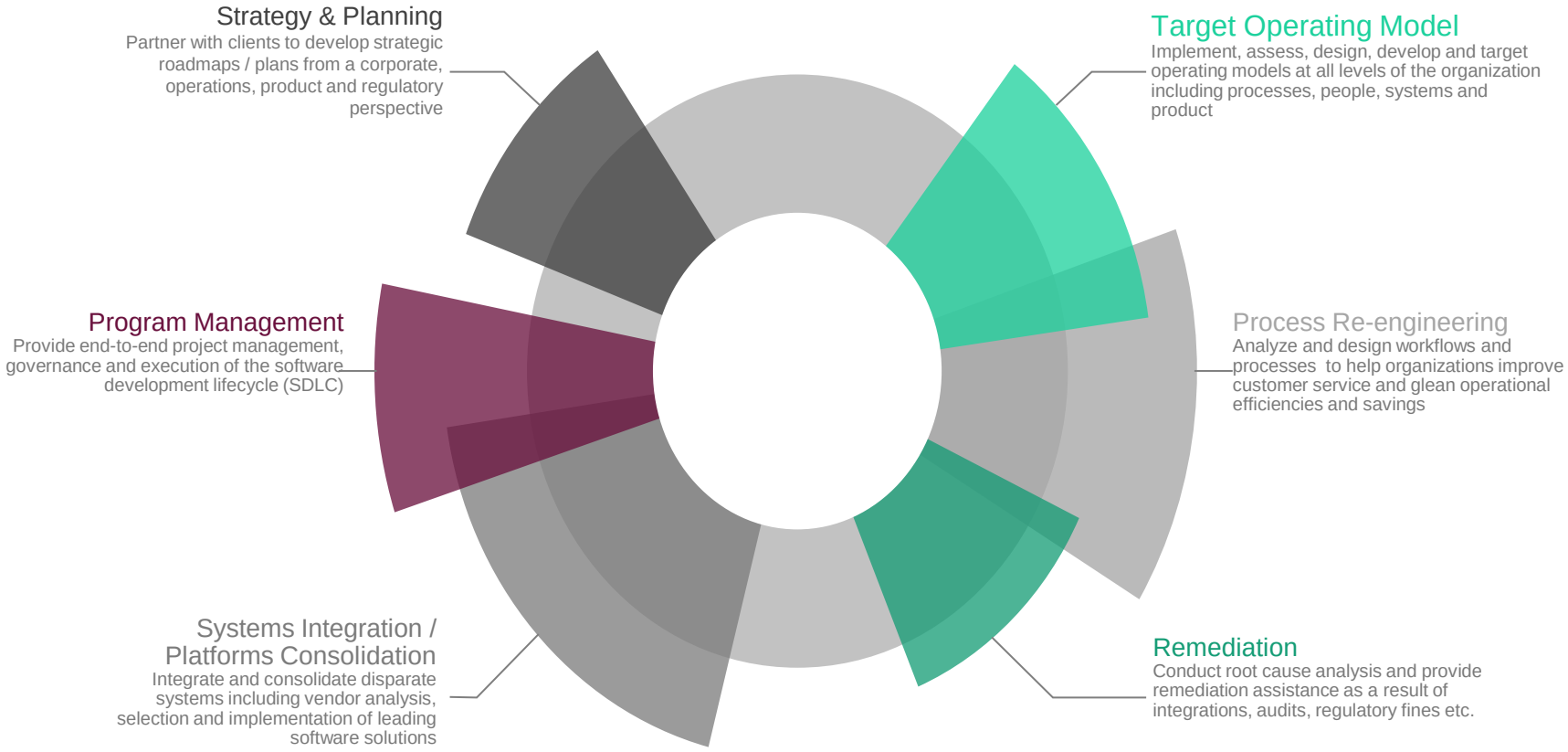
SECTORS

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

Our Capabilities



Consulting 4.0, Our Innovation Ecosystem

DATA SCIENCE EXCELLENCE CENTER

DIGITAL PLATFORM

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

APIFICATOR By siapartners

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

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

STUDIO

E-commerce
AI
Startup trends

IDEATION

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

Why Choose Sia Partners?

CULTURE	We pride ourselves on a “roll up your sleeves” culture and are not afraid to get into the details to better understand the challenges our clients face, including evaluating key processes and systems
LOW TURNOVER	Our turnover is well below the average of 20% in management consulting which has enabled our firm to retain and develop employees
EXPERIENCE	Our teams/employees have either worked at asset/investment and wealth management firms or consulting engagements across product, operations, and technology over the last 20 years
PRODUCT KNOWLEDGE	Our teams have a deep understanding of the various product areas such as Equities, Fixed Income, Derivatives, Mutual Funds, Alternatives, etc. and are uniquely positioned to assist J.P. Morgan Asset Management with the IBOR initiative
LARGE SCALE IMPLEMENTATIONS	We have led and participated in several large-scale implementations at multiple wire houses, broker dealers, etc. (Dodd Frank, CCAR, DOL Fiduciary Rule, Prime Brokerage and Settlement Utility)
INDUSTRY PERSPECTIVE	We participate in industry groups and frequently speak in panel discussions on topics related to Mutual Funds, Fixed Income, Derivatives, Money Markets, 529s, Insurance & Annuities
PRICING	Our pricing model is competitive and can offer a blended rate as well as rates based on the resource mix for the initiative

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

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

*Sia Partners Panama, a Sia Partners member firm