SAI GLOBAL
RISK | COMPLIANCE | ETHICS

SOLUTION WHITEPAPER

# How Financial Services Organizations Benefit by Integrating Vendor Risk and Business Resilience Programs

## New BCBS Cyber-resilience Range of Practices Report offers guidance for financial services organizations

The volume and frequency of cyber breaches that occur via third-party vendors is alarming, leading to millions of records containing privacy data for customers, consumers and employees being stolen all too frequently.

While financial services organizations are maturing in their approach to risk management, there are still significant gaps across silos of risk practices. In December 2018, the Basel Committee on Banking Supervision (BCBS) published *Cyber-resilience: Range of Practices*[1], which compares bank cyber-resilience practices across regulatory jurisdictions around the world. A key section of the report, Interconnections with Third Parties, found that banks across different jurisdictions require institutions to develop a management- and/or board-approved outsourcing framework for managing risk. The findings in this section support a strong business case for banks to

1 **Cyber-resilience: Range of Practices**, Basel Committee on Banking Supervision, December 2018, page 31.

integrate their vendor risk management (VRM) and business continuity management (BCM) programs to better manage dependencies and achieve economies of scale.

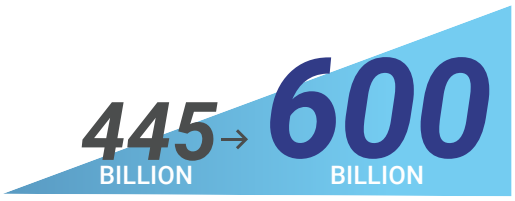
In an increasingly complex business ecosystem, critical activities depend on vendors, with regulations stressing the importance of aligning business continuity plans of critical vendors (and their subcontractors) with the needs and policies of financial services organizations, in terms of recovery, stability and security. These regulations drive improved resiliency through a detailed assessment of a vendor's risk and recovery programs.

This paper is a road map to integrate VRM and BCM disciplines by aligning technological advances and best practices with evolving risk appetites and tolerances. Financial services organizations must strive to close the gap between cybersecurity, vendor risk management, and business continuity to reduce risk to their customers and business, and to improve their overall operational resilience.

## Time to break down silos

VRM intersects with BCM when vendors' access or contribute to financial services organizations information networks and systems poses a continuity and recovery risk to the organization. Just as BCM encapsulates risk assessments, maps critical processes to people and assets and conducts Business Impact Assessments (BIA), VRM extends these practices to third- and fourth-party suppliers, partners and contractors.

Why focus so much on vendors? They provide an "entry point" to your financial services organizations' processes, technology, products and services. Financial services organizations must focus on two fronts: the maturity and effectiveness of the vendor's cybersecurity practices and technology, and the vendor's ability to recover from an incident and continue to provide products and services to your critical processes.




CYBER-CRIME COSTS BUSINESSES NEARLY USD 600 BILLION, UP FROM USD 445 BILLION IN 2014.

## The risk is real[2]:

- While cybersecurity issues affect all sectors and geographies, financial services organizations arguably make up the favorite target of cyber-attackers. Since 2003, cyber breaches have exposed more than 500 million customer records from financial services institutions.*
- A typical financial institution faces an average of 85 targeted cyber-attacks every year, of which a third are successful. According to the 2018 Ponemon Institute study of Data Breach Cost, the average cost of a data breach is USD $3,86 million, and the average cost per lost stolen record is USD $148.
- Cyber-crime costs businesses nearly USD 600 billion, which is up from USD 445 billion in 2014. Cybersecurity breaches are often traced to gaps in vendor information security programs.

The new digital economy is boundaryless. Financial services organizations must contend with real-time, free-flowing information between vendors and other partners that are susceptible to business interruption. How a financial services organization responds to an incident will determine their reputation as well as impact the potential for fines, loss of revenue and legal action.

Given the symbiotic relationship between vendor and business continuity programs,

* https://digitalguardian.com/blog/top-10-finserv-data-breaches

2 **Workshop 6 Cyber-security and operational resilience** International Conference of Banking Supervisors ICBS 2018, page 1.

why do financial services organizations' VRM and BCM programs often operate relatively independent of one another? When coordination is lacking, it becomes increasingly difficult to aggregate and report accurate, timely and complete resilience metrics and risk posture.

Too often, risk management practices fail to keep pace with rapidly evolving business models, which makes financial services organizations more susceptible to cyberattacks and breaches, operational breakdowns and business disruption. Customers have no tolerance for any down time, service disruptions, or data breaches. Social media empowers customers to bring added attention to continuity issues, which raises the stakes for financial services organizations boards and executives.

A financial services organization's response to a business disruption will have a lasting effect on its reputation: social media has become the reputational lens through which customers will determine their willingness to engage.

## Vendor risk and continuity planning

Regulators expect that information, cybersecurity, and/or continuity frameworks address crucial aspects of third-party arrangements, to ensure availability of critical systems and security of sensitive data that is accessible to, or held by, third-party service providers. However, many financial services organizations do not understand the broad range of impacts vendor products and services can have on their own continuity and recovery efforts. It is essential VRM includes contingency plans to address gaps in critical products and services left by vendors. The most common gap in financial services organizations' VRM is that organizations overlook the measurement of recovery time objectives (RTO) to vendor service level agreements (SLA). A vendor's contract SLAs must fall within the RTO of the process they provide products/services to, or the business is

### INTERNATIONAL BUSINESS CONTINUITY AND AVAILABILITY STANDARDS**

Regulators require that recovery tests for critical activities are based on realistic and probable disruptive scenarios and are conducted, at least, on a yearly basis and that service providers and significant counterparties are involved through collaborative and coordinated recovery testing. These tests are typically complemented by audits and monitoring activities (on availability, security incidents, etc.) of the outsourcing vendors.

Additionally, financial services organizations are generally required to manage or take the appropriate steps needed to ensure that their service providers protect their confidential information and that of their clients. Such steps include verifying, assessing, and monitoring security practices and control processes of the service provider.

**Cyber-resilience: Range of Practices, Basel Committee on Banking Supervision. December 2018, page 35

at great risk of not recovering from an incident before an impact is felt.

Typically, financial services organizations have a VRM team that works primarily in collaboration with the financial services organizations' businesses. However, depending on the institution and how it has grown (organic vs. inorganic), the genesis of establishing a vendor relationship may be with the business, not necessarily with the vendor risk management function. Consequently, gaps may exist when trying to codify the financial services organizations' vendors and specifics of their supporting role. The impacts could include duplication of similar services, voids in coverage, duplicative payments, contract lapses and litigious or financial exposure.

A thorough review of vendor recovery capabilities in conjunction with business continuity requirements should include evaluating the criticality of products and services, as well as the vendors' support of critical processes and applications.

The evaluation should result in an ability to:

- Demonstrate operational resilience;
- Identify outstanding issues requiring remediation;
- Address the role vendors play in supporting the financial services organizations' activities; and
- Determine appropriate contingency plans are in place, regularly tested, and updated as appropriate.

There are several proactive steps financial services organizations can take to protect their recovery activity from unpredictable vendor risk management. Consider financial services organizations' BCM program documents recovery time objectives (RTOs) of the business processes supported by each vendor. The financial services organizations' RTOs should be used to define contractual SLAs for vendors and hold them accountable when they fail to meet the services levels required to achieve financial services organizations RTOs. Too often, financial services organizations realize that critical RTOs do not align to SLAs and need to renegotiate contracts.

For example, if financial services organizations process has an RTO of four hours, then requires a vendor SLA of two hours, this would identify the need for a penalty if the vendor cannot recover in time. The lower the RTO and the more critical the process, the higher the penalty should be: this allows for transparency and directs the vendor to demonstrate and have confidence in their ability to recover within their SLA. Vendors should be contractually required to demonstrate their ability to recover within RTOs annually, or more often depending on the impact to the financial services organization for exceeding RTOs.

Another scenario is a financial services organizations process that has an RTO of 30 minutes: the financial services organizations should consider approving and onboarding two vendors to cover the risk of one going down. Vendor selection should not be based purely on cost.[3]

## Aligning VRM and BCM

Financial services organizations are in constant flux, as they seek clarity to understand how their business is changing – examples include technological advances, technological proliferation, inorganic growth and changes in their customer base.

These changes trigger businesses to revisit resiliency variables – RTO, impact analyses, roles and responsibilities, product/service criticality, communication and reporting to demonstrate preparedness.

VRM programs typically classify vendors into tiers to indicate the criticality of their products and services and, most importantly, the part they play in any operational resiliency program. When assessing vendor risk, information security is at the forefront of the mind of most financial services organizations. For example, an IT-shared services unit may rely on an external vendor for hosting

3 **Cyber-resilience: Range of Practices**, Basel Committee on Banking Supervision, December 2018, page 31.

## SIX ESSENTIAL QUESTIONS

1. What access do vendors have to financial services organization and customer data?
2. How critical are the vendor's products and services to the recovery of the process or application?
3. Does the vendor have a mature program for information security and BCM?
4. What were the results of the vendor's last Disaster Recovery exercise?
5. Were issues found and remediated that could impact the vendor's ability to fulfill their service level agreements as they relate to critical financial services organizations processes, products, and services?
6. What is our contractual recourse if the vendor does not meet their SLA?

or cloud services. The IT unit requires a cloud vendor available and online for critical applications. This vendor takes precedence as a critical or tier 1 vendor for contingency planning and recovery.

Understanding the impact a vendor has on a financial services organizations' ability to recover is essential. A point rating system provides a clear metric to measure vendor relevance. For example, a rating based on BIA that have been completed, reflects vendor products and services critical to recovery.

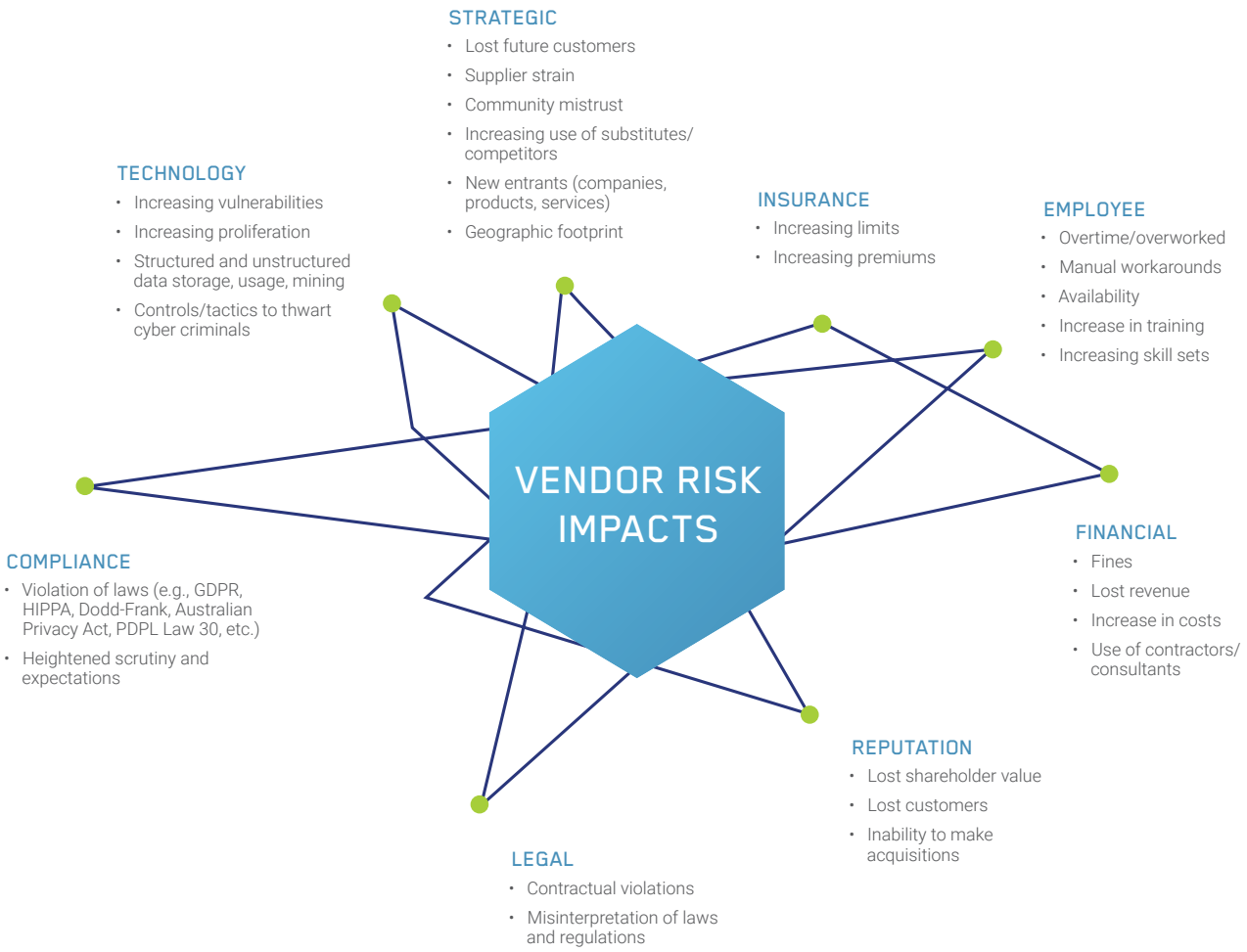
A point rating system also enables financial services organizations to rank vendors specific to recovery of a process or asset. However, it should not be arbitrary: it should be formulaic, based on the link to the business function in question, RTO and critical component inventories. Financial services organizations need to go deeper to ensure vendor recovery capability: they need to be able to perform Vendor Impact Assessments, which are modeled on BCM best practices used in BIAs, to further determine the risk associated with a critical vendor.

Business continuity typically has its roots in a financial services organizations' risk appetite statement, including reserves for capital expenditures to recover and maintain operations, which can be costly. This was especially true in the past when financial services organizations relied on brick-and-mortar options.

The cloud has done a lot to increase availability of applications and data, as well as to reduce the high costs of maintaining failover sites in different physical locations. However, the cloud has led to a marked increase in the risk of cyber breaches and continuity challenges.

Financial services organizations should create "scenario testing" that mitigate risks that affect the organization and its vendors. For example, a subset of risks facing the financial services organizations from a vendor or operational perspective can include a cyber-attack, natural disaster (e.g., flood, storms), or power outage.

## An illustration of potential impacts that financial services organizations face when evaluating the scope of vendor and institutional exposures




In each instance, the financial services organizations should explore how the risk impacts their operations. The business, vendor and risk management teams should ask such questions as, "How would a data breach at a critical vendor affect the risk profile of the financial services organizations?" or "What happens if there is a prolonged regional power outage at both the financial services organizations and a critical vendor?"

Assessing the cyber risk of vendors and carrying out continuous monitoring is essential – this integration of BCM and VRM data often surfaces areas of concern. If the results are above risk tolerances and the vendor supports a critical function, a deeper assessment is required.

The expectations are high. Financial services organizations supervisors demand a pragmatic and thoughtful business continuity approach to confirm availability of critical financial services. The objective of the business continuity plan should minimize financial losses to the financial services organizations, serve its customers and the financial markets with minimal disruption and manage negative effects on operations.

## Do you have the right tools?

To ensure operational resilience, it is essential to:

- Identify vendor products and services that are aligned to financial services organizations operations and core systems;

- Determine critical products and services and document alternate vendor sources;
- Link vendors to potential business impact;
- Evaluate critical vendors' ability to recover within RTO of financial services organizations operations;
- Validate that the critical vendor's contractual service level agreements support RTOs of the financial services organization's operations that the vendor supports;
- Demonstrate critical vendors can recover as required – sit at their tabletop exercises and invite them to yours; and
- Use external sources of assessment, including vendors that rate cybersecurity postures as additional points of information when making vendor assessments.

Ensuring vendors meet your RTOs is particularly important. For example, there may be only one vendor who makes a product that is important to financial services organizations operations — but what if that vendor cannot operate due to an incident? What if they were unable to deliver a key product for 24 hours, instead of within an SLA of four hours? It is important to have backup plans for critical vendors.

Essential planning and recovery questions for business disruption:

- What would the financial, regulatory, reputational and operational impact be to the financial services organizations?
- Can the financial services organizations recover operations effectively without the vendor within RTO?
- Are there alternative vendors that provide the same product or service?
- Has the vendor exercised this scenario? What was the outcome?

Often, organizations with few critical vendors perform assessments manually through spreadsheets, SharePoint and emailed surveys. These tools require significant manual manipulation and data movement, as non-integrated tools rely on human intervention to be useful, which increases the potential for human error. This approach inhibits a fundamental requirement – the ability to perform complete, timely, and accurate impact analysis – which results in assessments that are ineffective, time consuming and incomplete.

Without automation, it is nearly impossible to identify potential weaknesses and gaps: planning efforts become challenging when it is time to identify, document and remediate issues. While many BCM point solutions enable a company to identify vendors and associate them with business functions, they lack the ability to measure vendor risk.

## Value of GRC with BCM

Building business continuity functionality onto a governance, risk management and compliance (GRC) platform enables teams to establish a clear view of risk and recovery by enabling organizations to tie risk to recovery throughout the business continuity process. Teams can eliminate redundancy with one risk language across data and terminology for clear understanding across teams and report better insights and detailed analysis to management from one system of truth with common data.

## Elements of an integrated VRM and BCM program

Executives should consider the following points when integrating VRM and BCM programs:

### LEVERAGE WHAT'S ALREADY IN PLACE

There are prominent practices, resources, data, technology and information within both VRM and BCM functions. These reinforce the foundation of the business while assuring any disruption is met with

diligence and vigor. Take a proactive role to meld each team's methodologies to bring insight into what did not previously exist.

## GATHER INPUT FROM CROSS FUNCTIONAL TEAMS

Other functions and businesses may have tools, technology, or approaches to benefit VRM and BCM. The risk assessment is one example that provides insight. Additionally, legal and compliance provide insight on the applicability of laws and regulations. Insurance helps recover financial loss from the income statement and balance sheets. Audit provides support to the control environment. IT and information security cooperatively identify tools to mitigate exposures, such as cyber or data privacy. Take time to hypothesize how groups work together to share information (e.g., controls), then make it happen.

## USE TECHNOLOGY

Technology and software centralize data, perform risk tactics (e.g., assessment, risk scoring, analytics, etc.), perform continuous due diligence and extract information to understand the vendor criticality, concentration, management and control environment of supporting businesses. These tools can quickly and efficiently support the infrastructure for business continuity, business resilience, crisis management, vendor and integrated risk management. Organizations can then substantiate a vendor's ongoing due diligence items, such as financial health, ISO27001 controls, cybersecurity and procedures and resiliency.

## SEEK EXTERNAL INPUT

VRM typically occurs on a frequent basis (daily, weekly, monthly, annually), where BCM focuses on rare (long-tail) events that may have disastrous effects. In each case, to make the assessment meaningful, the financial services organization needs to rely on emerging risks and regulatory action. These topics aren't always well known from within the organization. Tapping into outside expertise and insights from the organization's vendors (even 2nd, 3rd or 4th tier) provides a thorough understanding of risk topics.

## PRIORITIZE ACTIONS FROM THE ASSESSMENT

The outcome of an assessment is, among other things, a roadmap to prioritize and an indicator of how actions can be managed or mitigated. Actions should be communicated and understood by all risk stakeholders – which likely includes not only functional areas like VRM and BCM, but the business, vendors, audit and regulators. Use the assessment to operationally plan how to use scarce capital and resources and as a starting point for ongoing testing and monitoring.

## KEEP ASSESSING

Vendor risk management is a process, not an event. To be effective, the assessment should not be a "one-and-done" exercise, but rather a dynamic tool to inform decision making as things change. Changes could include new customers, new products or services, the competitive and regulatory landscape, inorganic or

organic growth, financial stability, new and emerging technology, new vulnerabilities, new or failing vendors, etc. Whatever the change, a signal should be sent to revisit the risk assessment, business continuity plan and vendor relationship to ensure the business can not only meet its obligations, but also do so with efficiency and value.

## Effective governance

Ultimately, effective VRM and BCM requires financial services organizations hold all vendors to the same high standards of accountability that are established for the financial services organizations. It is the only way to close the window of vulnerability and prevent dangerous – and potentially catastrophic – scenarios that cripple the business.

## Conclusion

Most financial services organizations use a web of vendors and third parties to bring products to market, which broadens their exposure to risk with every connection. Considering the potential for vendors and third parties to impact financial services organizations operations, it becomes obvious financial services organizations need to do much more to understand the role vendors play in their ability to maintain resiliency. Integrating VRM and BCM programs enables financial services organizations to better profile and screen vendors, conduct impact assessments at the product level, determine assessment needs and maintain historical and auditable assessment records. Such integration enables risk professionals to better manage vendor products and services, their business impacts determine vendor risk scores, capture contract and SLA details, and access additional visualization and reporting capabilities.

Financial services organizations have an opportunity to integrate the principles and practices of their VRM and BCM programs to meet or exceed the standards of latest Bank of England regulatory findings to prioritize important business services, identify impact tolerances, conduct scenario testing and have a comprehensive understanding and mapping of the systems and processes to drive operational resilience on cyber-resilience range of practices. By unifying VRM and BCM data and practices, financial services organizations can capitalize on economies of scope and manage risk more holistically. This leads to better capital and resource management, reduced costs, improved business performance, compliance with regulations and ultimately protects the financial services organizations' reputation and brand.

### CONTACT US

To see a custom demo of our intuitive business continuity software that will allow you to instantly see value with automated responses and processes to drive organizational resilience with best practice driven business impact assessments, vendor risk assessments and crisis management and disaster recovery plans.


# ABOUT SAI GLOBAL

SAI Global helps organizations proactively manage risk to create trust and achieve business excellence, growth, and sustainability. Our integrated risk management solutions are a combination of leading capabilities, services and advisory offerings that operate across the entire risk lifecycle allowing businesses to focus elsewhere. Together, these tools and knowledge enable clients to develop an integrated view of risk. To see our **SAI360 platform** in action, request a **free demo**.

We have global reach with locations across Europe, the Middle East, Africa, the Americas, Asia and the Pacific. For more information visit **www.saiglobal.com/risk.**