Cyberattack, Pandemic and War: Address IT Vendor Risks to Ensure Business Resiliency

Luke Ellery

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."

Gartner®

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

1

Identify Which Risks Matter to Your Business

2

Determine Risk Mitigations for Each IT Category

3

Monitor IT Vendor Risks and Respond to Events

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Identify Which Risks Matter to Your Business

1

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

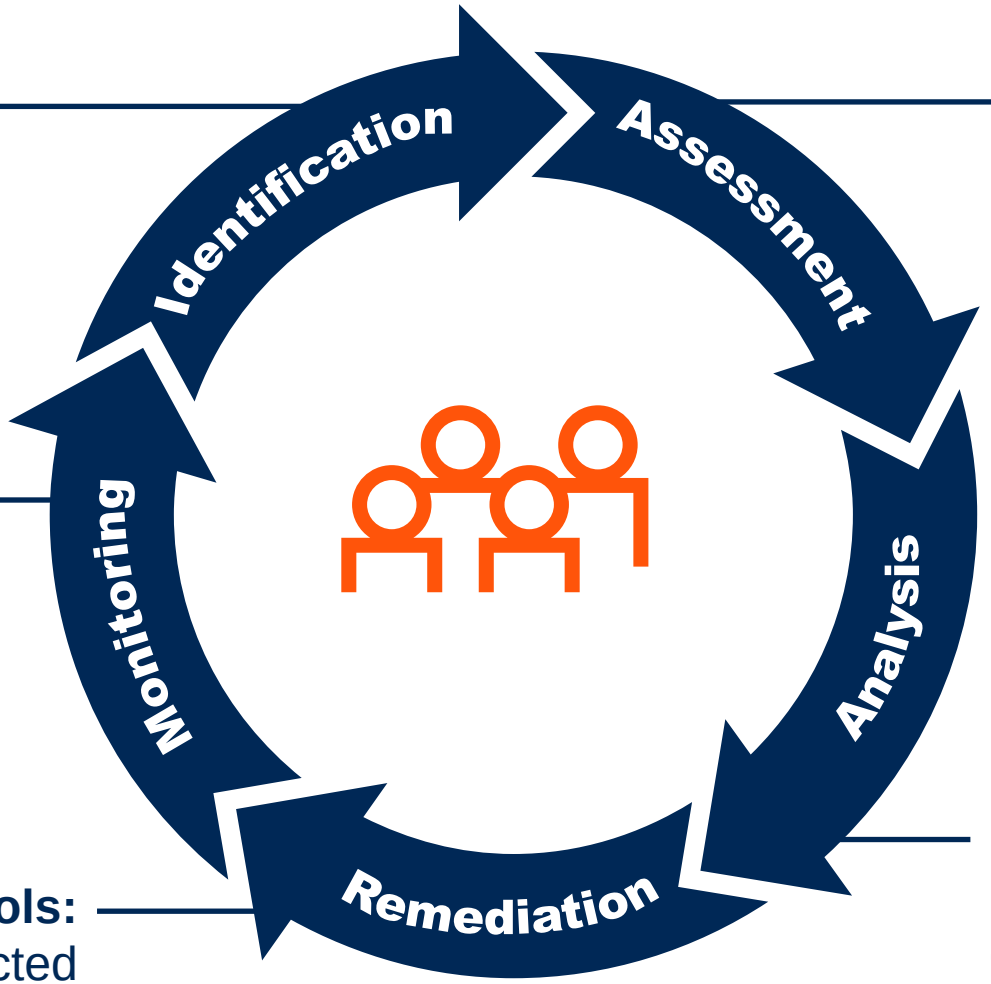
Gartner®

Fundamentals of IT Vendor Risk Management

1

Risk Triage:
Determine which risks apply to your vendors

Get Information:
Determine what controls are in place



Validate Controls:
Ensure they are effective

Decide:
Determine who implements controls and if they are sufficient

Implement Controls:
Ensure they are in place/contracted

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Which Risk Domains Are Relevant to Your Organization?

1

Capacity	Compensation	Corporate Compliance	**Corruption**
Data Privacy	**ESG/Sustainability**	Event Mapping and Monitoring	**Financial**
Geographic	Import/Export and Sanctions	**Operational/ Continuity**	**Performance**
Regulatory Compliance	**Security/Cyber**	**Vendor Strategy**	Workplace Health and Safety

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Identify Risk Owners for Each Risk Domain

Risk Domains	Risk Owners
IT Resiliency	CIO
Vendor Selection	Procurement
Vendor Performance	Vendor Management
Financial Viability	CFO
Cyber and IT Security	CISO and IT Teams
Privacy	Chief Privacy Officer
Sanctions	Legal and Compliance
ESG/Sustainability	Business Owner

1

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Ask Risk Domain Owners to Define Risk Triage Questions

1

1. Does the vendor access/control data? (Data sensitivity and volume)
2. Does the vendor access systems? (Criticality of the system)
3. Does the vendor support business processes? (Criticality of the process)

Yes

- Assess vendor controls
- Assess vendor security/risk capabilities
- Assess vendor BCM/DR, incident response
- Use focused questionnaires (e.g., SIG, SIFMA, etc.)
- Validate controls

- Analyze findings
- Quantify risk impacts
- Determine mitigation requirements
- Determine contract implications

No

No or minimal assessment

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner

Determine Risk Mitigations for Each IT Category

2

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Risk Controls Mitigate Our Risk

Technical: Encryption, Backup, Firewalls, Patching, Multifactor Authentication

Process: Background Checks, Disaster Recovery Test, Risk Acceptance

Contract: Obligations, Actions, Future Undertakings, Indemnities

Compliance: SOC, ISO, Regulatory, Legal

Third Party: Remote Backup, Insurance, Escrow

2

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Who Implements the Control?

2

Business Continuity

For Each Engagement Determine Who Implements the Control

No One | **Us** | **IT Vendor** | **Third Party**

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Business Continuity Plans — With Vendor

Planning

- Disaster scenarios
- Roles and responsibilities
- Key contacts and communication channels
- Definition of success (respective RTOs)

Testing

- Cadence: Annual/Biannual
- Scope: Based on risk priorities
- Responsibilities: Defined roles
- Outcome: Findings reported and recommended actions (i.e., additional mitigations)

2

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Business Continuity Plans — Without Vendor

2

- Identify mission-critical vendors:
  - — Based on recovery time, and
  - — Determined by a business impact assessment

Category	Recovery Time Objective	Description	Primary Site Location	Secondary/ Tertiary Site Location(s)	Organization Contingency Plan Meets RTO (Y/N)	IT Vendor Contingency Plan Meets RTO (Y/N)	Alternate IT Vendor(s) /Internal Capability
Mission Critical	<One Hour						
Business Critical	<24 Hours						
Important	Three-to-10 Days						
Deferrable	10+ Days						

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Risk Mitigation Checklist: SaaS

Example

Non-Negotiable Control Checklist			
Us	Them	Third Party	
			Multifactor Authentication
			Single Sign-on
			Encryption
			Remote Backup
			Endpoint Detection and Response
			SOC 2 Type 2/ISO 27001/Audit

Contract Checklist	
	Maintain Compliance (SOC, ISO, etc.)
	Report Security Breach — 48-72 Hours
	Encryption Standards
	Data Backup/Return/Destruction
	Rights to Terminate/Damages/Audit
	BCP Testing Annually
	Cyber Insurance
	Fourth Parties

Business Continuity Plan			
	Criticality: _____		Alternate Vendor(s): _____
	RTO Objective: _____ Hours		Internal Work Around: _____

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Risk Mitigation Checklist:
Infrastructure Services

Example

Non-Negotiable Control Checklist			
Us	Them	Third Party	
			Staff Background Checks
			Redundancy
			Physical Security
			Remote Backup
			Endpoint Detection and Response
			SOC 2 Type 2/ISO 27001/22301

Contract Checklist	
	Maintain Compliance (SOC, ISO, etc.)
	Report Security Breach — Four Hours
	Data Backup/Return/Destruction
	Rights to Terminate/Damages/Audit
	BCP Testing Bi-Annually
	General and Cyber Insurance
	Fourth Parties

Business Continuity Plan			
	Criticality: _____		Alternate Vendor(s): _____
	RTO Objective: _____ Hours		Internal Work Around: _____

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Risk Mitigation Checklist:
Application Services

Example

Non-Negotiable Control Checklist			
Us	Them	Third Party	
			Staff Background Checks
			Business Viability/Reputation
			Physical Security
			IP/Confidentiality
			Transition Support
			SOC 2 Type 2/ISO 27001/Audit

Contract Checklist	
	Step-in Rights
	Transition Support
	Rights to Terminate/Damages/Audit
	Acceptance Criteria
	Audit Rights
	Subcontractors/Fourth Parties
	WHS and Fair Work
	Local Sourcing Compliance

Business Continuity Plan			
	Criticality: _____		Alternate Vendor(s): _____
	RTO Objective: _____ Hours		Internal Work Around: _____

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Monitor IT Vendor Risks and Respond to Events 3

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Monitor Risk Domains With Subscription Services

3

Recorded Future

Dow Jones

Dun & Bradstreet

Blue Umbrella

Darkbeam

Certa

Capacity	Compensation	Corporate Compliance	Corruption
Data Privacy	ESG/ Sustainability	Event Mapping and Monitoring	Financial
Geographic	Import/Export and Sanctions	Operational/ Continuity	Performance
Regulatory Compliance	Security/Cyber	Vendor Strategy	Workplace Health and Safety

Graphite Systems

Black Kite

Cyberint

CyberGRX

EcoVadis

e-Attestations

BitSight Technologies

SecurityScorecard

APEX Analytix

Supply Wisdom

Representative Vendors — not an exhaustive list

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Monitor Use Change

3

Review at least annually:

- Use
- Purpose
- Data
- Materiality

May require a reassessment or additional controls.

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Unknown Unknowns

Crisis Response Team:

- Sponsor
- Identified staff (not full time)
- Identified IT vendor contacts
- Quarterly scenario tests
- Activation criteria
- Event war room and communications
- Regular business continuity tests (with IT vendors)
- Postincident/test review and improvement plan for learning

3

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Action Plan

Monday Morning:

- *Determine* **risk domains** and **owners** for your organization.

Next 30 Days:

- *Leverage* IT categories (HW, SaaS, etc.) to determine inherent risk profiles — use these to **identify minimum controls.**

Next 12 Months:

- ***Ensure* effective controls are implemented** by you, your vendor or third parties to reduce risk in your vendor ecosystem.
- *Develop* **continuity and contingency plans** and test regularly.
- ***Monitor*** vendor risks and use change over time.
- *Build* a **rapid response team** empowered to address unexpected risks to create a more resilient vendor ecosystem.

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Recommended Gartner Research

- **Formalize Vendor Risk Management to Reduce Business Disruption**
  Joanne Spencer, Luke Ellery and Edward Weinstein
- **4 Third-Party Risk Principles That CISOs Must Adopt**
  Luke Ellery and Sam Olyaei
- **Fundamental Elements of Business Continuity Management — Governance and Program Management**
  Roberta Witty, David Gregory, Jerry Rozeman and Others
- **Market Guide for Third-Party Risk Management Solutions**
  Luke Ellery, Joanne Spencer, Christopher Ambrose and Others
- **Tool: Vendor Identification for Third-Party Risk Management Solutions**
  Luke Ellery, Joanne Spencer, Edward Weinstein and Others

Access to Gartner research is subject to entitlement. For information, please contact your Gartner representative.

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Additional Resources

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Profile IT Subcategories to Risk Domain Threats

Example

Category / Risk Domain	Hardware	SaaS	Telco	Services
Cybersecurity	• Physical Access	• Data Access	• Data Access	• Physical Access • Data Access • System Access
Privacy	• N/A	• PII Data	• N/A	• PII Data • Corporate Data
Sanctions	• Import Sanctions	• Hosting Geography	• N/A	• Geographies
Operational Risk	• System Outage	• System Outage	• Network Outage	• Business Outage

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner®

Continuity Planning Template

Category	Recovery Time Objective	Description	Primary Site Location	Secondary/ Tertiary Site Location(s)	Organization Contingency Plan Meets RTO (Y/N)	IT Vendor Contingency Plan Meets RTO (Y/N)	Alternate IT Vendor(s) /Internal Capability
Mission Critical	**<One Hour**						
Business Critical	**<24 Hours**						
Important	**Three-to-10 Days**						
Deferrable	**10+ Days**						

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.