# RISK ASSESSMENT GUIDE

This guide is designed to assist organizations in determining when SaaS/software escrow business continuity protection should be considered for licensed third-party software.

This is helpful when entering into new software supplier relationships or when performing audits on your existing licensed software to determine their criticality and what would happen if the software supplier were to default or if you would otherwise lose functionality and support for a business-critical application.

**We have determined that there are a handful of categories to help you in qualifying your associated risks.**

## Understanding Criticality & Classification

- What business processes depend on this software?
- How do you classify the software/SaaS vendor – critical, high-risk, or strategic?
- Is this application considered mission-critical for revenue, compliance, or operations?
- How many departments, employees, or customers rely on this solution?
- Have you conducted a Business Impact Analysis (BIA) specific to this application? What were the findings?

## Assessing Operational Vulnerability & Resilience

- Do internal risk policies require contingency measures (e.g., DR, escrow) for critical vendors?
- Is there a documented and tested recovery or exit strategy if the vendor discontinues the service or ceases operations?
- How frequently do you receive data or code exports (if at all)?
- Does your contract include rights to source code, data export, or transition support in the event of vendor failure?
- Are there regulatory requirements (DORA, PRA, APRA, FFIEC) that mandate continuity of service or data control?
- In a worst-case scenario, how would you maintain access to critical IP or data if the vendor is no longer viable?
- Can you self-host or migrate to another vendor quickly if needed? What would that process require?

## Quantifying Financial & Reputational Risk

- How much revenue is processed or supported through the solution each day/month?
- Would a prolonged outage result in contract breaches, client churn, or reputational harm?
- Have you estimated the cost of disruption — including downtime, productivity loss, SLA penalties, or customer churn? What is the estimated cost per hour or day?
- Would the failure of this vendor impact contractual obligations to clients, partners, or regulators?
- What would be the reputational cost of a long-term outage or data unavailability?

## Risk Perception, Governance & Stakeholder Confidence

- On a scale of 1–10, how concerned are you about this SaaS becoming unavailable or unsupported?
- Have you evaluated the financial stability and historical performance of the SaaS vendor?
- Have auditors or regulators raised any continuity concerns regarding this provider?
- How would you defend your risk posture regarding this vendor to your CISO, CFO, or board?

## Need Help?


Web: www.escrowcompany.co
Email: hello@escrowcompany.co
UK Tel: +44(0)203-862-0380
USA Tel: +1-404-301-9593
AUS Tel: +61-2-7229-4872