Cyber Security Factsheet

Third Party Risk Management (TPRM)

BRITISH WOODWORKING FEDERATION

It is important for an organisation to identify, assess, mitigate, and monitor the risks associated with their relationships with external third-party suppliers.

These "third-party suppliers" can include vendors, suppliers, contractors, consultants, service providers, and any other entity that an organisation has a business relationship with and that could potentially introduce risk .

Important questions to ask when assessing the risk with a third-party supplier:

• Who are critical technology providers (for example IT, website, CRM database)

• Can we continue operations without them?

• If not, what are the financial implications?

• Does the company have a Business Continuity Plan (BCP) or a Disaster Recovery Plan (DRP)?

• Are the providers considered in both plans?

• Could a compromised provider/vendor account provide access into your IT environments?

• What critical data is being stored or processed by the provider (employee, customer, IP, etc)?

Terminology to be aware of for third party providers:

OSP (Operational Security Professionals) refers to individuals or teams specializing in security operations, while MSSP (Managed Security Service Provider) describes a third-party company that manages a client's security operations.

To help members carry out their due diligence with their third-party suppliers such as IT providers or website providers, the BWF has pulled together a "Third-Party Vendor Risk Assessment Questionnaire" that can be used to carry out an audit on their current providers or if they are looking to engage with a new provider .

The below questions (which are from the Third-Party Vendor Risk Assessment) have been supplied with additional information on the language and accreditations to look out for in a returned completed risk assessment so you can feel confident they are operating at the standard that protects your business.

If your provider cannot provide any or all of the examples, then you could be at risk and it would be time to course a new provider to protect your data and company.

1. Do you comply with any recognised security standards? Please provide details.

Examples should include:

• Standards like ISO 27001 - a globally recognized international standard for information security management. It provides a framework for organisations to establish, implement, maintain, and continually improve an Information Security Management System (ISMS). This standard helps organisations manage risks related to the confidentiality, integrity, and availability of their information assets.

• Payment Card Industry Data Security Standard PCI DSS) - a set of security standards designed to protect payment card information. It's a global standard that applies to any organisation that stores, processes, or transmits cardholder data, regardless of their size or transaction volume.

• NIST frameworks – are Cybersecurity Frameworks (CSF) which are a voluntary set of guidelines designed to help organisations manage and reduce cybersecurity risks. It provides a structured approach to understanding, managing, and communicating about cybersecurity risks, enabling organisations to better protect their assets and operations It focuses on risk assessment, data protection, and incident response, to ensure a secure supply chain.

BWF/CS/May 2025

Cyber Security Factsheet

Third Party Risk Management (TPRM)

BRITISH WOODWORKING FEDERATION

2. What insurance is in place and does this cover customer/third party impacts? Professional Indemnity/ Cyber etc?

• Professional indemnity (PI insurance) protects businesses against claims made by clients or third parties due to professional negligence or mistakes. It covers legal fees, expenses, and compensation costs if a client claims they suffered a loss because of inadequate advice or services. While not always legally required, it's often a contractual requirement for many professions.

Point to note: While some PI insurance policies might have limited coverage for cyber incidents, a separate cyber insurance policy is needed for comprehensive protection against data breaches, cyber-attacks, and related costs. It is advised that any third-party provider who is holding data on your behalf has separate cyber insurance.

• Cyber insurance is a type of insurance that protects businesses and individuals from financial losses resulting from cyberattacks, data breaches, and other cyber security incidents. It covers a range of costs, including incident response, remediation, legal fees, and third-party liability. In essence, it helps mitigate the financial impact of cyber risks.

3. How do you assess and manage your exposures?

IT providers and website companies should identify assets, assess vulnerabilities, prioritise risks, implement security controls, and continuously monitor for new threats and vulnerabilities. They will do this in a variety of ways, so it is worth being aware of what these processes are and if they mention any in the risk assessment. A specific area to focus on is the implementation of security controls.

1. Asset Identification and Mapping

2. Vulnerability Assessment

3. Risk Assessment and Prioritisation

4. Implementing Security Controls

• Implement security controls: Patch vulnerabilities, enforce strong passwords, implement firewalls, and use intrusion detection systems.

• Regularly review and update security controls: Ensure that security controls are effective and up to date.

4. What monitoring, detection and incident response capabilities do you have access to?

An IT provider and website company would likely leverage Managed Detection and Response (MDR) services, offering capabilities like 24/7 monitoring, threat detection, incident response, and threat hunting, utilising tools such as end point detection and response (EDR), network detection and response (NDR) network security technologies, and security information and event management (SIEM) systems, login and protective monitoring

5. What Cybersecurity controls do you have in place?

In a cybersecurity context, MFA (Multi-Factor Authentication), EDR (Endpoint Detection and Response), and Patching Cadence are security measures, and "access to" typically refers to securing access to systems and data. MFA adds extra verification steps, EDR detects threats on endpoints, and Patching Cadence focuses on timely vulnerability fixes.

6. Have you conducted security assessments including Vulnerability Scans and Pen Testing

Security assessments, including vulnerability scans and penetration testing (pen testing), are crucial for identifying and addressing security weaknesses in systems and applications, with vulnerability scans being automated and pen testing being a manual, simulated attack.

7. How is data backed up, is it tested and how quickly can it be recovered?

Data and website data backups involve creating copies of information to ensure recovery in case of loss, with testing and recovery times varying based on the chosen methods and infrastructure. Look out for how often it is backed up.

8. What indemnities do you provide customers for outages, security incidents etc

In many IT and website contracts, indemnities protect customers from financial losses due to outages, security incidents, or other issues. A vendor might indemnify a customer for losses arising from intellectual property infringement, data breaches, or service disruptions, covering costs like legal fees, regulatory fines, and compensation.

Download Third Party Risk Assessment Form

https://www.bwf.org.uk/wp-content/uploads/BWF-Third-Party-Vendor-Risk-Assessment-Questionaire-2025.pdf

BWF/CS/May 2025