THIRD-PARTY RISK MANAGEMENT

Program Design and Tiered Supplier Risk Assessment Questionnaire

Worked Example: Stark Industries Inc. and Its Cloud Infrastructure Supplier, AWS

Prepared by J Damien Scott, SRMP GRCP ITGRC

GRC Analyst, Portfolio Demonstration

July 2026

Portfolio note: Stark Industries is the same fictional SaaS company used in this candidate's ISO/IEC 27001:2022 portfolio piece. This document designs a complete third-party risk management (TPRM) program and applies it to Stark Industries' relationship with AWS, its cloud infrastructure supplier. The populated questionnaire responses in Section 6 are illustrative: they are built from AWS's own publicly published compliance documentation (its Shared Responsibility Model, published subprocessor list, and publicly referenced ISO and SOC certifications), not from an actual completed vendor questionnaire exchange. This is a work sample demonstrating applied TPRM process and questionnaire design capability, not output from a real client engagement.

Document Control

Field	Detail
Document title	Third-Party Risk Management Program Design and Tiered Supplier Risk Assessment Questionnaire
Organization (fictional)	Stark Industries Inc.
Worked example supplier	Amazon Web Services (AWS), cloud infrastructure provider
Frameworks referenced	NIST Cybersecurity Framework; ISO/IEC 27001:2022 Annex A controls 5.19-5.23; CSA CAIQ; GDPR; HIPAA; DORA
Document owner	GRC Analyst
Reviewed by	Information Security Manager (pending review)
Approved by	Business owner of the supported application (pending approval)
Version	1.0
Status	Draft, prepared for portfolio demonstration
Classification	Internal use only

Table of Contents

1. Executive Summary

This report designs a third-party risk management (TPRM) program for Stark Industries, a fictional small SaaS company, and applies that program to Stark Industries' most critical supplier: Amazon Web Services (AWS), which hosts its production infrastructure. TPRM is the process of managing the cybersecurity risk an organization inherits from the suppliers, vendors, and external service providers it relies on. It matters for three distinct reasons: suppliers hold organizational data that can be exposed even if the customer's own systems are never touched; suppliers with system access are a documented attack path into a customer's environment; and engaging a supplier with poor governance carries reputational and legal risk of association.

The program design follows a four-step process: build and maintain a supplier inventory, classify each supplier into one of three risk tiers, run a tiered questionnaire-based assessment with evidence review, and produce a report that both senior management and the relevant business owner formally sign off. The questionnaire design methodology draws primarily on the NIST Cybersecurity Framework, supplemented by ISO/IEC 27001 Annex A supplier-relationship controls and, where relevant, sector-specific requirements such as the GDPR or HIPAA.

Section 6 applies this program to AWS, which qualifies as a Tier 1 supplier because a disruption to its service would stop Stark Industries' platform from operating and because it holds direct infrastructure access. The worked assessment finds AWS's published security posture satisfactory at the infrastructure layer, but identifies two residual actions that belong to Stark Industries rather than to AWS: formally documenting the shared-responsibility boundary in writing, and confirming that Stark Industries' own account configuration actually uses the encryption and multi-region resilience capabilities AWS makes available. These two findings connect directly to gaps flagged in this candidate's companion ISO/IEC 27001 Statement of Applicability for Stark Industries.

2. Purpose and Scope

The purpose of this document is to design a complete, right-sized TPRM program for a small organization and to demonstrate that program in use through a fully worked supplier assessment. The scope covers supplier discovery, tiering, questionnaire design, evidence review, and reporting. It does not cover contract negotiation or legal review of supplier agreements, which sit with procurement and legal functions and are only referenced here where they intersect with security requirements.

3. Why Third-Party Risk Management Matters

3.1 Data Exposure Risk

Engaging a supplier typically means sharing sensitive information with them: architecture details, credentials for staging environments, and sometimes customer-facing data. That data can remain in the supplier's environment after a project ends. If the supplier is later breached, an attacker can reach organizational data even though the organization's own systems were never directly targeted. TPRM assesses how a supplier manages security inside its own organization, independent of how well it delivers the specific product or service in question. A supplier can ship a technically excellent product while running a weak internal security environment.

3.2 System Access Risk

Many suppliers maintain ongoing access to client systems for maintenance, updates, or managed services. If that supplier is compromised, an attacker can use the supplier's access as an entry point into the client's own environment. The clearest documented example is the 2013 Target breach, in which attackers first compromised a third-party heating, ventilation, and air conditioning contractor that had been granted network access as part of its service contract, then used that access to reach Target's payment systems. The breach resulted in the theft of approximately 40 million customer payment card records and remains one of the most cited examples of supply chain risk in the cybersecurity field.

3.3 Reputational and Legal Risk

Engaging a supplier also creates a risk of association. A supplier may be engaged in illegal or unethical activity, including money laundering or modern slavery in its labor practices. Due diligence before engaging any supplier should include a check for this kind of conduct, since an organization can face legal and reputational consequences for doing business with a supplier later found to be engaged in it, independent of any cybersecurity failing.

4. TPRM Process Design

4.1 Step 1: Supplier Discovery and Inventory

The first step is producing a comprehensive, accurate, and current list of all suppliers. Procurement is the starting point, since it tracks every vendor the organization pays. The IT team supplements this list with suppliers tied to critical applications, and business department heads validate the combined list and confirm current contacts. Priority goes to departments handling sensitive information first: finance, HR, and legal.

4.2 Step 2: Supplier Tiering and Classification

Once the inventory exists, every supplier is classified into one of three tiers by criticality and sensitivity.

Tier	Classification criteria
Tier 1 (highest priority)	Has direct access to organizational systems or environment; holds sensitive organizational data (personal data, employee PII, customer records); or provides a service so critical that its disruption would stop the business from operating.
Tier 2 (medium priority)	Handles some organizational data, but that data is not highly sensitive; provides a service whose disruption would not halt core business operations.
Tier 3 (lower priority)	Has no access to organizational systems or environment; holds no organizational data; provides a non-critical service.

4.3 Step 3: Assessment Workflow

The assessment itself follows a defined workflow from questionnaire delivery through to a signed-off report.

1. Send the cybersecurity questionnaire, tiered to the supplier's classification, to the supplier's designated security or compliance contact.
2. The supplier provides written answers and supporting evidence for each question.

3. The GRC analyst reviews the answers and inspects the evidence provided.
4. If answers are incomplete or unclear, the analyst requests a follow-up meeting with the supplier's cybersecurity team.
5. The analyst produces a formal assessment report documenting findings, risks, and recommendations.
6. The report is reviewed and signed off by senior management and the business owner of the application or service the supplier supports.

4.4 Step 4: Reporting and Sign-Off

Every assessment report states the supplier's name and the type of data or access it holds, the controls that were assessed, the findings and identified risks in plain language, recommendations for remediating each finding, and the risk acceptance or remediation decision made by management and the business owner. Both senior management and the business owner of the application or service the supplier supports must sign off, since both need to be aware of identified risk before deciding to accept it or require remediation.

5. Questionnaire Design Methodology

5.1 Framework Selection

The questionnaire is not based on a single framework. The NIST Cybersecurity Framework is the recommended starting point because it is comprehensive and suits most industries, and it is supplemented with sector- or jurisdiction-specific requirements where relevant.

Context	Relevant framework or standard
Healthcare (United States)	HIPAA / HITECH
Healthcare (Australia)	Privacy Act 1988 (personal information focus)
Any sector processing personal data in Europe	GDPR
General international baseline	ISO/IEC 27001, Annex A controls 5.19-5.23
Financial sector (European Union)	DORA (Digital Operational Resilience Act)
Cloud services	Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CAIQ)

5.2 Practicality and Question Grouping

A 900-question survey is counterproductive: suppliers ignore it, take unreasonably long to complete it, or submit low-quality answers. The design principle used throughout Section 6 is to group related controls into single, broader questions. Instead of five separate questions about encryption, the questionnaire asks one: is data encrypted, and if so, what approach is used for data at rest and in transit? One well-designed question can satisfy several framework controls at once.

5.3 Evidence Requirements

Every significant question includes space for supporting evidence, and yes/no answers are never accepted without verification. Acceptable evidence includes a relevant policy document, a

screenshot demonstrating the control, or a live screen-share demonstration. Where a supplier will not provide written evidence, a live session is an acceptable substitute, and any resulting limitation, for example being unable to take screenshots during that session, is documented in the report rather than silently dropped. The depth of evidence required should scale with the sensitivity of the system and the maturity of the supplier.

5.4 Tiered Questionnaire Depth

Tier 1 suppliers receive the most comprehensive questionnaire, with the greatest depth and the highest evidence bar. Tier 2 suppliers receive a moderate-depth questionnaire with some questions removed. Tier 3 suppliers receive a lightweight questionnaire covering only basic controls. Appendix A summarizes the Tier 2 and Tier 3 scope; Section 6 below is the full Tier 1 questionnaire applied to AWS.

6. Worked Example: Assessing Stark Industries' Key Supplier, AWS

6.1 Supplier Profile and Tiering Decision

AWS hosts the entirety of Stark Industries' production infrastructure, as documented in this candidate's companion ISO/IEC 27001 asset register. AWS meets two of the three Tier 1 criteria on its own: it has direct infrastructure-level access to Stark Industries' environment, and its service is critical enough that a sustained AWS outage would stop the platform from operating for customers. AWS is therefore classified as Tier 1 and receives the full questionnaire below, with the highest evidence bar the program defines.

6.2 Tier 1 Questionnaire: Questions, Responses, and Evidence

The table below records each question, a summary of AWS's publicly documented position, the evidence reviewed, and the reviewer's assessment. As noted in the portfolio note on the cover page, the response and evidence columns are built from AWS's own public compliance documentation rather than a private questionnaire exchange.

Domain / Question	Supplier response (summary)	Evidence reviewed	Reviewer assessment
Governance and certifications: Does the organization maintain independent third-party security certifications or attestations (for example, ISO/IEC 27001 or SOC 2 Type II)? Provide current certificates or reports.	AWS maintains ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and SOC 1, 2, and 3 attestations across its infrastructure services, renewed on a recurring cycle.	ISO/IEC 27001 certificate and SOC 2 Type II report summary, available through AWS Artifact.	Satisfactory. Certifications are current and their stated scope covers the services Stark Industries uses.
Shared responsibility boundary: Describe how security responsibilities are divided between your organization and customers for the services in use.	AWS publishes and maintains a documented Shared Responsibility Model: AWS secures the cloud (physical infrastructure, hypervisor, and managed-service internals); the customer secures what it puts in the cloud (guest operating system configuration, identity and	AWS Shared Responsibility Model documentation.	Satisfactory as a stated model, but flagged as a judgment item. Stark Industries must document its own side of this boundary in writing rather than relying on an informal understanding (see Section 6.3).

Domain / Question	Supplier response (summary)	Evidence reviewed	Reviewer assessment
	access management, encryption choices, network controls).		
Encryption: Is data encrypted? If yes, provide details of the encryption approach used for data at rest and data in transit.	AWS supports encryption at rest through its key management service for storage and database services, and encryption in transit through TLS on all API endpoints. Enabling encryption on customer-owned resources is a customer configuration choice.	Key management service documentation; TLS configuration confirmed on account endpoints during technical review.	Satisfactory, contingent on Stark Industries enabling encryption by default across its own resources rather than assuming it is on.
Incident management: Describe your incident detection, response, and customer notification process, including typical notification timelines.	AWS operates continuous security monitoring and an incident response function, and commits to customer notification obligations defined in its data processing terms and applicable service agreements.	AWS security incident response overview; notification clauses in the AWS data processing addendum.	Satisfactory for infrastructure-layer incidents. Stark Industries remains fully responsible for detecting and responding to incidents at the application layer, which is the gap this questionnaire cannot close on its own.
Business continuity and resilience: Describe your business continuity and disaster recovery capabilities, including redundancy across regions or availability zones.	AWS operates multiple geographically isolated availability zones per region and publishes documented resilience commitments for each service.	AWS global infrastructure documentation.	Satisfactory as a capability. The benefit only accrues to Stark Industries if its own architecture actually deploys across multiple availability zones, which is a configuration decision, not an AWS guarantee.
Subprocessor and supply chain management: Do you use subprocessors or subcontractors with access to customer data? If so, how are they managed and disclosed?	AWS publishes a list of subprocessors and commits to notifying customers of material changes under its data processing terms.	Published AWS subprocessor list.	Satisfactory.
Access control capability: What access control mechanisms are available to customers to enforce least privilege and segregation of duties?	AWS Identity and Access Management supports granular, role-based permissions, multi-factor authentication enforcement, and permission boundaries.	Identity and access management documentation; Stark Industries' own configuration confirmed separately during architecture review.	The capability itself is satisfactory. Whether Stark Industries actually configures it correctly is tracked separately under its own ISO/IEC 27001 Statement of Applicability, not under this supplier assessment.
Legal, regulatory, and contractual terms: Do your contractual terms address data protection, breach notification, and applicable regulatory obligations such as the GDPR?	AWS's standard customer agreement and data processing terms address data protection responsibilities, breach notification obligations, and standard contractual clauses for international data transfers.	AWS customer agreement; AWS data processing addendum.	Satisfactory.

6.3 Assessment Findings and Report Summary

AWS's published security posture is assessed as satisfactory at the infrastructure layer: current, relevant third-party certifications; a clearly published shared-responsibility model; encryption capability at rest and in transit; a documented incident and breach-notification process; multi-availability-zone resilience; disclosed subprocessor management; strong native access-control tooling; and contractual terms addressing data protection and international transfer.

Two findings, however, belong to Stark Industries rather than to AWS, and this report escalates them as residual actions rather than treating the supplier assessment as fully closed:

1. Document the shared-responsibility boundary in writing. Stark Industries currently treats this boundary as an informal understanding. This finding directly matches control 5.22 in Stark Industries' ISO/IEC 27001 Statement of Applicability, which flagged the same boundary as a judgment call needing explicit documentation rather than full independent oversight.
2. Confirm that Stark Industries' own account configuration actually uses the capabilities AWS makes available, specifically default encryption on storage resources and a genuinely multi-availability-zone production deployment. AWS provides the capability; whether it is switched on is entirely Stark Industries' responsibility, and this cannot be verified through a supplier questionnaire alone.

Recommended risk acceptance decision: given AWS's certification posture and scale, no further supplier-side remediation is required at this time. The two residual actions above are logged as internal action items owned by Stark Industries' Information Security Manager, not as findings against AWS, and this distinction should be preserved in the final signed report so that accountability is not misattributed to the supplier.

7. Program Governance: Common Pitfalls and How This Program Avoids Them

7.1 Automated External Scanning Is Not a Substitute for Assessment

Some vendors sell tools that run an external scan of a supplier's website and present the result as a cybersecurity assessment. This is not a valid substitute. An external scan cannot see internal security policies, staff training practices, data handling and disposal procedures, incident response capability, or access control maturity; it only observes what is visible from outside. The program in this report relies on questionnaires, evidence review, and, where needed, stakeholder interviews, precisely because the risks that matter live inside the supplier's organization, not on its public-facing website.

7.2 Remediation Follow-Up Failures

A common and serious failure occurs after the report is produced: identified risks are logged, then quietly deprioritized as cybersecurity teams get pulled into active incidents and support tickets. Six months later, an unencrypted-data finding, for example, may still be unresolved with no further action taken, which is not an unusual outcome without deliberate management. This program requires that every finding carry a named owner, a remediation action, and a clear deadline, and that follow-up be scheduled and tracked on a regular cadence rather than left to whichever team remembers to check.

7.3 Procurement Integration

The most effective way to keep TPRM in step with supplier onboarding is to connect it to the procurement workflow itself, so that a cybersecurity assessment ticket is generated automatically whenever a new supplier contract is created or an existing one is renewed. This ensures no supplier is missed and the cybersecurity team is notified at the right time rather than after the fact.

7.4 Realistic Timelines

Organizations routinely underestimate how long supplier assessments take. Tier 1 suppliers should be assessed first; Tier 2 and Tier 3 suppliers follow on a realistic plan. For a larger organization with a substantial supplier population, a proposal to assess every supplier within six months should generally be extended to twelve or eighteen months, since assessments consistently take longer than anticipated. Stark Industries, as a small organization with a short supplier list built around one Tier 1 relationship, is an exception where a compressed timeline is realistic; this program does not force a small organization into process built for a much larger one.

8. Conclusion and Recommendations

This program demonstrates that a right-sized TPRM process, three tiers, a tiered questionnaire, evidence review, and a formal sign-off, can be built and applied even for a small organization with a short supplier list. Applied to Stark Industries' relationship with AWS, the process did not simply produce a passing grade; it distinguished clearly between what the supplier is responsible for and what remains Stark Industries' own configuration responsibility, which is the distinction that a shared-responsibility cloud relationship most often gets wrong in practice.

Three recommendations follow. First, Stark Industries should formally document the AWS shared-responsibility boundary as a standing artifact, not only as a line item in this assessment, since it will be requested again at the next ISO/IEC 27001 audit cycle. Second, the two configuration-verification actions in Section 6.3 should be tracked to closure with named owners and deadlines, consistent with the remediation-tracking discipline in Section 7.2, rather than left as open text in this report. Third, as Stark Industries grows and takes on additional suppliers, the Tier 2 and Tier 3 questionnaire templates in Appendix A should be activated immediately, before the supplier list grows large enough to make retrofitting a tiering process difficult.

Appendix A: Tier 2 and Tier 3 Questionnaire Scope

Tier 2 and Tier 3 suppliers do not receive the full Tier 1 questionnaire in Section 6. The tables below summarize the reduced scope for each tier, consistent with the tiering principle in Section 5.4.

Tier	Questionnaire scope
Tier 2	Certifications held (self-attested list, no document review required unless a gap is flagged); encryption in place (yes/no plus brief description); incident notification commitment; subprocessor disclosure (yes/no); basic contractual data protection terms confirmed.
Tier 3	Confirmation that no organizational data is held and no system access exists; a single question confirming this scope statement, revisited only if the relationship changes.

Appendix B: Glossary of Key Terms

Term	Definition
CAIQ	Consensus Assessments Initiative Questionnaire: a standardized cloud-provider security questionnaire published by the Cloud Security Alliance.
Shared responsibility model	A cloud-provider framework dividing security obligations between the provider, which secures the underlying infrastructure, and the customer, which secures its own configuration, data, and access management within that infrastructure.
Subprocessor	A third party engaged by a supplier to process data on the supplier's behalf, requiring disclosure and management under most data protection regimes.
Tier 1 / 2 / 3 supplier	A three-level classification of suppliers by criticality and data sensitivity, used to scale the depth of a TPRM assessment to the level of risk a supplier actually presents.
TPRM	Third-Party Risk Management: the process of managing cybersecurity risk posed by suppliers, vendors, and external service providers.

References

Amazon Web Services. (2025). AWS shared responsibility model.

Amazon Web Services. (2025). AWS Artifact: On-demand access to AWS compliance reports.

Cloud Security Alliance. (2023). Consensus Assessments Initiative Questionnaire (CAIQ), Version 4.

European Union. (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

European Union. (2022). Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554.

International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection: Information security management systems: Requirements (ISO/IEC 27001:2022).

Krebs, B. (2014). Target hackers broke in via HVAC company. Krebs on Security.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, Version 1.1.

Office of the Australian Information Commissioner. (1988, as amended). Privacy Act 1988 (Cth).

U.S. Department of Health and Human Services. (1996, as amended). Health Insurance Portability and Accountability Act (HIPAA).