ISO/IEC 27001:2022

Information Security Risk Assessment, Risk Treatment Plan, and Statement of Applicability

Stark Industries Inc. (a fictional SaaS marketing platform hosted on AWS)

Prepared by J Damien Scott, SRMP GRCP ITGRC

GRC Analyst, Portfolio Demonstration

July 2026

Portfolio note: Stark Industries is a fictional organization used throughout. This document applies the concepts of Clauses 6.1.2 and 6.1.3 of the standard to that fictional scenario in full, including a complete 93-control Statement of Applicability. It is presented as a work sample demonstrating applied ISMS analysis capability, not as output from an engagement with a real client or employer.

Document Control

Field	Detail
Document title	ISO/IEC 27001:2022 Information Security Risk Assessment, Risk Treatment Plan, and Statement of Applicability
Organization (fictional)	Stark Industries Inc.
ISMS scope	The SaaS marketing platform, its source code, CI/CD pipeline, AWS production environment, and the data it processes
Standard referenced	ISO/IEC 27001:2022, Clauses 6.1.2, 6.1.3, and Annex A
Document owner	GRC Analyst
Reviewed by	Information Security Manager (pending review)
Approved by	Chief Executive Officer (pending approval)
Version	1.0
Status	Draft – prepared for portfolio demonstration
Classification	Internal use only

Table of Contents

1. Executive Summary

This report documents an information security risk assessment and risk treatment exercise conducted for Stark Industries Inc., a fictional small software-as-a-service (SaaS) marketing platform hosted on Amazon Web Services (AWS). The exercise follows the requirements of Clauses 6.1.2 and 6.1.3 of ISO/IEC 27001:2022, the international standard for information security management systems (ISMS).

The assessment identified five critical assets and five corresponding risk scenarios. Three risks scored in the High range and two scored in the Medium range under a 5×5 qualitative scoring model. Each risk was treated primarily through mitigation, drawing on 65 of the 93 controls in Annex A of the 2022 standard. After treatment, four of the five risks fall to a Low residual level and one, concerning production infrastructure availability, remains at a Medium residual level that the organization has chosen to monitor rather than treat further.

The Statement of Applicability presented in Section 7 addresses all 93 Annex A controls: 65 are marked applicable (in full or in part) and 28 are excluded with a documented justification, consistent with the traceability rule that every applicable control must trace to an identified risk and every exclusion must be defensible at audit.

The purpose of this document is twofold. First, it demonstrates a complete, audit-ready application of the ISO/IEC 27001:2022 risk assessment and treatment process to a realistic small-organization scenario. Second, it distinguishes clearly among four categories of statement used throughout: requirement (what the standard obliges), interpretation (a defensible reading where the standard leaves room), judgment (a practitioner or management decision), and recommendation (good practice that supports certification without being strictly required). That distinction is what allows an auditor, or an employer evaluating this work, to see exactly where the standard's authority ends and professional judgment begins.

2. Purpose and Scope

2.1 Purpose

The purpose of this document is to record how Stark Industries identified, analyzed, evaluated, and treated information security risk within the scope of its ISMS, and to declare which Annex A controls apply as a result. Under Clause 6.1.2, an organization must define and apply a repeatable risk assessment process; under Clause 6.1.3, it must treat the risks that process identifies and produce a Statement of Applicability. This document satisfies both requirements for the defined scope below.

2.2 Scope of the ISMS

The ISMS scope covers the SaaS marketing platform operated by Stark Industries: its source code, its continuous integration and continuous deployment (CI/CD) pipeline, its AWS production infrastructure, the developer endpoint used to build and maintain it, and the data the platform processes. The scope explicitly excludes physical office facilities, since the organization operates on cloud infrastructure under AWS's shared-responsibility model, and excludes any personal data processing, since the platform currently processes publicly available marketing data rather than identifiable customer information.

2.3 Organizational Context

Stark Industries is a small technology company. Its core commercial asset is the SaaS platform itself; its principal exposure is the loss of confidentiality, integrity, or availability of the code, infrastructure, and data that make that platform run. This context shapes every judgment made in this report: control selection stays proportionate to a small organization's resources, and scope decisions favor a tight, defensible boundary over an exhaustive but unmanageable one.

3. Risk Assessment Methodology

ISO/IEC 27001:2022 does not prescribe a specific risk assessment technique. It requires that the process be documented, repeatable, and capable of identifying risk to the confidentiality, integrity, and availability (the CIA triad) of information within scope, together with a named owner for each risk. The methodology below satisfies that requirement; the specific six-stage flow and the 5×5 scoring scale are practitioner judgments, endorsed by management, rather than requirements of the standard itself.

3.1 Process Overview

The assessment follows six stages:

1. Asset identification
2. Threat and vulnerability identification
3. Risk analysis (likelihood × impact)
4. Risk evaluation
5. Risk ownership assignment
6. Documentation of results

Threats and vulnerabilities were drawn from four recognized sources: the OWASP Top 10 for application-layer risk, NIST Special Publication 800-30 for general risk assessment guidance, current industry threat intelligence, and Stark Industries' internal incident history. No prior incidents were recorded for this fictional organization, so likelihood ratings below rely on the first three sources.

3.2 Risk Scoring Criteria

Likelihood and impact are each rated on a five-point scale, and risk score is calculated as likelihood multiplied by impact, producing a maximum possible score of 25.

Score	Likelihood label	Description
1	Rare	May occur only in exceptional circumstances
2	Unlikely	Not expected, but possible
3	Possible	Might occur at some point
4	Likely	Expected to occur occasionally
5	Almost certain	Expected to occur frequently

Score	Impact label	Description
1	Negligible	No significant disruption or damage
2	Minor	Minor disruption or limited financial or reputational impact

Score	Impact label	Description
3	Moderate	Noticeable impact requiring management attention
4	Major	Serious impact on operations, finances, or compliance
5	Severe	Critical impact, regulatory breach, or long-term damage

3.3 Risk Evaluation Criteria

Risk score	Risk level	Action required
1–6	Low	Acceptable; monitor only
7–14	Medium	Treatment or mitigation required, based on context
15–25	High	Unacceptable; immediate treatment required

3.4 Risk Acceptance Criteria

Low risks are acceptable with ongoing monitoring. Medium risks require a documented business justification or partial mitigation. High risks must be treated, or explicitly accepted in writing by senior management. These thresholds express the organization's risk appetite. That appetite is a management decision, not an analyst decision; the GRC analyst's role is to propose the criteria and ensure management formally endorses them before the assessment begins.

4. Asset Inventory and Classification

Assessing risk to an asset that has not been identified is not possible, so asset identification precedes risk analysis. Stark Industries classifies information according to a four-level scheme anchored to the CIA triad.

4.1 Classification Scheme

Level	Meaning	Example
Confidential	Highly sensitive; restricted to a specific audience	Source code, company secrets
Restricted	Limited access and operational use	Production environment configuration
Internal use only	For employees generally, not for outsiders	Intranet content, internal communications
Public	Anyone may read	Website content

4.2 Asset Register

Five assets fall within the defined ISMS scope. Confidentiality, integrity, and availability (C / I / A) ratings feed directly into the risk analysis in Section 5.

ID	Asset	Type	Classification	C	I	A
1	Source code repository	Information / IT	Confidential	High	High	Low
2	AWS EC2 production environment	IT infrastructure	Restricted	High	High	High
3	CI/CD pipeline	IT	Confidential	High	High	Medium
4	Developer laptop	IT endpoint	Internal use only	Medium	Medium	Medium

ID	Asset	Type	Classification	C	I	A
5	Processed customer and marketing data	Information	Confidential	High	High	Medium

Confidentiality is rated High for the source code repository, the production environment, the pipeline, and the data asset, because disclosure of any of them would let a competitor copy or undercut the product. Integrity is rated High across nearly every asset, because tampering with code, infrastructure, or data directly corrupts the product; the developer laptop is rated Medium on the assumption that it should hold no confidential material at rest. Availability ratings vary: production must remain available to customers and is rated High, while the source code repository can be briefly unavailable without stopping an already-deployed application and is rated Low.

Scoping judgment: only the primary developer's laptop was included in scope, not every employee endpoint. The reasoning is that a tight scope focused on the application and its code keeps the assessment manageable, and controls proven effective on one laptop generalize readily to others without expanding the audit surface. This is a defensible choice validated by an auditor, not the only possible choice; management could reasonably decide to include all endpoints.

5. Risk Assessment Results

Each asset was assessed against applicable threats and vulnerabilities. For a small organization such as Stark Industries, one risk scenario per asset is typical; the number of risks scales with the size of what is in scope, not with thoroughness pursued for its own sake.

5.1 Risk Identification

Risk ID	Asset	Threat	Vulnerability
R1	Source code repository	Code theft; insider threat	Weak repository permissions
R2	AWS EC2 production environment	Denial-of-service attack; misconfiguration	Misconfigured VPC or IAM permissions
R3	CI/CD pipeline	Pipeline compromise; secret leakage	Hard-coded secrets; insufficient logging
R4	Developer laptop	Malware; phishing; physical theft	No endpoint protection; low security awareness
R5	Processed customer and marketing data	Unauthorized access; data corruption	Weak access control

5.2 Risk Scoring and Ownership

Risk ID	Likelihood	Impact	Score	Level	Risk owner
R1	4 (Likely)	4 (Major)	16	High	Software Developer (Engineering Lead)
R2	3 (Possible)	5 (Severe)	15	High	IT Infrastructure Engineer
R3	4 (Likely)	4 (Major)	16	High	Software Developer (DevOps Lead)
R4	4 (Likely)	3 (Moderate)	12	Medium	IT Infrastructure Engineer
R5	3 (Possible)	4 (Major)	12	Medium	Information Security Manager

Three risks (R1, R2, R3) scored in the High range and two (R4, R5) scored in the Medium range. Under the acceptance criteria in Section 3.4, all five require treatment; none qualifies for acceptance without mitigation. Section 6 records the treatment decision and the resulting residual risk for each.

6. Risk Treatment Plan

Clause 6.1.3 requires the organization to select a treatment option for each unacceptable risk, determine the controls that implement it, and re-score the risk once controls are applied. Four treatment options exist in established risk management practice: mitigate (reduce likelihood or impact through controls), avoid (stop the activity that creates the risk), transfer (move the risk to another party, such as through insurance), and accept (tolerate the risk as a cost of doing business). All five risks in this assessment were treated through mitigation; none warranted avoidance, transfer, or unmitigated acceptance given the criticality of the underlying assets.

6.1 Treatment Selection

Risk ID	Treatment option	Selected Annex A controls
R1	Mitigate	5.3, 5.15–5.18, 8.2, 8.3, 8.4
R2	Mitigate	5.23, 5.30, 8.9, 8.14, 8.15, 8.16, 8.20–8.22
R3	Mitigate	5.3, 8.15, 8.16, 8.24, 8.25, 8.26, 8.28, 8.31
R4	Mitigate	6.1, 6.3, 8.1, 8.7
R5	Mitigate	5.12, 5.15–5.18, 8.10, 8.15, 8.16, 8.24

6.2 Residual Risk

Residual risk is the exposure that remains once controls are applied. It is calculated during treatment, not during the initial assessment, because it cannot be known until the controls that will reduce likelihood or impact have been selected.

Risk ID	Residual likelihood	Residual impact	Residual score	Residual level	Status
R1	2 (Unlikely)	3 (Moderate)	6	Low	Treated
R2	2 (Unlikely)	4 (Major)	8	Medium	Treated – monitor
R3	2 (Unlikely)	3 (Moderate)	6	Low	Treated
R4	1 (Rare)	2 (Minor)	2	Low	Treated
R5	2 (Unlikely)	3 (Moderate)	6	Low	Treated

Four risks fall to a Low residual level after treatment. R2, the risk of a production outage, is deliberately left at a Medium residual level rather than forced down to Low. Even with configuration management, monitoring, redundancy, and incident management controls in place, a severe-impact scenario in a cloud production environment retains meaningful residual exposure; treating every risk as fully resolved after one round of controls would misrepresent the organization's actual posture. This risk is retained on the register for ongoing monitoring rather than closed.

6.3 Risk Owner and Management Approval

Under Clause 6.1.3, each risk owner must approve the treatment plan for their risk, and residual risks must be formally accepted by senior management, since management holds ultimate accountability for the organization's risk appetite. In this fictional exercise, the following sign-off structure applies: the Software Developer (Engineering Lead) owns R1 and R3, the IT Infrastructure Engineer owns R2 and R4, and the Information Security Manager owns R5. All residual risk levels, including the Medium-level residual on R2, require sign-off from the Chief Executive Officer before the treatment plan is considered closed.

7. Statement of Applicability

The Statement of Applicability (SoA) is the mandatory document required by Clause 6.1.3. It lists every control in Annex A of ISO/IEC 27001:2022, ninety-three controls across four themes in the 2022 edition, states whether each is applicable, justifies the decision, and names the document that will provide implementation evidence. Annex A itself is not a checklist to implement in full; it is a completeness check against the organization's own risk-driven control selection. A control may enter the SoA only because the risk assessment in Sections 5 and 6 identified a need for it. Marking a control not applicable while a corresponding risk exists would be a non-conformity at audit.

The Stark Industries workshop that this exercise draws on left eleven of the ninety-three decisions unstated. Each of those eleven is completed independently in the tables below and marked "(J)" for judgment, distinguishing it clearly from the decisions carried forward directly from the source material. Across all four themes, 65 controls are applicable in full or in part and 28 are excluded with justification.

Theme	Total controls	Applicable	Not applicable
Organizational (5.1–5.37)	37	29	8
People (6.1–6.8)	8	8	0
Physical (7.1–7.14)	14	0	14
Technological (8.1–8.34)	34	28	6
Total	93	65	28

7.1 Organizational Controls (A.5.1–A.5.37)

Control	Title	Decision	Justification	Implementing Document
5.1	Policies for information security	A	An information security policy is already established and governs the ISMS.	Information Security Policy
5.2	Information security roles and responsibilities	A	Roles and responsibilities are already defined for the ISMS.	Roles and Responsibilities Record
5.3	Segregation of duties	A	The assessment identified a need to manage permissions and prevent unauthorized pipeline access, reducing insider-threat likelihood.	Access Control / IAM Policy
5.4	Management responsibilities	A	Management responsibilities for information security are set out in policy and apply to all staff.	Information Security Policy

Control	Title	Decision	Justification	Implementing Document
5.5	Contact with authorities	NA	No confidential or regulated personal data is stored within the defined ISMS scope.	N/A
5.6	Contact with special interest groups	NA	Out of scope for current organizational needs.	N/A
5.7	Threat intelligence	NA	Out of scope at the current stage of ISMS maturity.	N/A
5.8	Information security in project management	NA	No formal project management function exists in scope at this time.	N/A
5.9	Inventory of information and other associated assets	A	An asset inventory is required to support risk assessment and ownership.	Asset Management and Data Classification Policy
5.10	Acceptable use of information and other associated assets	A	Protects information assets from leakage and is best practice for the application.	Acceptable Use Policy
5.11 (J)	Return of assets	A	Judgment completed for this report. Offboarded employees and contractors must return devices and revoke credentials to prevent retained access to the source code repository and production environment.	Asset Management and Data Classification Policy / HR Offboarding Procedure
5.12	Classification of information	A	Assets in scope require classification anchored to the CIA triad.	Asset Management and Data Classification Policy
5.13	Labelling of information	A	Logical labelling of assets in scope is required to enforce classification.	Asset Management and Data Classification Policy
5.14	Information transfer	A	Transfer of information is governed alongside classification and labelling.	Asset Management and Data Classification Policy
5.15	Access control	A	Access governance is required for the source code repository, production environment, and data.	Access Control / IAM Policy
5.16	Identity management	A	Identity governance is required to support access control.	Access Control / IAM Policy
5.17	Authentication information	A	Authentication governance is required to support secure access.	Access Control / IAM Policy
5.18	Access rights	A	Access rights governance is required, including provisioning and de-provisioning.	Access Control / IAM Policy
5.19 (J)	Information security in supplier relationships	A	Judgment completed for this report. AWS and any future service providers are suppliers whose security posture affects the ISMS and must be governed by policy.	Supplier Management Procedure / AWS Agreement
5.20	Addressing information security within supplier agreements	A	AWS is a supplier; the agreement with AWS must address information security obligations.	AWS Supplier Agreement

Control	Title	Decision	Justification	Implementing Document
5.21	Managing information security in the ICT supply chain	A (partial)	Applies to the AWS ICT supply chain; no physical product supply chain exists in scope.	Supplier Management Record
5.22	Monitoring, review and change management of supplier services	A (partial)	Judgment call under the AWS shared-responsibility model: AWS manages the infrastructure layer and Stark Industries manages configuration. This boundary should be documented explicitly and reviewed periodically rather than treated as full independent oversight.	Supplier Oversight Record
5.23	Information security for use of cloud services	A	The SaaS platform runs entirely on AWS cloud infrastructure.	Cloud Services Policy
5.24	Information security incident management planning and preparation	A	An incident response capability is required for the production environment.	Incident Management Policy
5.25	Assessment and decision on information security events	A	In scope and governed by the incident management policy.	Incident Management Policy
5.26	Response to information security incidents	A	In scope and governed by the incident management policy.	Incident Management Policy
5.27	Learning from information security incidents	A	In scope and governed by the incident management policy.	Incident Management Policy
5.28	Collection of evidence	A	In scope and governed by the incident management policy.	Incident Management Policy
5.29 (J)	Information security during disruption	A	Judgment completed for this report. Minimum security controls, particularly around access and logging, must be preserved even while the organization is responding to a disruption to production availability.	Business Continuity and Disaster Recovery Policy
5.30	ICT readiness for business continuity	A	The application must remain available to customers, so ICT continuity planning is required.	Business Continuity and Disaster Recovery Policy
5.31	Legal, statutory, regulatory and contractual requirements	A	No sector-specific privacy statute applies at this scale, but customer and supplier contractual obligations must still be tracked.	Compliance Register
5.32	Intellectual property rights	NA	Out of scope for the current ISMS scope statement.	N/A
5.33	Protection of records	NA	Out of scope for the current ISMS scope statement.	N/A
5.34 (J)	Privacy and protection of personally	NA	Judgment completed for this report. The platform processes publicly available marketing data rather than customer PII within the defined scope. This exclusion	N/A

Control	Title	Decision	Justification	Implementing Document
	identifiable information (PII)		should be revisited immediately if the scope expands to include personal data.	
5.35	Independent review of information security	A	Internal audits, and potentially independent penetration tests, are required to validate the ISMS.	Internal Audit Programme
5.36 (J)	Compliance with policies, rules and standards for information security	A	Judgment completed for this report. Follows directly from 5.35; internal audit and compliance monitoring must confirm that staff and systems operate within approved ISMS policy.	Internal Audit Programme
5.37	Documented operating procedures	NA	No mature business-as-usual operating procedures exist for this application yet.	N/A

7.2 People Controls (A.6.1–A.6.8)

Control	Title	Decision	Justification	Implementing Document
6.1	Screening	A	Hiring without screening creates exposure to data theft or unethical conduct; the HR screening policy provides evidence.	HR Screening Policy
6.2	Terms and conditions of employment	A	Security responsibilities are embedded directly in employment terms.	Employment Contract Template
6.3	Information security awareness, education and training	A	An effective ISMS depends on every staff member understanding and accepting the policy; this is treated as a core control.	Security Awareness Training Programme
6.4–6.8	Disciplinary process; post-employment responsibilities; confidentiality agreements; remote working; event reporting	A (group)	Treated as broadly necessary to protect confidentiality, integrity, and availability. Most of these are already performed through standard HR practice; each should still be individually confirmed and evidenced.	HR Policy Suite

7.3 Physical Controls (A.7.1–A.7.14)

Control	Title	Decision	Justification	Implementing Document
7.1–7.14 (all)	Physical security controls (all 14 controls in the 2022 catalogue)	NA	The ISMS scope excludes physical office buildings and CCTV. Physical security of the hosting environment is handled by AWS at the infrastructure layer under the shared-responsibility model.	N/A

All fourteen physical controls are excluded as a group because Stark Industries operates on cloud infrastructure and has no in-scope office facility to secure directly. This is a single, defensible scoping judgment rather than fourteen independent decisions, and it should be revisited if the organization ever takes on physical premises within the ISMS scope.

7.4 Technological Controls (A.8.1–A.8.34)

Control	Title	Decision	Justification	Implementing Document
8.1	User endpoint devices	A	Protects the developer laptop against malware and unauthorized use.	Endpoint Security Standard
8.2	Privileged access rights	A	Controls privileged access to production and the source code repository.	Access Control / IAM Policy
8.3	Information access restriction	A	Restricts access to information and source code to authorized personnel.	Access Control / IAM Policy
8.4	Access to source code	A	Directly protects the source code repository identified as a critical asset.	Access Control / IAM Policy
8.5	Secure authentication	A	Strong authentication is required across production and repository access.	Access Control / IAM Policy
8.6	Capacity management	A	Handled through standard infrastructure engineering practice.	Infrastructure Operations Procedure
8.7	Protection against malware	A	Endpoint and system malware protection reduces likelihood on the developer laptop and production risks.	Endpoint Security Standard
8.8	Management of technical vulnerabilities	A	Vulnerability management is explicitly in scope and tied to an ISMS objective.	Vulnerability Management Procedure
8.9	Configuration management	A	Secure configuration of the AWS production environment addresses the misconfiguration vulnerability identified in R2.	Cloud Configuration Standard
8.10	Information deletion	A	Controlled deletion of data is in scope, particularly for the data asset.	Data Retention and Deletion Procedure
8.11	Data masking	NA	Out of scope; no production data is currently masked for non-production use cases.	N/A
8.12	Data leakage prevention	NA	Out of scope at the current stage of ISMS maturity.	N/A
8.13 (J)	Information backup	A	Judgment completed for this report. The risk treatment for R2 and R5 explicitly relies on reliable backups to reduce impact; this control cannot be excluded once that reliance exists.	Backup and Recovery Procedure
8.14	Redundancy of information processing facilities	A	Supports availability of the production service for customers.	Business Continuity and Disaster Recovery Policy
8.15	Logging	A	Logging is required for monitoring and post-incident investigation across R1, R2, and R3.	Logging and Monitoring Standard
8.16	Monitoring activities	A	Continuous monitoring is required to detect the threats identified in the risk assessment.	Logging and Monitoring Standard
8.17	Clock synchronization	A	Handled by default through standard infrastructure configuration.	Infrastructure Operations Procedure
8.18	Use of privileged utility programs	NA	Not applicable to the current technology stack.	N/A
8.19	Installation of software on operational systems	A	Restricts unauthorized software installation on the production environment.	Cloud Configuration Standard

Control	Title	Decision	Justification	Implementing Document
8.20	Networks security	A	Secures the network layer supporting the production environment.	Network Security Standard
8.21	Security of network services	A	Secures network services consumed by the platform.	Network Security Standard
8.22	Segregation of networks	A	Network segregation limits the blast radius of a production compromise.	Network Security Standard
8.23 (J)	Web filtering	NA	Judgment completed for this report. At this organization's size, this exposure is addressed through endpoint malware protection (8.7) and security awareness training (6.3) rather than a dedicated filtering control.	N/A
8.24	Use of cryptography	A	Encryption is required to protect source code, production data, and the data asset.	Cryptographic Controls Standard
8.25	Secure development life cycle	A	Critical control to avoid releasing a vulnerable application; directly treats R3.	Secure Development Lifecycle Policy
8.26	Application security requirements	A	Application security requirements are critical given the platform is customer-facing.	Secure Development Lifecycle Policy
8.27 (J)	Secure system architecture and engineering principles	A	Judgment completed for this report. Follows directly from the applicable secure development controls (8.25, 8.26, 8.28); architecture principles should govern how the platform and its AWS infrastructure are designed.	Secure Development Lifecycle Policy
8.28	Secure coding	A	Secure coding practices are required and directly treat R3.	Secure Development Lifecycle Policy
8.29 (J)	Security testing in development and acceptance	A	Judgment completed for this report. Ties directly to the ISMS objective committing to application penetration testing and remediation of findings.	Secure Development Lifecycle Policy / Penetration Testing Procedure
8.30 (J)	Outsourced development	NA	Judgment completed for this report. Development is performed in-house by Stark Industries' own engineering staff; no outsourced development exists within the current scope.	N/A
8.31	Separation of development, test and production environments	A	Standard best practice and directly treats R3.	Secure Development Lifecycle Policy
8.32	Change management	NA	Out of scope for the current, small-scale ISMS implementation.	N/A
8.33 (J)	Test information	A (partial)	Judgment completed for this report. Test and staging environments must not use unmasked production data, consistent with the separation of environments control (8.31).	Secure Development Lifecycle Policy
8.34	Protection of information systems during audit testing	A	Both internal and external audits are anticipated for certification.	Internal Audit Programme

8. Residual Risk Summary and Management Approval

The table below compares initial and residual risk across all five scenarios, giving management a single view of the assessment's outcome.

Risk ID	Initial score / level	Residual score / level	Change
R1	16 / High	6 / Low	Reduced two levels
R2	15 / High	8 / Medium	Reduced one level; retained for monitoring
R3	16 / High	6 / Low	Reduced two levels
R4	12 / Medium	2 / Low	Reduced one level
R5	12 / Medium	6 / Low	Reduced one level

Approval record (to be completed upon management review):

Role	Name	Signature	Date
Risk owner – R1, R3			
Risk owner – R2, R4			
Risk owner – R5			
Information Security Manager			
Chief Executive Officer			

9. Conclusion and Recommendations

This assessment demonstrates that a small SaaS organization can build a complete, defensible risk assessment, treatment plan, and Statement of Applicability under ISO/IEC 27001:2022 without disproportionate cost or complexity. Five assets produced five risk scenarios; each was traced through scoring, treatment, control selection, and residual re-scoring, with every control decision in the Statement of Applicability justified and, where applicable, traced back to a specific identified risk.

Three recommendations follow from this exercise. First, Stark Industries should formalize the AWS shared-responsibility boundary in writing (control 5.22), since that boundary currently rests on an implicit understanding rather than a documented agreement, and auditors will ask for it explicitly. Second, the organization should revisit control 5.34 (privacy and protection of PII) immediately if its data processing ever expands beyond publicly available marketing data, since that would change several other decisions in this report as well. Third, the residual Medium-level risk on R2 should be reviewed at every management review under Clause 9.3 rather than treated as a one-time decision, since production availability risk in a cloud environment tends to shift as the platform's architecture and traffic evolve.

Taken together, the risk register, the treatment plan, and the Statement of Applicability in this report form the core evidentiary chain that an internal or external auditor would expect to see when validating conformance with Clauses 6.1.2 and 6.1.3 of ISO/IEC 27001:2022.

Appendix A: Glossary of Key Terms

Term	Definition
Annex A	The reference catalogue of 93 controls, organized into four themes, in ISO/IEC 27001:2022. Controls are selected according to identified risk, not implemented as a blanket set.
CIA triad	Confidentiality, integrity, and availability: the three properties an ISMS protects, and the basis for risk identification under Clause 6.1.2.
ISMS	Information Security Management System: the governance framework of policies, processes, and controls that manages information security within a defined scope.
Mandatory by implication	A document not explicitly named as mandatory by the standard, but which a mandatory process depends on, making it effectively required to reach certification.
Residual risk	The risk that remains after controls are applied. Calculated during treatment (Clause 6.1.3), not during the initial assessment (Clause 6.1.2).
Risk acceptance criteria	The conditions under which a risk is tolerated without further treatment; a management decision, not an analyst decision.
Risk appetite	The level of risk an organization is willing to tolerate in pursuit of its objectives, expressed operationally through its risk acceptance criteria.
Risk owner	The individual with the authority and accountability to manage a specific risk, required under Clause 6.1.2.
Statement of Applicability (SoA)	The mandatory document required by Clause 6.1.3 that declares which Annex A controls apply, with justification for every inclusion and exclusion, and that must trace back to the risk assessment.

References

CertiKit. (2025). ISO 27001 Statement of Applicability: A practical guide. https://www.certikit.com/

CertPro. (2026). Understanding the Statement of Applicability in ISO 27001:2022. https://certpro.com/

CyberZoni. (2025). ISO 27001 Clause 6: Risk management, objectives and changes. https://cyberzoni.com/standards/iso-27001/clause-6/

Drata. (2025). ISO 27001:2022 example ISMS plan. https://help.drata.com/en/articles/7208186-iso-27001-2022-example-isms-plan

Elevate. (2026). ISO 27001:2022 Annex A controls overview. https://elevatesecurity.com/

ForensicSpot. (2026). ISO/IEC 27001 clause structure and requirements. https://forensicspot.com/topics/information-security-audit-and-compliance/iso-27001-standard-and-structure

GlocertInternational. (2026). The Statement of Applicability under ISO/IEC 27001:2022. https://www.glocertinternational.com/

GRC Solutions. (2026). ISO 27001:2022 Clause 6: What's changed and what you need to do about it. https://grcsolutions.io/iso-270012022-clause-6-whats-changed-and-what-you-need-to-do-about-it/

High Table. (2022). ISO 27001 Clause 6.1.1 planning general. https://hightable.io/iso-27001-clause-6-1-1-planning-general/

High Table. (2026). How to implement ISO 27001 Clause 6.1.2 and pass the audit. https://hightable.io/iso-27001-clause-6-1-2-information-security-risk-assessment-guide/

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

iseoblue. (2025). Exploring the clauses of ISO 27001. https://www.iseoblue.com/post/exploring-the-clauses-of-iso-27001

iseoblue. (2026). ISO 27001 Clause 6 explained: Planning, risk assessment and treatment. https://iseoblue.com/iso-27001/clauses/clause-6/