Service Definition Document: IT Security

1. Overview

This document defines the IT Security Services offered to organizations seeking to safeguard their digital assets, systems, networks, and data. These services act as comprehensive protective measures against cyber threats, unauthorized access, and potential breaches. By functioning as virtual bodyguards, they encompass a range of solutions including firewalls, continuous monitoring, risk assessments, incident response, and employee training. The primary goals are to ensure secure operations, regulatory compliance, and the maintenance of customer trust. These services are designed to align with leading standards such as ISO 27001:2022 and integrate best practices from various cyber security frameworks to provide robust, compliant protection.

2. Service Description

IT Security Services provide professional, end-to-end solutions designed to protect an organization's critical digital infrastructure. These services are tailored to address evolving cyber risks in a proactive and strategic manner, incorporating controls and requirements from ISO 27001:2022 for information security management systems (ISMS). Key components include:

- **Firewalls and Access Controls**: Barriers to prevent unauthorized entry into networks and systems, aligned with ISO 27001 Annex A technological controls.
- **Monitoring and Surveillance**: Real-time oversight to detect anomalies and threats, supporting logging and monitoring requirements.
- **Risk Assessments**: Systematic evaluations to identify potential vulnerabilities, in line with organizational and threat intelligence controls.
- **Incident Response**: Rapid protocols for handling breaches and minimizing damage, following structured incident management processes.
- **Training and Awareness**: Programs to educate staff on security best practices, corresponding to people controls in ISO 27001.

These elements work together to create a resilient security posture, enabling organizations to operate confidently in a digital landscape fraught with challenges while achieving compliance with international standards and frameworks.

3. Service Features

The following features outline the core capabilities of the IT Security Services, enhanced to support ISO 27001:2022 compliance:

- **Tailored Security Strategy Development**: Customized strategies that align with the organization's unique needs and goals, incorporating ISO 27001 policies for information security.
- **Proactive Threat Assessment**: Ongoing evaluation of emerging threats to stay ahead of potential risks, including threat intelligence (Annex A 5.7).
- **Vulnerability Identification and Prioritisation**: Scanning and ranking vulnerabilities based on severity and impact, aligned with management of technical vulnerabilities (Annex A 8.8).

- **Customised Risk Mitigation Plans**: Personalized plans to address identified risks with targeted actions, supporting risk assessment and mitigation controls.
- **Integrated Security Architecture**: Holistic design that incorporates security into all layers of IT infrastructure, following secure system architecture principles (Annex A 8.27).
- **Principle-Based System Design**: Adherence to foundational security principles such as least privilege and defense in depth, integrated with ISO 27001 requirements.
- **Efficient Incident Detection Protocols**: Advanced tools and processes for quick threat identification, in line with monitoring activities (Annex A 8.16).
- **Structured Response and Recovery Processes**: Defined workflows for incident handling, containment, and restoration, including ICT readiness for business continuity (Annex A 5.30).
- **Independent Control Evaluations**: Objective assessments of existing security controls, supporting independent review of information security (Annex A 5.35).
- **Embedded Vulnerability Testing in Development**: Integration of security testing into the software development lifecycle (e.g., DevSecOps), aligned with security testing in development (Annex A 8.29).
-

4. Service Benefits

Engaging with IT Security Services delivers tangible advantages to organizations, enhancing their overall security and operational efficiency while facilitating compliance with ISO 27001:2022 and other frameworks.

The key benefits include:

- **Strategy Planning**: Develops tailored plans that align security measures with business objectives, ensuring long-term resilience and ISMS compliance.
- **Threat Assessment**: Identifies potential risks early, allowing for preventive actions before issues escalate, in accordance with threat intelligence controls.
- **Risk Identification**: Pinpoints vulnerabilities across operations, minimizing financial impacts and operational disruptions through prioritized vulnerability management.
- **Risk Mitigation**: Implements robust controls and continuous monitoring to reduce exposure to threats, supporting Annex A organizational controls.
- **Robust System Architecture**: Integrates security principles like encryption, authentication, and segmentation for fortified protection (e.g., Annex A 8.24 Use of cryptography).
- **User-Centric Security Design**: Balances strong protection with usability, improving operational efficiency without hindering productivity, aligned with people controls.
- **Incident Detection and Response**: Utilizes structured frameworks for quick containment and resolution of security incidents, including learning from incidents (Annex A 5.27).
- **Post-Incident Analysis and Improvement**: Conducts thorough forensics and lessons-learned sessions to refine future security practices, with evidence collection (Annex A 5.28).
- **Independent Security Audits**: Evaluates controls objectively, identifies gaps, and recommends enhancements for compliance and effectiveness, per Annex A 5.36.
-

5. Alignment with ISO 27001:2022 Standards and Controls, Including Cyber Security Frameworks

Our IT Security Services are fully aligned with ISO/IEC 27001:2022, the international standard for information security management systems (ISMS). This alignment ensures that organizations can achieve certification or maintain compliance by implementing the standard's requirements, including the 93 controls outlined in Annex A. These controls are grouped into four themes: Organisational (37 controls), People (8 controls), Physical (14 controls), and Technological (34 controls). Below is a structured summary of the Annex A controls, with services designed to support implementation in each area:

Organisational Controls (Annex A 5)

Focus on policies, roles, asset management, supplier relationships, incident management, and compliance.

People Controls (Annex A 6)

Address human factors such as screening, training, and remote work security.

Physical Controls (Annex A 7)

Cover physical security measures to protect facilities and equipment.

Technological Controls (Annex A 8)

Focus on technical safeguards like malware protection, backups, and network security. 8.29 Security testing in development and acceptance. In addition to ISO 27001:2022, our services incorporate best practices from other leading cyber security frameworks to provide comprehensive coverage.

These include:

- **NIST Cybersecurity Framework (CSF)**: A voluntary framework for managing cybersecurity risk, which complements ISO 27001 by focusing on identify, protect, detect, respond, and recover functions.
- **CIS Critical Security Controls**: A prioritized set of actions to defend against common cyber threats, aligning with ISO 27001's technological and organizational controls.
- **SOC 2**: Focuses on service organization controls for security, availability, processing integrity, confidentiality, and privacy.
- **COBIT**: Provides governance and management practices for IT, integrating with ISO 27001 for enterprise-wide alignment.
- **PCI DSS**: For payment card security, which can be mapped to relevant ISO controls for data protection.
- **HITRUST Common Security Framework (CSF)**: Consolidates controls from multiple standards, including ISO 27001, for healthcare and beyond.
- **HIPAA**: Health Insurance Portability and Accountability Act, aligning with privacy and protection controls in ISO 27001.

By leveraging these frameworks, our services ensure a multi-layered approach to cyber security, adaptable to various industry needs and regulatory requirements.

6. Scope and Exclusions

- **In Scope**: All features and benefits listed above, delivered through consulting, implementation, and ongoing support, including assistance with ISO 27001:2022 certification audits.

- **Out of Scope**: Physical security measures, hardware procurement (unless specified), or legal advice on compliance issues. Custom extensions can be discussed as add-ons.

7. Delivery Model

Services are delivered via a combination of on-site consultations, remote monitoring, and cloud-based tools. Engagement typically begins with an initial assessment, followed by strategy development, implementation, and maintenance phases. Pricing and timelines are determined based on organizational size, complexity, and specific requirements, with options for framework-specific alignments.