ATECH IOMART

Service Definition Document

Cyber Security Risk Assessment

Contents

Solution Overview

Aims and Objectives

Addressing modern and rapidly evolving security concerns requires a comprehensive approach, including employee training, strong password policies, regular software updates and patching, network security measures, data backups, incident response plans, and ongoing monitoring and risk assessment. Collaborating with managed security service providers (MSSPs) or outsourcing security functions can also help organisations enhance their cybersecurity posture.

To identify the key risks to an organisation and help improve their cyber posture, Iomart and Reliance Cyber has an established solution designed specifically for small to medium sized enterprises.

The Cyber Risk Assessment contains several steps which rapidly assesses the target organisation and provides practical insight and a series of actionable, risk-based recommendations that can be implemented by the organisation or with help from a security specialist, such as Iomart.

Cyber Risk Assessment Description

Kick-off Meeting

- Establish a shared understanding of the project's objectives, scope, timeline, and deliverables. Gain an understanding of company structure and key cyber and strategic business risks.
- All parties establish a strong foundation for the project and a schedule is agreed.

Documentation Review

- Assess the effectiveness and scope of various documents, policies, procedures, guidelines, and standards related to cyber security within the organisation.
- Describe high level opportunities for improvement and future areas to focus on.

Threat Assessment

- An analysis of potential threats that are likely to target an organisation like the client and would realise their key risks.
- This is performed in conjunction with an architecture overview with the client.
- The output is a discreet report section and context for the other sections.

Tabletop Cyber Crisis Exercise

- A simulated scenario-based activity designed to assess and enhance an organisation's preparedness and response capabilities to cyber security incidents - bringing together key stakeholders from IT, security, and the wider business.
- A valuable opportunity to test incident response capabilities in a controlled, simulated, and safe environment. Fosters collaboration and critical thinking to enhance preparedness and response effectiveness.

Technical Exercise & Report Contribution

- A sample of penetration testing activities to look for themes and common root causes of technical risk within the environment.
- By identifying broad themes of technical risk within the client's environment a triangulation can be made between risk and observable vulnerability.

Final Report

- Provides an overview of the findings, analysis, and recommendations resulting from each activity stream.
- Communicates the assessment results to relevant stakeholders, including management, IT teams.
- Recommendations provided are risk based, prioritised, and aligned to a client remediation roadmap.

Presentation to Client

- The final presentation to the client provides valuable insights to the organisation's security strengths, weaknesses, and areas for improvement. Presenting this to key management helps capture buy in and appetite for improving.
- This serves as a foundation for making informed decisions regarding key areas for resource allocation, security investments, and prioritising efforts to enhance the organisation's overall cyber security posture.

What is Cyber Risk Assessment

The primary objective of the Cyber Risk Assessment is to safeguard your business operations, data, and reputation against evolving cyber threats. Given the rapidly evolving threat landscape it is now imperative to maintain the highest standards of cybersecurity to protect sensitive information. By conducting this assessment, Iomart will seek to:

- **Identify Vulnerabilities:** Identify and prioritise potential weaknesses and vulnerabilities within our IT infrastructure, networks, and systems that could be exploited by malicious actors.
- **Assess Threats:** Evaluate the likelihood and potential impact of various cyber threats, including data breaches, malware attacks, phishing attempts, and other forms of cybercrime targeting your organisation and its stakeholders.
- **Enhance Security Measures:** Develop and implement robust security controls, policies, and procedures to mitigate identified risks and strengthen our overall cyber resilience posture.
- **Ensure Regulatory Compliance:** Ensure compliance with relevant data protection regulations and industry standards, such as GDPR, CCPA, and ISO 27001, to maintain trust and confidence among our customers and regulatory authorities.

Key Components of the Assessment

The Cyber Risk Assessment will encompass a comprehensive review, including.

- Data Protection Practices: Evaluate the effectiveness of your data encryption, access controls, and data retention policies to safeguard sensitive information from unauthorised access or disclosure.
- Incident Response Plan: Review incident response procedures and protocols to ensure readiness to detect, respond to, and recover from cyber incidents in a timely and effective manner.
- Employee Training and Awareness: Assess the adequacy of current cybersecurity training programs to educate employees about cyber threats, best practices, and their roles and responsibilities in maintaining a secure work environment.
- IT Infrastructure: Targeted assessments to investigate the security of networks, servers, endpoints, and cloud-based services to identify potential vulnerabilities and misconfigurations[1].

In conclusion, the Cyber Risk Assessment is a proactive measure to strengthen your cybersecurity defences and uphold the commitment to providing a safe and trusted online experience for users. By identifying and mitigating potential cyber risks, Iomart aims to help mitigate financial losses, protect brand reputation, and preserve the trust and confidence of customers and stakeholders.

[1] This is a sample of penetration testing activities to look for themes and common root causes of technical risk. This is not a comprehensive fully scoped platform penetration testing exercise. This would require scoping and pricing, handled via a separate engagement.

Key Features

- Identify vulnerabilities that could be exploited by malicious actors
- Model and assess threats, evaluating likelihood and impact
- Develop and implement robust security controls
- Review compliance with relevant data protection regulations and standards
- Review incident response ensuring readiness to detect, respond, recover
- Assess adequacy of cyber security training programs to educate employees
- Includes targeted assessment of infrastructure to identify vulnerabilities and mis-configurations
- Recommending risk mitigation strategies, remediation plans and control enhancements
- Comprehensive reporting of findings, risks, and recommended actions
- Recommendations including prioritised investment road-map and strategy

Key Benefits

- Identify vulnerabilities before they can be exploited by cyber threats
- Gain clear understanding of most critical risks facing your organisation
- Enhance security posture with actionable intelligence to strengthen security controls
- Ensure compliance with relevant industry regulations and standards
- Safeguard critical assets including data, intellectual property and customer information
- Mitigate threats disrupting operations, damaging reputation, resulting in financial loss
- Develop a proactive approach and cyber resilient operation
- Provide stakeholders with comprehensive risk information supporting decision-making
- Evaluate cyber security risks posed by third parties and suppliers
- Establish ongoing risk motioning and assessment enabling continuous improvement

Planning Activities

Meeting	Threat Assessment	Tabletop Exercise	Technical Exercise
Purpose	A systematic evaluation and analysis of potential threats and vulnerabilities that could compromise the security of an organisation's information systems, data, networks, and technology infrastructure.	A simulated scenario-based activity designed to assess and enhance an organisation's preparedness and response capabilities to cyber security incidents - bringing together key stakeholders from IT, security, business, etc.	A sample of penetration testing activities to look for themes and common root causes of technical risk within the environment.
Duration	2 hours contact. A guided online workshop conducted by Threat Intelligence specialists.	3 hours contact. Cyber simulation exercise conducted remotely involving business and IT experts.	No mandated contact.
Client Attendees	Business asset owners who can provide details on business context and 'crown jewels;' technology experts who can describe technical landscape and deployed controls.	Business and technical leaders who would be responsible for making critical decisions in the event of a significant cyber incident.	A point of contact should be available to support if needed, this would usually be someone from the IT team.
Outputs and Outcomes	Identification of potential risks; outputs inform the tabletop exercise and final report.	Highlights and recommendations from the exercise form key element of the final report to help embed cyber resilience.	A technical section integrated into the main report.

Scope and Duration

It is anticipated that on commencement of the risk assessment, it will take approximately 4 weeks of elapsed time to complete each of the component pillars, develop report and present.

Deliverables

The deliverable for the cyber risk assessment is the performance of the necessary consulting services along with a final written risk assessment report.

Key Outcomes

- Business-led, rather than technology focused.
- Engagement from top level management in exercises.
- Minimal overhead due to experienced project planning and experienced consultants delivering each workshop.
- Helps solve client problems rather than impose solutions.
- Prioritised roadmap informs next steps leading to follow on work to mitigate residual risk.

Assumptions and Pre-requisites

Assumptions

No.	Assumption
1.	All relevant staff are available for calls, meetings, document reviews and workshops (if applicable).
2.	Access to relevant systems is available upon commencement of any work.
3.	Any standards, documentation templates, security policies etc. to be provided to Iomart in advance of the engagement commencing.

Pre-requisites & Engagement Activities

No.	Prerequisite
1.	**It will be necessary for to provide the following in advance of any testing:** • Contact details of personnel to provide support and to resolve any issues with the system(s) under test, should any arise. • IP addresses and hostnames of the targets • Any documents, network Architecture or design details if available. • User credentials for testing the application at each level of authority. Two users at each level per tester. • URLs and other details necessary to reach the targeted application(s). • Whitelisting or similar mechanism to facilitate remote testing of attack IPs.

Data Protection & GDPR

Atech, part of the Iomart Group, is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. Our Data Protection policy sets forth the expected behaviours of Iomart Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to an Iomart Contact (i.e. the Data Subject). Iomart, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in our Data Protection policy (available on request).

Iomart's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Iomart Employees and Third Parties to share in this commitment.

Iomart uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of Iomart Entities.
- To provide services to Iomart customers.
- The ongoing administration and management of customer services.
- The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

Each Iomart Entity will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Iomart will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the Data Subject prior to entering a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party.

Why Partner with Atech?

Credentials and Capability

Atech is the one of the UK's most accredited providers of secure hybrid cloud managed services, delivering deep expertise across Microsoft technologies, data protection, and cybersecurity. We hold Microsoft designations for **Modern Work, Security, Infrastructure (Azure)** and are recognised as an **Azure Expert MSP** - a status achieved by only 60 partners globally and 15 in the UK.

As part of the Microsoft AI Cloud Partner Program, we have validated technical capabilities across the full cloud lifecycle. Our inclusion in the **Azure Expert MSP Program** reflects proven excellence in people, processes, and tools, ensuring sustainable, repeatable, and scalable managed services. This means you can rely on a partner that consistently delivers best practice and operational efficiency.

Partnering with us gives you access to over **200 Microsoft cloud specialists**, including **two Microsoft MVPs**, ensuring unparalleled technical depth and experience.

Microsoft Endorsements and Specialisations

We hold multiple Microsoft Solutions Partner designations, including:

- Digital & App Innovation (Azure)
- Data & AI (Azure)
- Business Applications

Figure 1: Microsoft Accreditations

In addition, we have achieved advanced specialisations in areas such as:

- Cloud Security
- Identity and Access Management
- Threat Protection
- Infra & Database Migration
- Azure Virtual Desktop
- Enterprise Application Migration to Azure

Figure 2: Microsoft Designations

These credentials validate our ability to deliver complex, secure, and innovative solutions aligned to Microsoft best practices.

Security and Compliance

Security is at the heart of our services. Atech is **ISO 27001 certified, Cyber Essentials Plus accredited**, and a member of the **Microsoft Intelligent Security Association (MISA)** – an invitation-only program granting access to Microsoft's top security experts. We also hold **CREST accreditation** and participate in the **Microsoft MSSP Program**, one of only 12 partners in the UK, giving our customers direct benefits such as access to product teams and funded workshops.

Further reinforcing our security leadership:

- **Microsoft Gold Partner Status** alongside **Azure Expert MSP**
- **Microsoft MSSP Program** (1 of only 12 UK partners)
- **Microsoft Fastrack Ready Partner** (1 of only 300 globally)
- **Microsoft XDR status**

These credentials provide you with assurance that security is embedded throughout design, migration, and ongoing management. Combined with our advanced specialisations and industry recognition, they demonstrate our ability to deliver secure, compliant, and future-ready solutions.


ATECH IOMART
6 Atlantic Quay, 55 Robertson Street, Glasgow, G2 8JD