avanade

G-Cloud 15

Lot 3 – Cloud Support Services (Additional Services)

Avanade Security Strategy & Transformation Services

Table of Contents

1. Scope of our services

Businesses are experiencing an increasing number of cyber security incidents and attacks; this figure has been rising year on year and shows no sign of slowing down. Heightened connectivity, flexible working, and the need for organisational change at pace have, in many instances, introduced new security pressure points and weaknesses to control environments.

To successfully address security concerns, it is imperative that organisations understand their People, Processes and Technology controls and address any gaps which fall outside of best practices and acceptable risk levels. Human beings remain the greatest weakness in the security landscape; because of this, training, awareness, governance, and logical controls should be designed to support employees whilst giving the organisation the best chance at security success.

The Cyber Security landscape is ever evolving and requires organisations to have a detailed understanding of their People, Processes and Technology to remain resilient, compliant, and effective in business. Malicious security activity has experienced an exponential rise over the past 12 months, and because of this, organisations must become more vigilant and secure than in previous years. Through understanding organisational strengths, weaknesses, risks, threats, control effectiveness and a realistic path to success, we help our clients carve out a journey to a more secure state.

In the current security landscape:

- 68% of business leaders feel their cybersecurity risks are increasing.
- 17% of all sensitive files are accessible to all employees.
- 50% of large enterprises (with over 10,000 employees) are spending $1 million or more annually on security, with 43% spending $250,000 to $999,999, and just 7% spending under $250,000.
- Remote workers have caused a security breach in 20% of organizations.

Our security advisory support clients to address security challenges faced by organisations today:

What does good look like?

- With such a range of available technology, controls and sector-specific requirements, how do we know what we are doing in the security space is appropriate and commensurate with the level of risk we face?

Are suppliers or M&A activities introducing unacceptable risk?

- Is our data, infrastructure, reputation and employees safe from attacks that could 'piggyback' on to supplier connections? Are the people we associate with as secure as they say they are?

We have documentation and processes in place but are they embedded and effective?

- We created some processes many years ago; others are newer, but how can we be sure they are well defined and actually uphold good security principles? Are our employees being directed in a suitable manner when it comes to our organisational guidance?

We do not know what we do not know

- There are some known areas for improvement across the organisation, but we need a security expert to highlight the things we have missed. What are the gaps in our security control environment?

What should years 1, 2 and 3 look like?

- We are committed to improving security but are fearful of coming off track. How can we get it the right first time and plan for the years ahead?

What specific security risks and threats are we facing?

- We know the general themes that are currently impacting organisations but what specifically should we be aware of that is either unique to us or more applicable to us?

What is our current security posture?

- How do we accurately define our current cyber security maturity across the organisation as a whole? We want to know how secure we are as a business rather than how specific technology is performing.

What do we address first, and why?

- How do we ensure we do not focus time and effort in the wrong areas, and how do we get comfort that investing in a given improvement initiative will give us the benefit we need?

2. Approach

Our Security Assessment and Strategy methodology can be adapted and directly aligned to meet numerous client security needs.

2.1. Engagement Initiation

Project and Delivery Management

We use a structured project and delivery management system, which sets the engagements up for success. The following items are fundamental aspects of this methodology:

- Agreement on the project scope, terms of reference, key objectives, dependencies and deliverables
- Agreement on reporting lines and project stakeholders from both Avanade and your organisation
- Agreement on the project timescales, including any mid-point reviews that may be required
- Agreement on secure data exchange and notification of any sensitive issues that we should be aware of ahead of delivery and employee interactions
- Confirmation of the employees, contractors, third parties and any other contacts who will be required to take part in the review, e.g., for specific control assessment workshops
- Information that can be requested and processed ahead of workshops and delivery dates is strived for to ensure efficient delivery. Examples of this include a pre-site documentation request list and workshop planner that can be completed collaboratively.

Client Organisation Context

To successfully assess your security landscape and advise on an appropriate and effective strategic roadmap, it is imperative that we understand the security context around your organisation. This focus on key drivers for change, organisational goals and current risk posture ensures our recommendations and guidance is aligned to your core values and business needs.

Some examples of discussion points which would be explored in a Context Discovery Workshop include:

- Current and future Security Goals
- Security incidents and near misses (Past or Present)
- Security culture and any risk and threat motivators – Environmental, reputation, political, employee familiarity with technology and security
- Technology overview: Headline critical systems, applications and overarching architecture
- Business overview: Business objectives, critical processes, business units and services

2.2. Strategic Business Impact Assessment (SBIA)

Understand Critical Information Assets from a Security Perspective

The Strategic Business Impact Assessment (SBIA) supports risk and threat management through identifying key information assets and classifying them in accordance with their sensitivity and security impact.

Ensure Business Drivers Feed into Strategy and Future Investment

By highlighting the security impacts of key systems, locations, hardware, software and supporting assets, it is possible to ensure future improvement initiatives protect these critical business items and promote security across operations.

SBIA Process

- Identify the high-level information assets that are critical to running the business (usually, approx. 20 items split across headline critical systems, services, physical locations and kit etc.)
- Confirm ownership, description, scope and operation details

- Define Confidentiality, Integrity and Availability scores for each critical asset to articulate the impact should a compromise of that nature take place.
- Validate scoring and outputs with business owners

SBIA Benefits

- Gain a strategic view of the security impact on critical assets
- Gain assurance that future security plans protect the 'Crown Jewels'

***Example SBIA Output**

#	Asset Name	Description	Confidentiality	Integrity	Availability
1	Document Management Application	The document management system houses key client, business and operational information. It was noted that IT configuration files, network diagrams and financials which would warrant high privileged access are stored here. MFA and consistent information classification, and subsequent protection, are not deployed consistently throughout this application.	**5 – Catastrophic**: Unauthorised exposure of a wide range of files in this application would result in significant legal, regulatory, reputational and financial damage. One of the highest impact scenarios was defined as client contract exposure.	**4 – Major**: Unauthorised alteration of files within this application could result is incorrect contractual terms, insecurely configured IT systems and notable impact to operations and project timelines.	**3 – Moderate**: The document management application is used for multiple day-to-day processes, but an outage could be sustained for 1-2 days before significant disruption and impact on customers would be realised.

2.3. Security Controls Review & Maturity Assessment

A True View of Organisational Security

We will conduct workshops with key stakeholders to review what security controls are in place and the extent to which they are defined, documented, automated and optimised. Through examining available supporting evidence and exploring control capabilities with client SMEs, we can define current maturity, highlight any gaps and formalise an appropriate target maturity. Target maturity definitions take into account your business aims, the risks and threats faced, security best practices and the organisational resource and appetite to improve.

A Tailored Approach Support by Security Best Practice

We typically deliver our control review using the NIST Cyber Security Framework, which is comprised of 108 controls spanning key security domains such as asset management, data security and incident response. Where clients are striving for ISO27001 certification in future or are already aligning to a different framework, such as CIS Top 20 Critical Security Controls, we are able to facilitate a control review using the desired framework to ensure outputs are best aligned to client plans. By following industry recognised standards, we can ensure we provide a rich picture of security as a whole rather than focusing on a single domain or problem area.

Control Review Benefits

- Highlight any gaps and weaknesses across the whole security landscape
- Gain assurance over alignment to industry recognised standards and best practice
- Understand current security posture and distance from an appropriate target maturity
- Have a security expert validate areas of good practice and investment

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS,MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 1

2.4. Cyber Risk & Threat Assessment

Your Personal Risk and Threat Landscape

Through analysis of your control environment, combined with open-source information gathering, we provide detail on the cyber security risks and threats you could potentially be vulnerable to. By mapping risks and threats back to the controlled assessment, we can confirm whether any existing control weaknesses exacerbate potential risks. The example to the right shows how Insider Threat capability is enhanced to a rating of 'High' due to a lack of appropriate logging and monitoring as well as overly broad access rights across the user base.

Cyber Security Risk and Threat Assessment Process

- Definition of a suite of headline cyber security risks, which are validated by exploring the potential impact of current security control weaknesses and areas for improvement
- Analysis of a range of Threat Actors, which includes an assessment of their capability, level of motivation and overall threat rating
- Key threats will include examples of likely attack paths and what assets could potentially be targeted

Control Review Benefits

- Understand what security risks and threats you are facing
- Gain oversight of which control weaknesses are contributing to what risks
- Gain assurance that recommendations from the Cyber Security Assessment support you in building resilience to the risks and threats you face

Threat Name	Capability	Motivation	Threat rating
Insider Threat	High	Medium	Likely

Figure 2

Risk	Key Validation(s)
The threat misuses access rights and their established relationship with your organisation's network, assets, and general information to disclose, modify or delete sensitive information or disrupt services. Successful insider threats can result in significant legal, regulatory, reputational and financial damage. Recent trends have shown an increase in employees being approached by organised crime groups to aid cyber-attacks for financial gain. Insider threats can be particularly difficulty to spot in a timely manner. To bolster security in this area, a combination of consistent procedures, training and awareness, robust logging and monitoring practices and DLP solutions are advised. It is important to note that insider threat compromises can come from accidental, negligent and malicious activity.	A large amount of Company X employees have either local administrator rights or overly broad access. This enables them to bypass security guidance such as the Acceptable Use Policy. Periodic testing, assurance activities or monitoring of physical security is not enforced. Furthermore, a strict visitor process is not in place. Logging and monitoring blind spots exist in the current control environment. On-prem infrastructure does not benefit from active monitoring.

2.5. Analysis, Reporting and Security Strategy

Analysis and Reporting

The final deliverable from the Avanade Security Assessment and Strategy is a robust report which explicitly defines your current security posture, noted weaknesses and prioritised recommendations to support your improvement initiatives. Key report sections include:

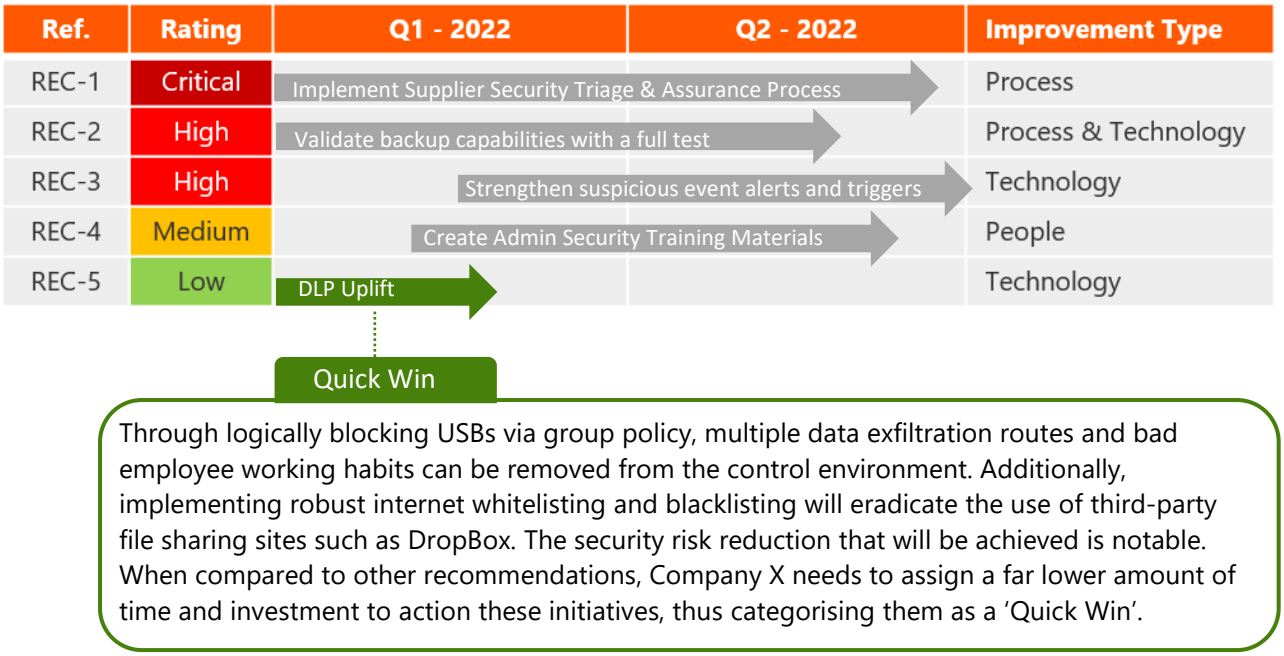
- Executive summary
- Detailed Findings – Context, SBIA, Risk and Threat Assessment, Control Assessment
- Prioritised Recommendations
- Strategic Roadmap
- Next Steps
- Appendices

Avanade Cyber Security Assessment and Strategy Report Benefits

- A consolidated view of your organisations security landscape which takes as input your critical information assets, control maturity, risks, threats, prioritised recommendations, and a strategy to a more secure organisation.
- A defined future state and target control maturity which is supported by best practices and a strategic roadmap.

Security Strategic Roadmap

- We will provide a recommended timeline of activity to transition your organisation from its current maturity to the proposed target state.
- We will define which risks and control gaps each recommendation addresses and highlight whether the change is aligned with People, Processes or Technology.
- You will be presented with any quick wins which are available to bolster security with lower time and resource investment compared to some larger recommended improvements.



2.6. Debrief and Next Steps

Project Debrief and Next Steps

Following the creation, issue and acceptance of the final deliverable (our branded report), the delivery lead will facilitate a project debrief which is suited to your specific needs. This can take place as but is not limited to a summary presentation to Senior Leadership or a detailed recommendation discussion with individual teams.

The purpose of the debrief is to ensure you feel supported in upcoming security decisions, and strategic direction and have another opportunity to ask any further questions that may have arisen.

Avanade will also define key next steps for your security journey, which will aid the successful navigation through upcoming recommendation remediation and security strategy progression.

Debrief and Next Steps Benefits

- The opportunity to discuss findings and recommendations to ensure all involved parties understand actions and rationale
- An entirely flexible format, in-person or remote, which can be tailored to specific stakeholder groups. E.g., Delivery of a presentation to Board and Project Sponsor to highlight key recommendations and immediate actions vs. line-by-line discussion of recommendations with management.
- A project concluding touchpoint to ensure you have the tools to succeed on your security journey.

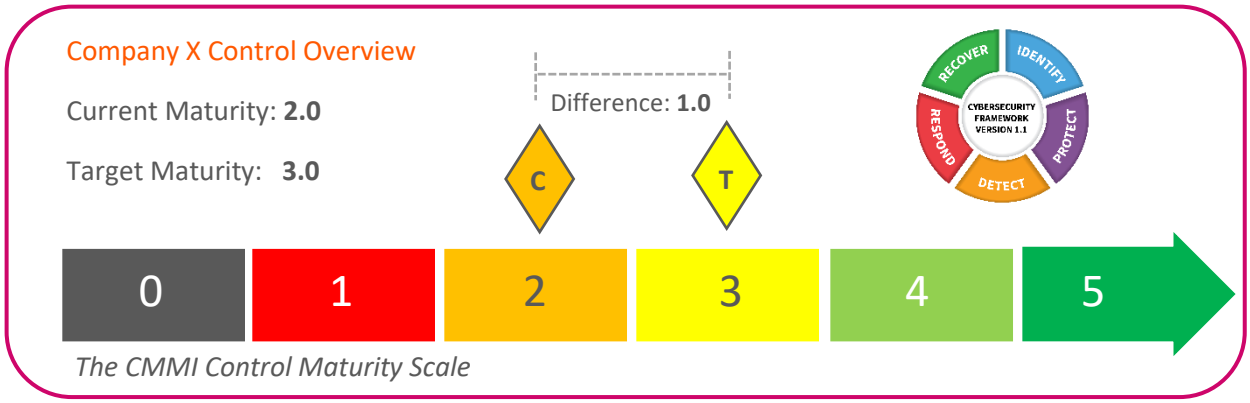


Figure 3

Delivery Flexibility to Support Your Needs

- Our Security Assessment and Strategy can be delivered in a format that is most suited to your current requirements. This can take place entirely remotely, via online workshops, using Microsoft Teams, or may include a mix of both on-site and remote working.
- The recent pandemic has forced a change in the way we work and our reliance on secure connectivity and technology. We recognise that the importance of certain controls and processes has dramatically increased recently and factor this into our review methodology. Topics such as remote access, home working environment, business continuity and incident response all receive appropriate representation in our assessment.
- Every organisation is different. As a result of this, we look at the security needs specific to you and tie them together into a personalised and cohesive improvement plan.

3. Assets and tools

Asset
Cyber security roadmap and strategy
Cyber security business impact assessment
Cyber security controls maturity framework
Cyber risk and threat profiles
Cyber security strategy and transformation report

4. Pricing

Please refer to the associated Pricing Document relevant to this Service.

5. Contacts

Sangeeta Pierce

Head of Avanade UK Health & Public Services

Email: uk.hps.support@avanade.com

Telephone: +44 20 7025 1000

6. About Avanade

Avanade, a joint venture between Accenture and Microsoft, is a privately held company was founded in 2000 with the goal of delivering innovative services and solutions to enterprises worldwide using the Microsoft platform. Avanade's main business focus is to purely deliver innovative services and solutions to enterprises worldwide on Microsoft technology. Avanade is a global organisation with over 56,000+ professionals worldwide, serving our clients in major geographic business areas in 26 countries.

This vast network of highly skilled resources is further complemented by our network of delivery centres that we refer to as Advanced Technology Centres (ATCs). This complementary capability provides the agility, cost efficiency and diversity of skills that today's businesses demand. This construct underpins the results we generate for our clients and forms the foundation for our long-term relationships with them.