savanti

Overview of Cyber Security Assessment Service

savanti

Background

Many organisations are required to perform or commission cyber security assessments. It might be to provide assurance to internal stakeholders; to meet external compliance; or to simply understand how effective their controls are and what to do next.

We know that some organisations who've been through this previously have been frustrated with the process, which can be slow and cumbersome, together with generic outputs, which lack practical next steps.

As a result, Savanti have developed a cyber security assessment service to provide a holistic view of maturity which considers the causes of incidents and the mitigating controls already in place, and provides meaningful reporting with practical improvement actions.

savanti

Introduction

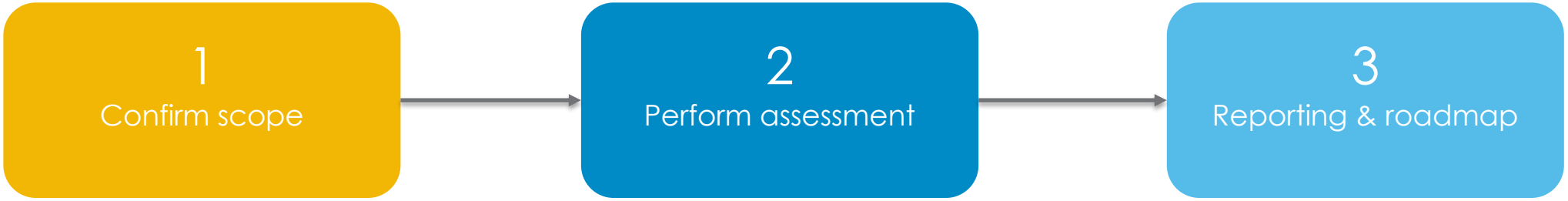
Our assessments are built around Savanti's Cyber Security Controls Framework which consists of 15 domains that cover the organisational and technical security requirements that make for good cyber security. The controls are not new but are grouped into:

- Coherent domains that reflect modern threats and the actual causes of incidents, to
- Provide a pragmatic model to implementing a strategic response to cyber risk.

Using our Framework we assess the key aspects of security risk to the information, systems and infrastructure in order to provide you with swift analysis of your cyber security maturity and help you shape your information security programme. Further information on the Framework is presented in the Appendix.

savanti

Typical approach



We will work with you to define and agree the scope of the assessment and understand any existing artefacts that can support the review.

We will perform the assessment against our cyber security framework to provide a holistic view of security risk and controls.

We will deliver our report and work with you to develop a pragmatic improvement roadmap for the accelerated reduction of security risk.

savanti

Example deliverables

Unless required, we don't produce long wordy reports. Instead, we believe it's important to provide senior stakeholders with the overall status and key actions to take; and empower responsible staff with the specific steps needed to improve security.

savanti

Executive summary – maturity dashboard

Your mean maturity score is

2

You have a **repeatable** cyber security control environment where controls are in place to some degree but are not all applied consistently.

Priority controls implemented

12 (out of 20)

that best mitigate the common causes of incidents.

savanti

3.1 Employee Security - Findings

Domain requirement: All staff are made aware of their responsibilities in securing information and the security threats relevant to their role and the organisation.

Control	Status	Control	Status
3.1.1 Background verification checks shall be carried out for all employment candidates in accordance with relevant laws, regulations and ethics and are proportionate to the information assets to be accessed. **(Priority control)**	✓	3.3.1 New joiner training must be completed prior to staff starting in role / within x days of starting in role.	✓
3.2.1 All staff and contractors are made aware of their information security responsibilities (including responsibilities valid after termination or change of employment) as part of a clear "joiners, movers and leavers" process.	×	3.3.2 All staff are provided with access to the organisation's information security communications, training material and tools as part of the onboarding process.	×
3.2.2 The contractual agreements with employees and contractors shall state their individual and the organisation's responsibilities for information security.	✓	3.4.1 Information security training courses and awareness campaigns are developed and delivered to all staff throughout the year.	✓
3.2.2 The contractual agreements with employees and contractors shall state their individual and the organisation's responsibilities for information security.	×	3.4.2 A schedule for the delivery of information security training and awareness campaigns is maintained.	×

Current maturity score

1

Desired maturity score

5

Priority controls

6 (out of 8)

savanti

3.2 Employee Security - Remediation Plan

Current score 1 → 12 month score 3 → Desired score 5

	0-6 months	6-12 months	12-24 months
Employee Security	**3.2.1** Ensure that staff information security responsibilities are included in employment contracts going forward. **(Quicker win)** **3.2.2** Implement induction training for newly onboarded employees and that they are made aware of relevant policies, processes and standards. **(Quicker win)**	**3.2.3** Put in place procedure for pre-employment screening, e.g. UK DBS check, for critical roles. **3.2.3** Implement an annual security awareness refresher for all staff. **3.2.4** Ensure that leavers processes include the return on equipment and the secure disposal or re-use of assets.	**3.2.5** Develop and implement an annual programme of continuous awareness raising and training to include: • Online training courses. • Simulated phishing campaigns. • Role-based training to provide specific information to key or high-risk staff. • Distribution of reinforcement collateral for key messages.

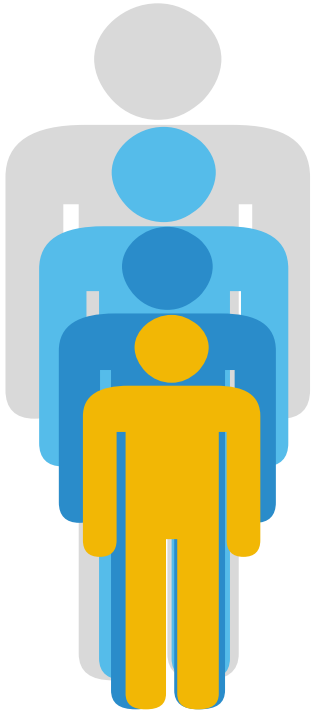
savanti

Engagement team

The engagement will be led by one of our experienced Senior Consultants who all have a proven track record in scoping, performing and reporting on cyber security assessments at a range of organisations.

The assessment will be performed by a delivery team made up of skilled consultants, who all have a blend of industry and consulting experience, to meet your specific requirements.

The team will draw on support of colleagues where needed and have access to the full Savanti knowledge base to accelerate delivery.

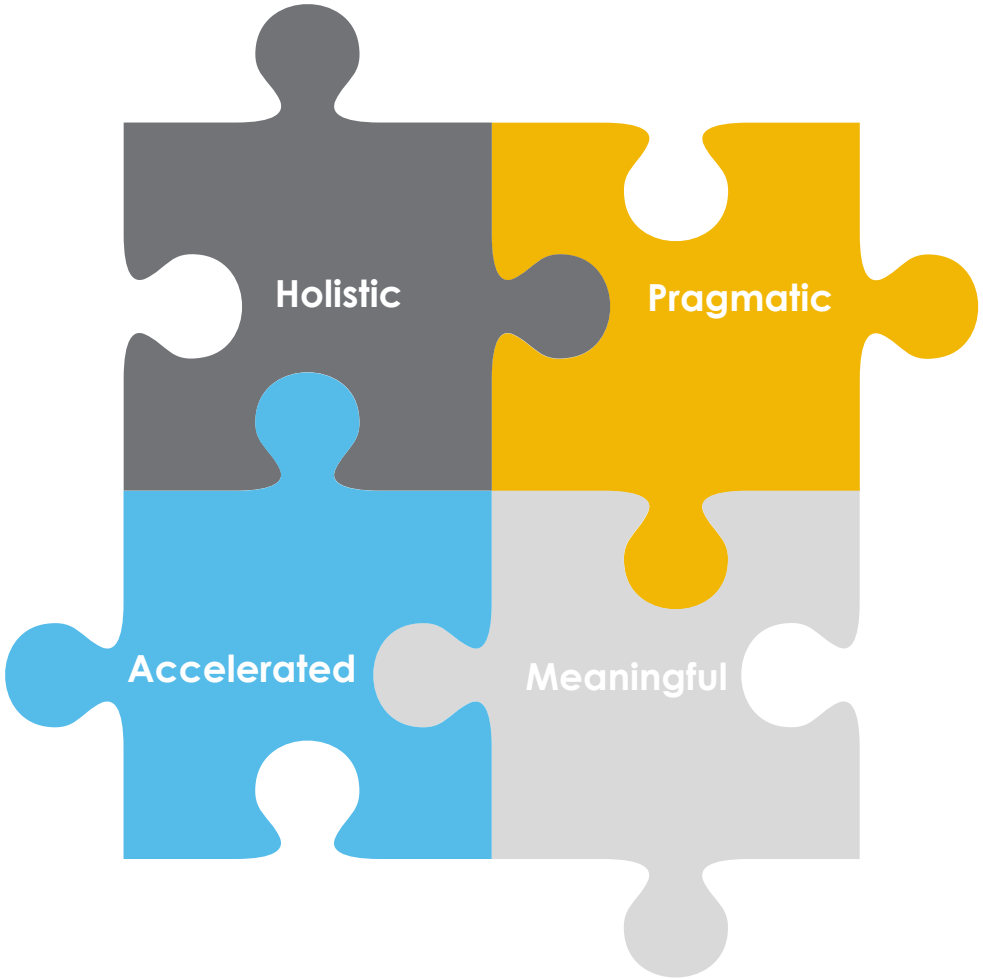


savanti

Benefits

Our assessments provide a holistic view of cyber security leveraging industry good practice requirements.

Our skilled and experienced consultants quickly understand your environment to expedite delivery.



Whilst we leverage good practice, we focus on the actual causes of incidents and their mitigating controls.

Our reporting is designed to give senior stakeholders what they need and practical improvement actions for control owners.

savanti

Client testimonial

"Savanti performed a cyber security assessment for us. I found that the consultants were highly knowledgeable and worked effectively with me and our stakeholders. The project ran smoothly and was successful in helping me meet my objectives."

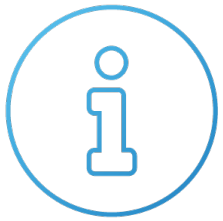
Ste Watts, Head of Cyber Security at Rathbones Brothers Plc

Rathbones
Look forward

savanti

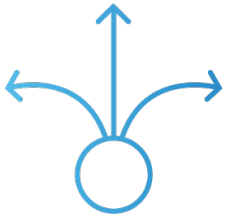
Other assessments

We have extensive experience in performing a range of security assessments to ensure your security controls are effective and that you comply with relevant standards and regulatory requirements in areas outlined below.



Performing detailed, tailored reviews of specific areas such as data loss, infrastructure security components and physical security to ensure that the processes and controls in place are effective at mitigating security risks

Assessing your level of compliance against the 12 requirements of PCI-DSS to support you in completing your Self-Assessment Questionnaire (SAQ) or to prepare for an external audit from a Qualified Security Assessor (QSA)



Performing audits of critical third parties and suppliers who store and process your data to provide assurance that they meet both your security requirements and the contractual obligations in place

Assessing software security maturity using the OWASP Software Assurance Maturity Model to ensure that your software is free from security vulnerabilities at any point during its lifecycle that could lead to service and information compromise

savanti

About us

Savanti provides practitioner-led cyber security services to remove the fear, uncertainty and doubt associated with cyber risk, allowing you to get on with what you do best. Our consultants specialise in providing information security leadership and have a proven track record in delivering successful information security change.

Savanti is currently engaged by some of the world's largest companies to address their global information security challenges.

Unilever

verisure

QBE

savanti

ISO 27001 CERTIFIED
UKAS MANAGEMENT SYSTEMS 8289
British Assessment Bureau 212802

Contact

Brad Harris
Commercial Director

brad.harris@savanti.co.uk
+44 (0) 7540 418 742
+44 (0) 20 7608 5632

savanti.co.uk

20-22 Wenlock Road,
London, N1 7GU

Richard Brinson
CEO

richard.brinson@savanti.co.uk
+44 (0) 7795 222930
+44 (0) 20 7608 5632

savanti

Appendix

savanti

Cyber Security Controls Framework

Our Cyber Security Controls Framework is made up of 15 domains that cover the governance, **organisational** and **technical** security requirements that make for good cyber security.

The controls are not new but are grouped into coherent domains that reflect modern threats and the actual causes of incidents.

These controls are mapped to common industry standards to support external compliance activities where required. If preferred, we also perform assessments against common standards, such as NIST, ISO27001 and CIS.

savanti

Cyber Security Controls Framework

Our cyber security framework is made up of controls underpinning the following requirements per domain.

1. Security Governance

Information security is effectively embedded into the organisation's corporate governance and enterprise risk management mechanisms.

2. Compliance & Assurance

The design and effectiveness of the information security arrangements across the organisation are independently reviewed and assured on at least an annual basis.

3. Employee Security

All staff are made aware of their responsibilities in securing information and the security threats relevant to their role and the organisation.

4. Data Management

There is a documented approach to asset identification, data classification and handling implemented across the business.

savanti

Cyber Security Controls Framework

5. Third Party Security

There are documented procedures to verify that all third parties who access/process data have appropriate security arrangements in place supported by appropriate contractual provisions.

6. Physical & Environmental

All premises and IT facilities are physically secured from unauthorised access and protected from environmental hazards.

7. Incident Management

All IT activities are performed in line with secure configuration and development practices across the IT lifecycle.

8. Access Control

Access to IT resources are controlled through documented procedures and access to privileged resources are protected through multifactor authentication.

9. Anti Malware

All endpoints are protected by anti-malware software that is centrally configured and maintained.

10 Email & Internet Security

All users are protected by email and internet gateway security arrangements.

savanti

Cyber Security Controls Framework

11. Security Monitoring

The scope of security monitoring covers all on-premise and cloud environments and the full endpoint estate and is of sufficient quality to enable effective management of security events and incidents.

12. Network Security

The network is protected by perimeter defences, internal segmentation, and intrusion protection.

13. Secure IT Configuration

There are documented incident response procedures, including full business continuity plans, which are exercised at an operational and management level at least annually.

14. IT Backup & DR

There are documented plans to restore critical services and systems following a compromise or loss of availability, which are tested at least annually.

15. Vulnerability Management

All operating systems, databases and applications are under security support from the vendor/distribution, and there is a documented procedure to identify and remediate security vulnerabilities across the IT estate.

savanti

Cyber Security Controls Framework

Individual controls are assessed to provide an overall maturity score for the domain.

Maturity scores

0 **Non-existent:** No controls in the domain exist.

1 **Initial:** Some of the controls exist but are not applied consistently.

2 **Repeatable:** All controls are in place to some degree but are not all applied consistently.

3 **Defined:** All controls exist and are applied consistently but assurance of controls is ad-hoc.

4 **Manageable:** All controls exist and are applied consistently, and assurance activities take place to confirm the effectiveness of controls.

5 **Optimised**: All controls exist and are applied consistently, assurance activities take place to confirm the effectiveness of all controls, and evidence exists to demonstrate improvements from lessons learned.