Service Description

Security Baseline Assessment

Contents

Who needs this?

Organisations of all sizes and capabilities who understand the importance of effective cybersecurity and need assistance to implement effective tools and practices or are starting on any cyber security improvement programme.

Fordway's Security Baseline Assessment puts in place the foundational elements to ensure your organisations can achieve better, more appropriate and more cost effective cybersecurity.

What the service provides:

Fordway's Security Baseline Assessment reviews the core elements of an organisations' cybersecurity. It is offered as either a high level, discussion and evidence based review, or an in-depth assessment including asset audits, policy review and access control tests plus an optional penetration test.

For both options the deliverable is a report detailing the findings from the review and recommendations to improve the security posture of an organisation to meet its desired capability with budgetary costs, skills plan and resources needed to implement them.

01 Service Overview

The high level version of this service provides an excellent starting point to understand and define required cybersecurity strategy improvements. The comprehensive option, which includes an asset audit plus review of an organisation's security posture is a critical element to implement effective Cloud Security Monitoring and Cloud Security Management.

Many organisations do not have a full inventory of what they are ultimately responsible for. As defined by the CIS and other security best practice frameworks, this is the foundation of good security as it provides surety that all your devices are covered and meet the appropriate security posture requirements. Fordway also complete a risk assessment and review your security governance processes to allow you to articulate the cyber threat level back to your organisation.

The comprehensive option comprises:

• **Discovery.** This element of the service uses agent or agentless technology to discover exactly what IT assets you have deployed. This is an important step as any SAM, ITAM, or ITSM processes will suffer downstream if this is not complete and thorough. Every device that connects to and within your organisation and accesses or uses your data should be accounted for:

- Network and security devices – routers, switches, proxies, & firewalls
- End user equipment – laptops, PCs, mobile phones, tablets
- On premise, 3rd party and cloud hosted server & storage infrastructure
- Cloud IaaS & PaaS instances and environments
- Deployed applications
- SaaS applications that can be discovered by API

Business security assessment. Fordway have extensive experience working with both public sector and private sector organisations, we understand the legislative and organisational requirements of both. Our customers include central and local government, NHS, civil nuclear and other critical national infrastructure providers, giving us an effective starting point to ensure a better result, faster for our customers:

- Organisational security policies review
- Review current capabilities to enforce and manage
- Agree organisational risk profile and define risk appetite
- Regulatory profile, against UK Government/NCSC, FCA or GDPR etc.
- Organisation security history and previous security incidents

Understand security governance maturity level.

- What cybersecurity capabilities do you have in house or contract?
- Do you hold and regularly review a business risk register?
- Does your organisation have or wish to have a security manager, CIO, or CISO?
- Is IT and data security risk regularly reviewed and discussed at board level?
- Is your organisation committed to continual improvement of Information Security?

Risk assessment. This is a full inventory and complete risk assessment, which will be presented back to the IT department or at board level, as required, to complete the service.

Fordway will tailor the assessment to assist with:

- **Cyber Essentials –** Recognised UK Government National Cyber Security Centre (NCSC) scheme. Provides guidance on basic technical security controls, to protect an organisation's:

1. Data
2. Programs
3. Network
4. Devices
5. Servers

Against most threats. These are self-audited. Can be uplifted to Cyber Essentials Plus, with external audit where a certified independent third party verifies you have the tools and controls in place and are using them effectively, issuing a conformance certificate.

- **ISO 27000 –** an internationally recognised certification confirming that an organisation has effective cybersecurity practices and follows those policies to correctly classify, store and keep information secure. Fordway's Security Baseline Assessment provides a starting point to help organisations progress towards this standard. ISO27000 requires an Information Security Management System (ISMS) and tested for compliance with regular audits. The ISO27017 extension to ISO27000 specifically covers assessment and compliance with specific controls for cloud data security.

• **GDPR (General Data Protection Regulation) –** laws governing the use of personal data. GDPR is a legal requirement and substantial penalties can be incurred as a result of data breaches. Specifically, for identifiable information regarding a living person, it defines:

- How to use/process
- Storage and management
- Data minimisation
- Accuracy
- Accountability

A well-defined ISMS solution can assist in achieving GDPR Compliance, and the ISO27018 certification extension to ISO27000 provided third party assurance that the policies and controls are in place and enforced.

• **IT Health Check/Penetration Test:**

- Review of IT systems and their health
- Formal check of security
- Highlighting potential vulnerabilities
- Recommendations and remediation options

As required, a detailed report will be produced, including a gap analysis of where the organisations current security posture sits, aligned to the above. Fordway can then work with the IT staff to reduce the risks and threats, explaining how to re-configure systems, or can be contracted to assist with operating and managing the customer's security.

02 Key Benefits

• **Increased Understanding of Security Requirements –** deliver detailed assessment report aligned to business requirements

• **Take Advantage of the Latest Technologies –** use Fordway's experience of the new tools and applications available to improve business performance. Independent – Fordway will provide independent feedback on the benefits and limitations of the cloud security solutions as well as enhance them

• **Experienced Personnel –** From business, project management and technical viewpoint, Fordway have multi-years of experience of real-world deployments and operational requirements

• **Comprehensive Cloud Security Assessment –** Fordway will perform a detailed analysis against the current configuration, how to incorporate the new technologies and where real business benefits can be gained. Provide full testing and gap analysis and arrange a penetration test as needed

• **Collaboration –** Fordway's personnel will work alongside your IT staff and any third parties collaboratively, as each has skills necessary.

• **Detailed Knowledge of Management Tools –** Fordway have extensive knowledge of the Microsoft management tools, including Lighthouse, Monitor, Sentinel and Arc. These can be configured to deliver the necessary statistics and dashboard for each organisation and used as part of the assessment.

• **Understand Legacy –** Fordway know companies have legacy systems with potential integrations that cannot just be ignored

• **Clear Recommendations –** Fordway will produce a set of costed recommendations and options, on how to get the best out of the Cloud Security, reducing the risks/threats to the business

03 Service Initiation (on-boarding)

The service is a consulting engagement. The following procedure will be used to provide the service:

• Provide a combination of Project Manager, Account Manager, Relationship Manager, Lead Consultant and appropriate consultancy team, depending on the scope of the engagement. Fordway will generally seek to provide a peering alignment with the customer.

• Agree and formalise Non-Disclosure Agreements

• Review the customer requirements and determine the contractual requirements

• Agree the scope of the engagement with the customer and provide a Project Initiation Document which will define the engagement.

• Schedule work

• Commence engagement

• Provide deliverables

• Complete engagement

All engagements are run to Fordway's PRINCE2 Agile processes.

Service Connectivity

Required connectivity to access the Customer's environment will be defined as part of the Project Initiation Document.

Trial of Service

Not applicable to this service.

Data Security

Any information processed by Fordway will be transitory in nature and Fordway will comply with the customer's data security procedures during the engagement and off-boarding.

Technical Requirements

There may be a need to install and configure tools, agents and updates to support the service which will be defined within the Project Initiation Document if appropriate. All changes will be applied through change control with relevant communication and scheduling.

04 Ordering

Fordway services can be ordered by contacting your Fordway account manager or other members of our team on **01483 528200**, emailing **sales@fordway.com** or using the contact form on **www.fordway.com**.

Our Accreditations

ISO 9001 ISOQAR

ISO 27001 ISOQAR

ISO 14001 ISOQAR

Microsoft Solutions Partner
Infrastructure
Azure

CYBER ESSENTIALS PLUS

HSCN HEALTH & SOCIAL CARE NETWORK COMPLIANT

PSN Public Services Network

FORDWAY

Fordway Solutions Ltd,
Charterhouse Suite
Ground floor, Mill Pool House
Godalming,
Surrey GU7 1EY