Cyber Security Overview

CAPITA Employee Solutions Information Security

Table of Contents

Author:	**Version:**	**Review Date:**	**Reviewed By:**
Stewart James	1.0	24/09/2019	Tim Miles

1. Document Introduction

The purpose of this document is to provide a high level overview of the security controls and mitigations that are in place within Capita. Cyber security is important for Capita, ensuring client and company data is secured to the best industry standards.

The following topics are covered within this document:

- Employment Screening
- Employee Training
- Certifications
- Security Management Systems
- Risk Management
- Security Policies
- Monitoring & Assurance Activities
- Patching
- Penetration Testing
- Vulnerability Scanning
- Delivering Service in a secure manner
- Account Security
- Awareness
- Internet Security
- Email Security.

Capita Employee Solutions (CES) has a dedicated Head of Information Security (Nigel Garwood), who manages a team of 5 located at various Capita sites. The Information Security team supports the CES ISMS, are responsible for maintaining security processes throughout CES and ensure the business remains compliant with legislation, certifications and client requirements.

2. Cyber Security Processes

2.1. Employment Screening

2.1.1.

At the start of the employment process, new hires are required to undertake security vetting. Employees are required to submit a varying amount of information that aids Security Watchdog in their vetting process (a 'level 1 check'). Information that is required during this process includes:

- Identity
- Right to work
- Address
- Criminality Check
- Financial probity
- Sanctions
- Adverse media
- Minimum 1-year reference.

2.1.2.

All employees must undergo security vetting every 3 years. If an employee or new hire fails the vetting process, their contract is terminated and the employee is escorted off site with their access revoked.

2.2. Employee Training

2.2.1.

All employees are required to complete the Capita mandatory CBT (Computer Based Training) on an annual basis. CBT's ensure that staff are trained in the appropriate areas for the business. Capita Information Security focuses on 5 primary CBT's that need to be successfully completed, with testing, annually. They are:

- Information Security Awareness
- Data Protection Awareness & GDPR
- Anti-Money Laundering
- Financial Crime
- Treating Customers Fairly

2.2.2.

Users have 3 attempts to complete CBT testing. Upon a third failure the user will be asked to review the training material again and their manager notified. This action is also fed back to the Learning & Development team who will assess the training material and decide how the user proceeds with the training.

2.3. Certifications

2.3.1.

Capita is audited on an annual basis for multiple certifications – including ISO 27001:2013. The ISO 27001:2013 certification is the Information Security Management System standard. A number of CES offices hold certification, including:

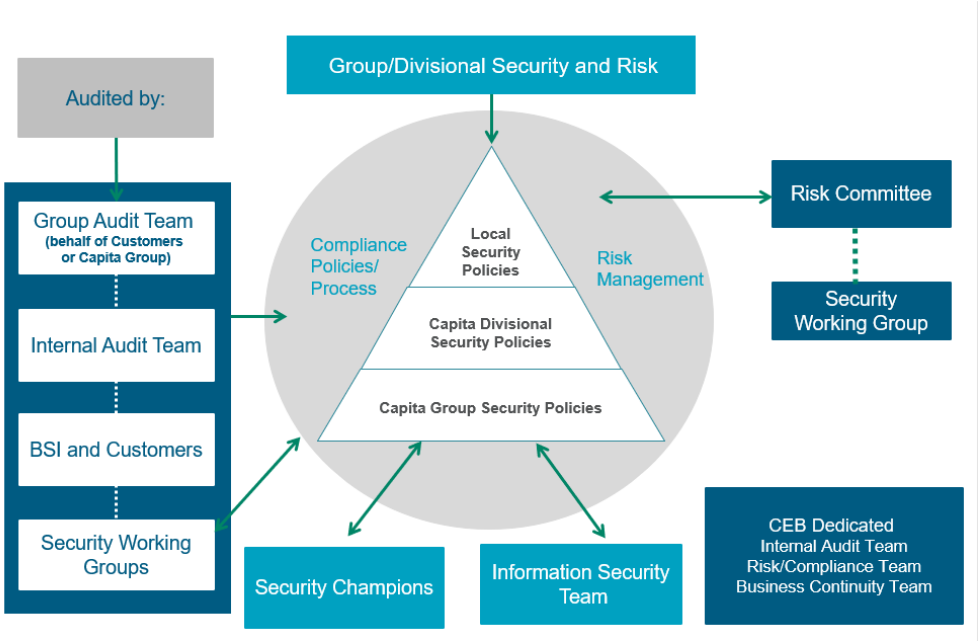
- Bristol
- Darlington
- Harrogate
- London Gresham Street
- Reading Bridge House
- Sheffield Hartshead House
- Swindon Stirling House.

2.3.2.

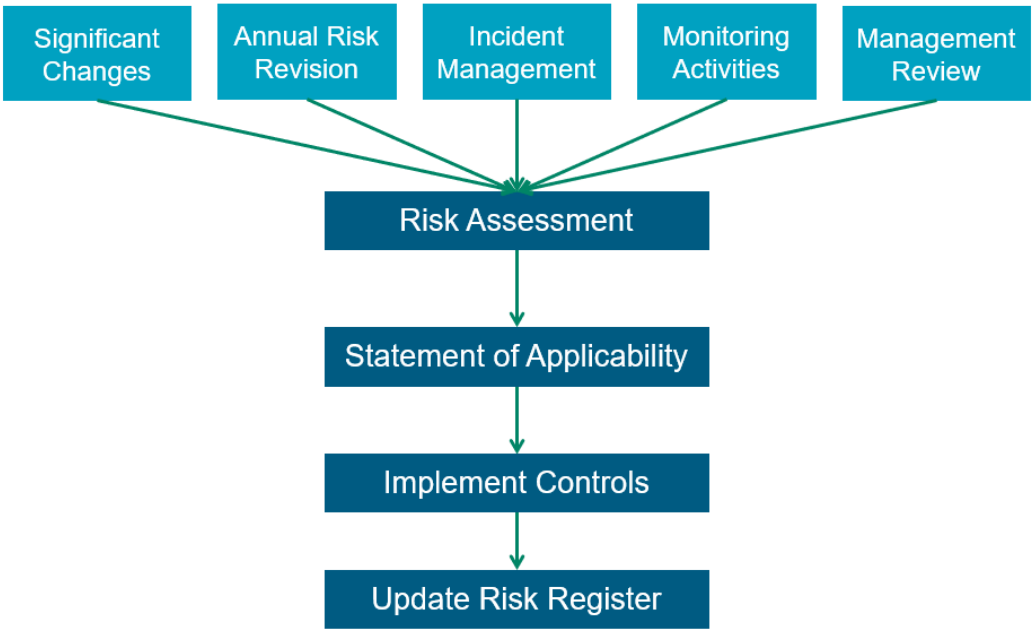
Capita has also committed to maintaining other relevant certifications, such as:

- ISO 9001:2015 Quality Management Systems
- ISO 20001:2011 Service Management
- ISO 22301:2012 Business Continuity
- ISO 14001:2004 Environmental Management
- TickIT+ Software Development
- AAF Audit Assurance Faculty

2.4. Security Management System



2.5. Risk Management & Security Policies



2.6. Monitoring and Assurance Activities

2.6.1.

Continued protective monitoring is important to Capita. We ensure that our servers and applications are appropriately monitored and issues alerted upon. Our service provider manages a 24-hour Network Operations Centre located within the Data Centre which is staffed 24/7.

2.6.2.

Logs are collected at all levels and are processed by our service provider's logging application.

2.6.3.

For Microsoft Azure environment hosted applications, Capita currently uses Microsoft Azure Sentinel for all Azure monitoring activities; including alerting on security events.

2.6.4.

For Amazon Web Service environments, the ELK (Elasticsearch, Logstash, Kibana) stack is used in protective monitoring. Alongside ELK, FAIL2BAN is used to automatically ban IP addresses that have been identified attempting malicious activities.

2.7. Patching

2.7.1.

Patching is centrally managed by Capita's Infrastructure team, with patches being deployed automatically to devices.

2.7.2.

All patches go through the Capita change management process and are tested on a central server before being pushed to end devices. Capita monitors patching on devices to ensure they have received the latest patches.

2.7.3.

Capita will patch devices to the following timescales:

Type	Risk	Criticality	Timescale
External facing servers	Within Tolerance	Low / Medium	30 days
	At Tolerance	High	7 days
	Uncomfortable / At Critical Limit	Critical	24 hours
Internal facing servers	Within Tolerance	Low / Medium	40 days
	At Tolerance	High	7 days
	Uncomfortable / At Critical Limit	Critical	24 hours
Endpoint devices	Within Tolerance	Low / Medium	60 days
	At Tolerance	High	30 days
	Uncomfortable / At Critical Limit	Critical	7 days
Network devices	Within Tolerance	Low / Medium	40 days
	At Tolerance	High	7 days
	Uncomfortable / At Critical Limit	Critical	24 hours
Databases	Within Tolerance	Low / Medium	40 days
	At Tolerance	High	7 days
	Uncomfortable / At Critical Limit	Critical	24 hours

2.8. Penetration Testing

2.8.1.

Capita conducts penetration tests on environments and applications at least once per year. Tests are arranged with Capita testing partners and can be conducted to both CHECK and CREST requirements.

2.8.2.

On all pre go live projects, testing must be conducted at least once before going live. Issues that have been raised are risk assessed by Information Security and passed to the appropriate team for remediation.

2.8.3.

When required, a re-test can be scheduled to confirm the closure of issues raised previously.

2.9. Vulnerability Scanning

2.9.1.

Capita conducts monthly vulnerability scans against its environments. Capita uses Tenable Nessus to carry out scans, scheduled to run against Capita servers.

2.9.2.

Vulnerability scans check the server for commonly known vulnerabilities and flags any that are found. Issues are given a rating from "Informational" to "Critical". Issues that been identified are risk assessed by Information Security and are registered on Capita's internal risk tracker. Issues are passed to the appropriate team for remediation.

2.10. Delivering Service in a Secure Manner

2.10.1.

Capita ensures that service is delivered securely for all clients as a tiered security approach. This includes:

- IDS/IPS Technology
- Multi-Level Firewalls
- Security Hardened Servers
- Primary and Secondary Data Centres certified to ISO 27001, 9001 and 22301
- Monthly patching schedule
- Annual Penetration testing
- All external communications are encrypted
- Software Development is in-house. All code is tested prior to implementation.

2.10.2.

Capita ensures that all employees follow strict policies when using a Capita device and enforces security policies that the user cannot avoid. These include:

- Multi-layer anti-virus protection
- All laptops and mobile devices are encrypted
- Use of removable media is restricted and requires prior approval to use. Once access to removable media is approved, the device must be encrypted
- String password policy with Multi-Factor Authentication for remote access (VPN)
- Internet access is controlled and monitored
- All staff are trained on Data Protection and Information Security
- Regular security bulletins and awareness.

2.11. Account Security

2.11.1.

All users are required to have a minimum of 8 alpha-numeric characters in their password. Devices will not allow users to set a password that does not meet this requirement.

2.11.2.

Users are required to change their password every 90 days. Allowing users to change their passwords every 90 days instead of 30 allows for more secure passwords.

2.11.3.

Users are locked out of their accounts after 3 failed login attempts. If a user does get locked out, they must contact their local IT and Service Desk to get their account unlocked. Users must verify their identity before their account will be unlocked.

2.12. Awareness

2.12.1.

Capita conducts bi-annual phishing tests against employees. Capita generates an email designed to trick employees into clicking links within it and filling out a form. Stats are generated from this exercise and are fed back to local Information Security teams who can build awareness campaigns to educate colleagues on phishing attacks.

2.12.2.

Regular security awareness bulletins are shared across the business to educate employees on Information Security. Awareness campaigns include:

- ID Pass security awareness
- Clear desk awareness
- Locked pedestal awareness
- IT Security awareness.

2.12.3.

Capita designates a Security Champion for each site. Employees who take this role on alongside their regular role are required to perform monthly building and physical security checks. Security issues identified during the checks are reported back to Information Security who investigate the issue further.

2.13. Internet Security

2.13.1.

Capita employees are restricted with what they can do on the Internet. Capita utilises Forcepoint Cloud to block websites that are deemed to be unnecessary for work or a security risk. For example, file sharing sites like Dropbox and Google Drive cannot be accessed from the Capita network.

2.13.2.

Capita monitors all traffic that passes through the Forcepoint proxy.

2.14. Email Security

2.14.1.

Capita users must classify all emails before sending them. Capita utilises an Outlook add-on that prompts users upon sending an email. Emails sent externally can be encrypted by using a “Confidential” tag, which will ensure the email is sent securely.

2.14.2.

Capita emails are powered by Microsoft Office365 (O365). O365 uses UK Azure Data Centres to store data, which is not sent outside the UK.

2.14.3.

Capita performs a virus scan on every email that comes into the business. Emails that are found to have anything malicious content or payload are quarantined and reported on.

2.14.4.

Users cannot send emails with attachments over 40MB and are also prevented sending and receiving emails that contain an executable file (e.g. .exe, .msi, .bat, etc.).