Cyber and Information Security Statement

HSBC Cybersecurity

Date: June 2019

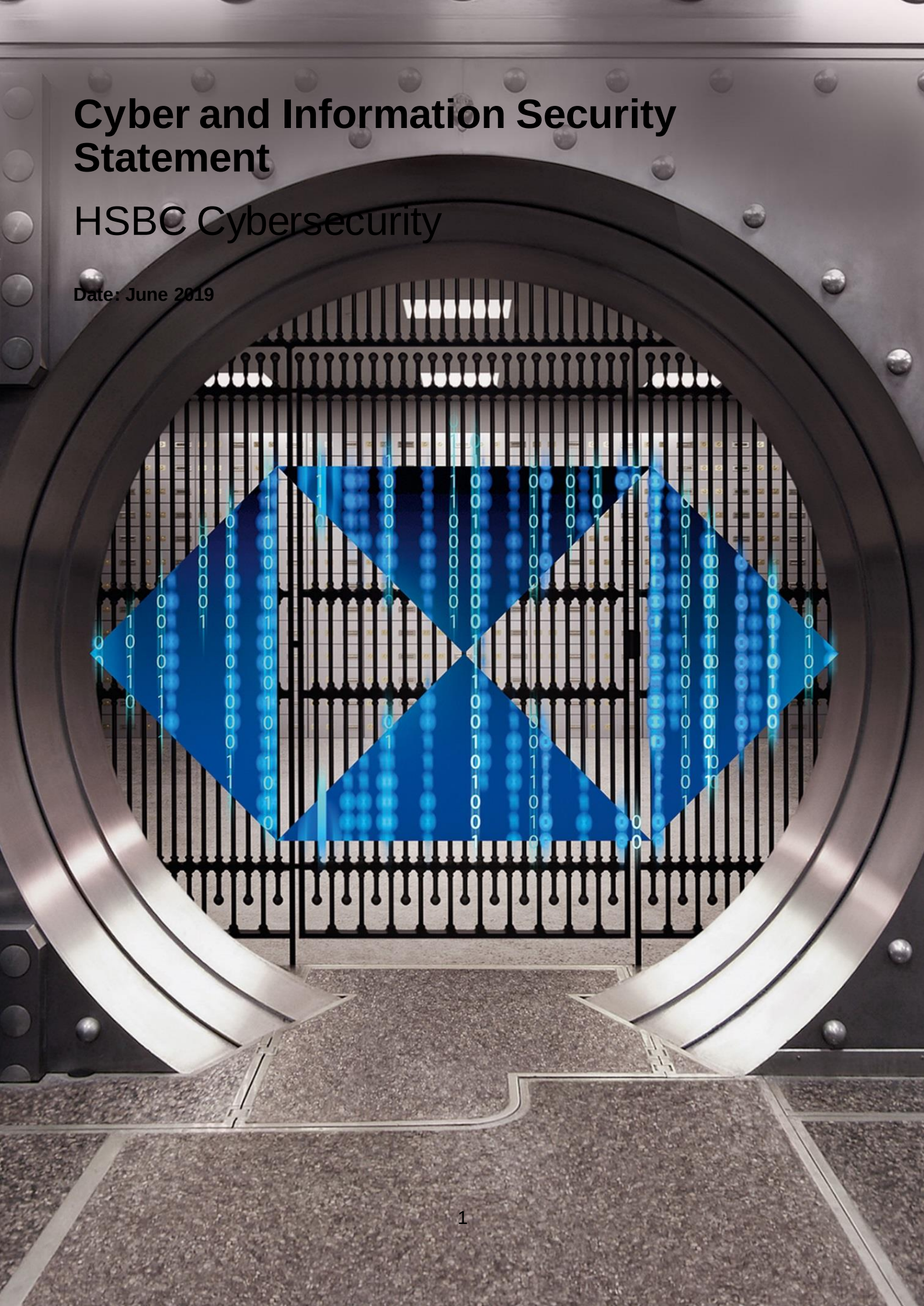


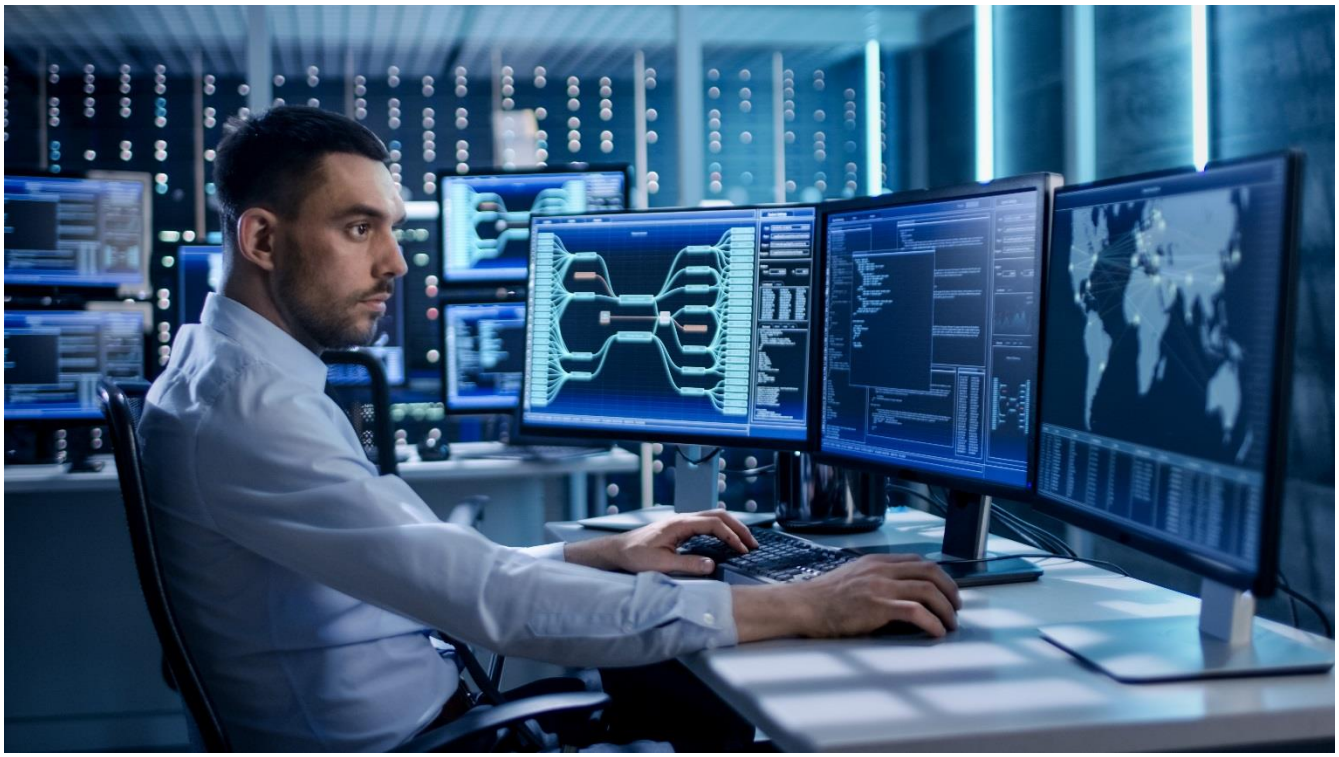
Table of contents

Introduction

This Information Security Statement aims to provide a summary of information security controls within HSBC.

The document is for use with 3rd Parties (clients) who are engaging HSBC to provide a service to us and who have questions on our security arrangements.

This Information Security Statement is reviewed at least once per annum.



Security Commitment

HSBC is committed to maintaining and continually improving information security to meet our responsibilities to our customers and regulators and to reduce exposure to legal sanction, operational loss or reputational damage. We are committed to ensuring:

- The confidentiality of corporate, client and customer information.
- The integrity of our information.
- The availability of our information.
- That regulatory and legal requirements are met.
- That information security and risk awareness training is provided to all staff.
- That breaches of information security, actual or suspected, are reported to and investigated by HSBC.

HSBC Cyber and Information Security Overview

Information Risk and Cybersecurity Organisation

HSBC's management as a whole, are accountable for identifying, assessing and managing the broad spectrum of risks to which HSBC is subject.

HSBC adopts a 'Three Lines of Defence' model to ensure that risks and controls are properly managed by its businesses, functions and technology teams on an on-going basis.

- First Line – Operational and business teams. Specialist business information risk officers are embedded in the first line to drive compliance to policies and standards over the business' use of systems and processes. Specialist technical teams in the first line are responsible for the installation and operation of the IT environment. This includes a dedicated Cybersecurity team responsible for the implementation and operation of security controls on IT infrastructure and networks.
- Second Line – Information Security Risk teams, formulate and monitor policies and provide assurance over control compliance and operation within the first line. Second line teams also provide subject matter expertise for the development and implementation of controls, tooling and projects.
- Third line – Internal auditors provide independent review of the control state of the first and second lines and the interaction between them.

HSBC Staff

Vetting is a key Group defence against Insider and other risks. Minimum requirements for vetting are set out at HSBC. All HSBC employees, including contractors, service provider workers and contingent workers are subject to vetting prior to starting in role.
Key vetting objectives are to;

- Confirm the candidate's identity, employment history and relevant qualifications with respect to the post for which they are applying;
- Test their integrity in accordance with HSBC values;
- Confirm that there are no legal or regulatory barriers to the Bank employing them

The vetting process also seeks to provide a level of assurance that an applicant's background does not raise reasonable concerns that their employment would expose the Bank to unacceptable levels of risk.

Background checks are completed, as allowed by local law, including where possible:

- Verification of name and address
- Criminal record check
- Public media research check
- Name check for Sanctions, Politically Exposed Persons and other financial crime risks
- Credit check
- Verification of the previous five years employment history (six years for regulated roles)

- Verification of education (highest achieved academic qualification)
- External Directorship checks where required

HSBC does operate a revetting programme for higher risk staff.

Security Awareness

HSBC has an ongoing security awareness programme employing various channels to engage staff including, intranet content, posters, e-mails, new employee education and annual mandatory information security awareness training for all staff. Completion of annual mandatory training is monitored and failure to complete training results in formal management action.

HSBC Policy

HSBC employs controls globally through enforcement of global policies, standards, and guidelines covering information security and risk. Each policy document is controlled and maintained by a specific owner within the second line of defence.

HSBC policies include, but are not limited to:

- Defined information security responsibilities for employees, contractors and 3rd parties.
- Testing to identify missing controls or control deficiencies.
- Acceptable usage policies for all users including but not limited to, email and internet usage.
- Defined criteria for access control, including need to know, least privilege principle, unique ID, password complexity, access approvals, recertification transfer and leavers processes, privileged access and remote access controls.
- Software development life cycles for applications including code review, separation of duties, security reviews for web services.
- Change control and disaster recovery / business continuity planning requirements.
- Defined information classification procedures (High level 4 tier classification system, Public, Internal, Restricted and Highly Restricted. These terms are referenced in this document).
- Detailed instructions for encryption, secure data transmission and destruction.
- End User Environment policies, covering data extraction, non-IT managed data processing (End User Computing), data classification, labelling, secure storage destruction and remote working.
- Technical configuration and control settings for IT infrastructure, networks and platforms.
- Physical security.

Risk Management

HSBC utilises risk management across the lines of defence to identify, report and manage risks across the organisation. Information security frameworks within HSBC follow internationally recognised best practice standards.

Risk assessments are performed periodically to address changes in the bank's information security requirements or risk appetite and when significant changes occur. HSBC performs risk assessments on a variety of assets within the organisation. These may be physical assets, people, processes, software, and information. For example regular information security risk assessments are performed upon application and infrastructure technologies to:

- Identify, quantify, and manage information security risks to achieve business objectives.
- Provide means to identify activities and factors which pose the greatest security risk to HSBC.
- Ensure information security issues are managed according to their risk rating, and that controls are proportional to the level of risk discovered.
- Provide an enterprise view of information security risks and respective remediation plans to develop the information security strategy.
- Plan the deployment of resources to areas that provide the greatest reduction in risks to customer / corporate information.
- Assess all aspects of information security risks, threats and vulnerabilities to our assets.

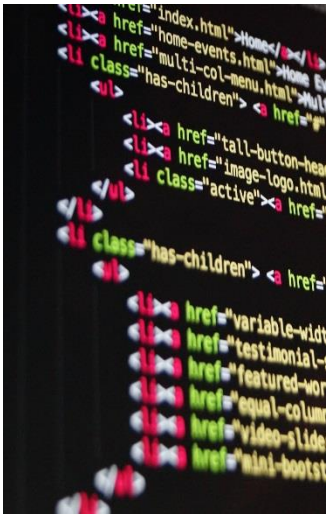
Access Management

Identity and Access Management own and operate the Global Access Management Control within HSBC. This ensures regulator aligned and policy driven access management across the lifecycle of supporting controls:

Services provided by Identity and Access Management Operations teams include:-

- Joiners, Movers and Leavers controls incorporating segregation of duties principles to ensure authorised least level of privilege entitlements are maintained for all user activities.
- Privileged Access Management controls with appropriate justification and authorisation, incorporating validation of activities via a robust logging and monitoring process.
- Access Recertification controls to ensure all accounts and associated entitlements are reviewed, and maintained or revoked, periodically by the appropriate reviewer.

Application Security



Technical Application Security teams in the first and second lines of defence identify threats, controls and undertake testing, including -

- Application security consultancy and risk assessments – to ensure risks within HSBC applications and systems are managed to an acceptable level;
- Technical and information security risk advice to businesses, functions' projects or initiatives.
- Defining and testing application system controls relating to information security.
- Input to system build standards and procedures.
- Installation and monitoring of application level controls.
- Development of minimum baseline security standards.
- Conduct security testing i.e. application penetration test (which includes vulnerabilities covered by the OWASP framework) and code reviews.

Network Security

To enable effective management HSBC utilises various technologies deployed strategically throughout its network.

Intrusion Detection and Prevention Systems

Network and host-based intrusion detection and prevention systems are deployed across HSBC. These systems are managed by the first line of defence. HSBC networks and infrastructure security are subject to 24/7 monitoring.

Wireless Network Management

Wireless network infrastructure in our offices and branches is secured using mechanisms for access control and monitoring, authentication and encryption and capabilities to guard against rogue wireless access points.

Denial of Service Protection

HSBC has a 3 layer Distributed Denial of Service (DDoS) mitigation approach:

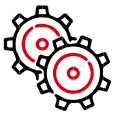
- Internet Service provider border router devices that are configured to sense DDoS attacks.
- Utilisation of an external service provider, which provides an always on DDoS mitigation.
- The Bank's Intrusion Prevention System DDoS appliances provide alerts and filter DDoS attacks.

Internet Access Filtering

Staff may be permitted internet access for business use. Access is filtered according to centrally defined rules. Additional management approval is required for any non-standard access and may be subject to additional monitoring.

Data Loss Prevention

HSBC's Data Loss/Leakage Prevention Programme is in place to reduce our exposure to data loss/leakage risk through technical controls and process as well as user education. It includes processes to detect and automatically protect Restricted and Highly Restricted information sent externally from HSBC. This includes outbound e-mail, file transfers and web uploads. HSBC monitors for data leakage to guard against the risks of theft, accidental loss or deliberate exposure of confidential information.



Infrastructure Security Testing

Infrastructure security testing is a component of HSBC technical security reviews, and is used to validate the security posture of any given technology. Such penetration testing is performed by our own teams against HSBC systems as part of technology improvement processes and also at regular intervals. In addition, independent testing by specialist third parties may be commissioned, using advanced techniques and latest industry standards to provide additional assurance.

The output of such testing is managed within HSBC's risk management process and framework.

Cryptography

HSBC data is classified according to its sensitivity to determine the level of controls required including but not limited to encryption to maintain information confidentiality, prevent unauthorised data leakage or to provide integrity checks or digital signatures.

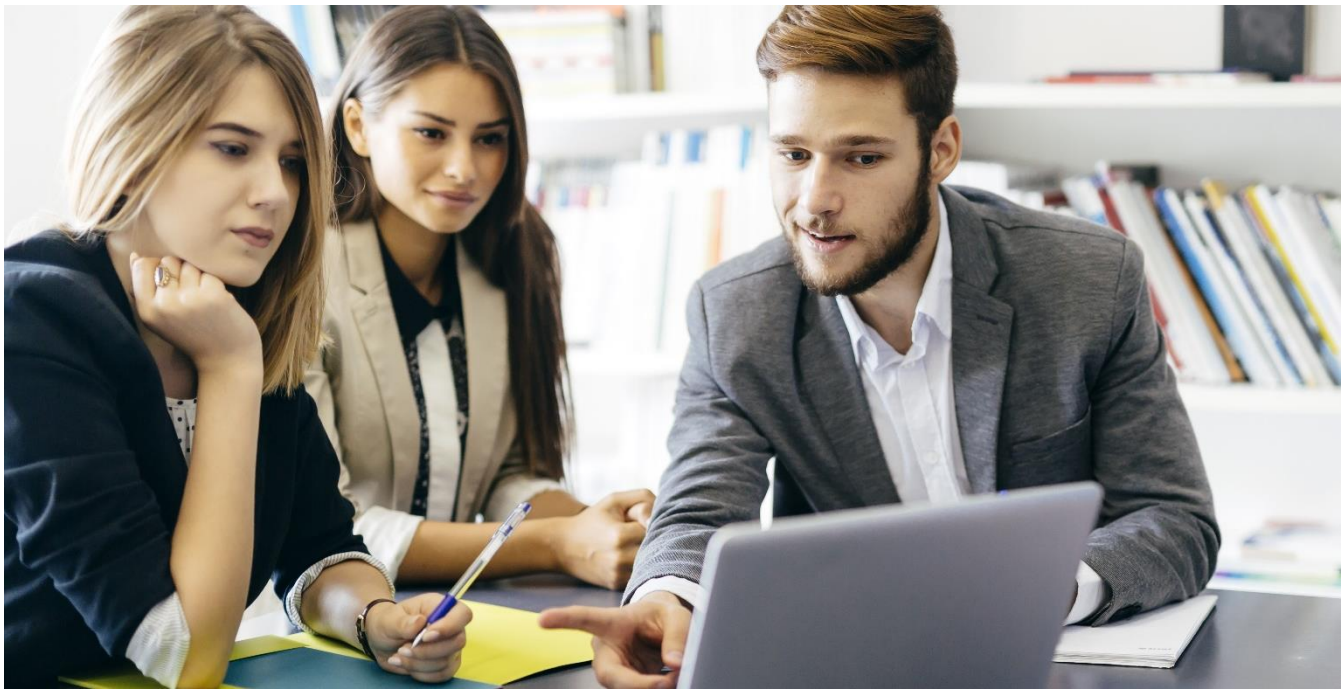
HSBC have clearly defined cryptographic standards which mandate appropriate cipher suites and key lengths to meet specific objectives.

Host Security

Workstations Laptops and Mobile devices

HSBC workstations and laptops have anti-virus software incorporated into default operating builds, set to automatically check files as part of its regular full-time “on access” scanning and obtain updates as they become available.

- Desktops/laptops have a single, pre-installed customised build which limits users’ administrative access.
- Laptops are protected against data leakage from device loss via a centrally managed endpoint (disc) encryption solution.
- Writing data to removable media is locked down to a limited number of approved staff only and encryption controls are automatically applied when data is written.
- Access to the HSBC internal network from outside of the office is restricted to authorised devices controlled by industry standard remote connectivity and multi factor authentication controls.
- Internet access and network connectivity from HSBC laptops is routed through the HSBC network. VPN software ensures that HSBC laptop users cannot connect directly to the public internet.
- HSBC provided mobile devices are managed through a Unified Endpoint Management solution (UEM) enforcing policies and controls to limit information exposure.
- Limited number of bring your own device (BYOD) solutions protected using an industry standard mobile data management solution, enforcing a secure container under HSBC’s control on the devices in the question.
- Mobile data management capabilities provide encryption for data in motion or at rest and capabilities to securely wipe data from lost or stolen devices.



Server Platform

System security is built into our server platforms.

Hardening measures and controls are incorporated into server builds; these include but are not limited to;

- Unnecessary and redundant services, devices, processes, protocols, system and network utilities, programs and accounts, are disabled/removed.
- Operations/services are run with the minimum privileges required; appropriate file system security is applied.
- Strong user account and password controls are implemented for all users enforcing length, complexity, history and lockouts. Automated password control with logging and auditing applied to privileged accounts.
- Additional monitoring capabilities are in place at the database level to protect sensitive data.
- Configuration settings are defined based on the 'least privilege' principle.
- Monitoring and reporting of any non-compliance.
- Audit trail management.

Patch Management

First line teams receive product vendor notifications of vulnerabilities and recommended patch responses. Prioritisation for deployment across HSBC's global estate is determined by the Patch Priority Classification, assigned as part of the assessment process which uses the Industry Standard Framework Common Vulnerability Scoring System.

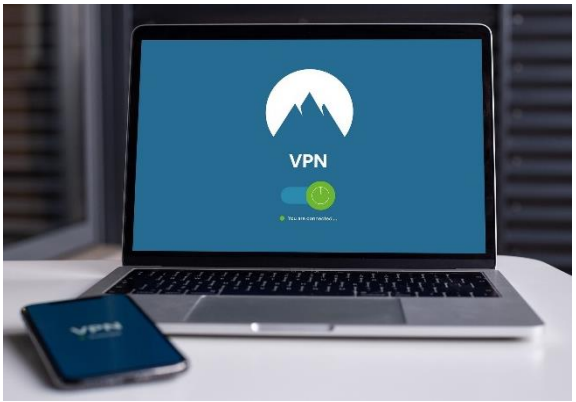
Patches are tested in non-production environments globally prior to deployment into production systems. All patch deployments are managed following HSBC's Global Change Management and Incident Management Processes.

Appropriate governance and oversight is exercised through regular engagement and communication with the global businesses and functions in accordance with the established framework. Monthly patch compliance status of security and operational patches is measured, reported and distributed.

End User Computing

End User Computing (EUC) which is defined as "Processing (e.g. calculation, manipulation or transformation) of data outside the Information Technology (IT) controlled environment in support of a recurring operational business process", is governed through an EUC Management process that includes the identification and risk assessment of EUCs, together with application of controls around the EUC itself to ensure confidentiality, availability, and integrity.

Remote Working



HSBC supports remote working capabilities where appropriate for its staff. Additional controls and guidance for staff working remotely include but are not limited to:

- Training and education on remote working risk which must be completed before remote access is provided.
- Full disk encryption on laptops.
- Secure mobility clients on laptops enforcing VPN use.
- Provision of managed mobile devices or support of 'Bring Your Own Device' via specialist applications offering secure containerisation.

Physical Security

Protective security counter measures are implemented to prevent unauthorised access to HSBC facilities, resources or information. Protective security controls are reviewed on a regular basis.

Measures deployed by HSBC include, but are not limited to.

- Physical barriers and security guards
- Access control systems and identity cards
- Baggage and vehicle searches
- Surveillance Video Systems
- Intrusion Detection Systems
- Secured data and network cabinets
- Facilities to securely destroy physical data (secure waste process and shredding)

Security Operations

HSBC's Cybersecurity Operations function leverages multiple security solutions to provide proactive 24/7x365 monitoring, technical analysis support and threat response. These automated solutions enable early threat identification and assessment and allow the formulation of a consistent response plan for potentially malicious and unauthorised activity.

Services covered by Cybersecurity Operations teams include:

- Forensic analysis of digital media and electronic artefacts
- Data leakage monitoring
- Malware detection and mitigation
- Network and host intrusion detection and monitoring
- Assessment of emerging technology threats
- Monitoring of suspicious system access attempts
- Cyber threat intelligence
- Global Cybersecurity incident management

HSBC's Cyber Intelligence and Threat Analysis (CITA) team conduct holistic investigations of malicious cyber actions and actors to inform, educate, and advise HSBC and the broader cybersecurity industry. CITA's research is emboldened by participation in numerous internal and external engagements that span industry, academic, and government sectors. CITA's formal reporting and technical analysis allow threats to be proactively assessed and mitigated while maintaining an informed constituency across all of HSBC's estate.

Incident Management

HSBC's global Cybersecurity Operations Incident Management & Response processes:

- Co-ordinate Cybersecurity incidents to ensure that all required tasks are completed and that duplicative or contradictory efforts are avoided
- Ensure that Cybersecurity incidents are investigated in a timely manner
- Ensure that the risk associated with an incident is appropriately identified, measured, and controlled
- Ensure that required internal notifications and external reporting is completed
- Ensure all Cybersecurity incidents are centrally tracked for trend analysis and consolidated reporting to management

Non-disclosure and Confidentiality Agreements

HSBC only discloses information to 3rd parties if the appropriate controls have been considered and implemented (as applicable) to manage the 3rd party's access to, use and storage of HSBC information. These controls may include:

- Agreeing confidentiality and information security obligations with the 3rd party;
- Making appropriate assessments of the information itself, how and why it is to be disclosed; and
- The transfer of information is secured using appropriate technical or process controls as required by HSBC to meet our legal responsibilities, customer obligations and regulatory requirements

Vendor Security Management

HSBC has a Third Party Risk Management policy to identify and control risks (including information security risks) associated with vendor relationships and contracts. HSBC requires third parties to meet at least the same level of security as per HSBC Group policies and standards, covering legal and regulatory requirements that apply to HSBC information or systems accessed in the provision of service to HSBC.

Furthermore, third parties with access to HSBC's network or information are subjected to information security due diligence reviews based on their potential risk to the organization. Specific information security clauses are included into terms and conditions of contracts with third parties. These may include the right to undertake audits of third party premises, physical and logical security controls.

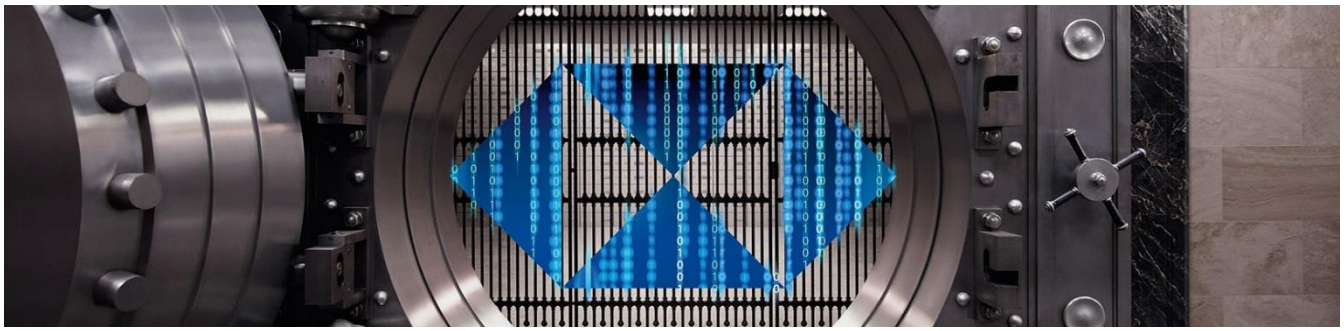
Third parties' employees with access to our systems are subject to annual access recertification.

Governance

As noted, HSBC operates a three lines of defence model. First line teams execute controls in line with policies produced by the second line teams, overseen by the third line independent audit function.

Internal and external parties (including internal and external auditors) regularly review HSBC business units, systems and processes, utilising best practice control frameworks. Additionally, reviews are also undertaken by HSBC Information Security Risk teams across global HSBC businesses and functions.

Whilst some audit cycles are predetermined by regulatory or similar stipulations, in general audits throughout the HSBC Group are carried out on a frequency determined by an assessment of the current risks using a risk prioritisation model.



Regulatory

HSBC is regulated and monitored by financial services regulators and other regulatory organisations globally. HSBC complies with regional and local banking control requirements including those related to information security, systems and controls, cybersecurity and operational resilience.

These include, but are not limited to:

- UK - Financial Conduct Authority (FCA) & Prudential Regulation Authority (PRA);
- Hong Kong - Hong Kong Monetary Authority (HKMA); Securities and Futures Commission (SFC), Hong Kong SAR; Office of the Privacy Commissioner for Personal Data (PCPD)
- USA - Federal Reserve Board (FRB); Financial Industry Regulatory Authority (FINRA); Office of the Comptroller of the Currency (OCC); Federal Deposit Insurance Corporation (FDIC);
- Singapore - Monetary Authority of Singapore (MAS);
- China - China Banking and Insurance Regulatory Commission;
- Mexico - Comision Nacional Bancaria y de Valores;
- Brazil - Banco Central do Brasil;
- Germany - Federal Financial Supervisory Authority, Germany;
- Switzerland - Swiss Financial Market Supervisory Authority (FINMA).

HSBC also follows international cybersecurity frameworks such as National Institute of Standards and Technology (NIST), ISO 27001 and guidance from organisations such as the UK National Cyber Security Centre. Such risk frameworks are for voluntary use by critical infrastructure owners and operators, including financial institutions, and guide cybersecurity activities and consideration of cybersecurity risks as part of the organisation's risk management processes.