Information Security at SHL

05 April 2021

Contents

Information Security at SHL

Geographic Coverage	Global
Document Owner	IT Information Security
Document Author	Stephen Spick
Classification	Confidential

Author

Author(s)	Job Title
Stephen Spick	Information Security Officer

IT Approval

Author(s)	Job Title
Mark Brincat	Chief Technology Officer

Legal Approval

Author(s)	Job Title
Emmy Hackett	General Counsel, Chief Compliance Officer and Global Data Protection Officer

Version History

Version	Summary of Changes	Issue Date
0.1	Creation of Information Security document following the separation from Gartner	29 March 2018
1.0	Approved version.	3 April 2018
2.0	Updated to reflect Cloud hosting	3 July 2018
3.0	Updated for Legal compliance and infrastructure upgrades	31 Oct 2018
3.1	Updated to include AWS backup locations	21 March 2019
3.2 - 3.6	Updated following AWS migrations	16 Sept 2019
3.7	Updated for Aspiring Minds	3rd Jan 2020
3.8	Updated following Schrems II Ruling	2nd April 2021

Please note that printed versions of this document are uncontrolled.

Message from the Chief Technology Officer

The confidentiality of our client's information is extremely important to us. Our systems and policies have been developed to protect our clients' information as well as our own intellectual property.

We have implemented a comprehensive Information Security Program to prevent unauthorized access to client information and to protect against evolving threats. We employ a defense-in-depth strategy, which means that multiple layers of security protect our data assets. The technology layers include firewalls, intrusion prevention systems, log monitoring, real time alerts, vulnerability scanners, and anti-virus protection.

The technical security solutions are complemented by industry-standard policies and best practices. Need-to-know and principle-of-least-privileges practices are followed throughout the organization. We maintain multiple industry-standard certifications in diverse service areas. We follow ISO international standards for information security, business continuity, and service management. Our Information Security Program is continually reviewed and validated by independent regulatory institutions and third-party security assessments organizations to ensure that we continue to meet or exceed security expectations.

We actively promote compliance with laws and regulations in various jurisdictions as well as our company policies. Our security policy and processes are designed to address the requirements of the European General Data Protection Regulation, which applies to many of our clients as data controllers. We recognize client and business information security as a top priority.

Thank you for your interest in the Information Security Program at SHL. The security booklet that follows provides an overview of our program. If you have any questions, please do not hesitate to contact the information security team.

Mark Brincat
Chief Technology Officer

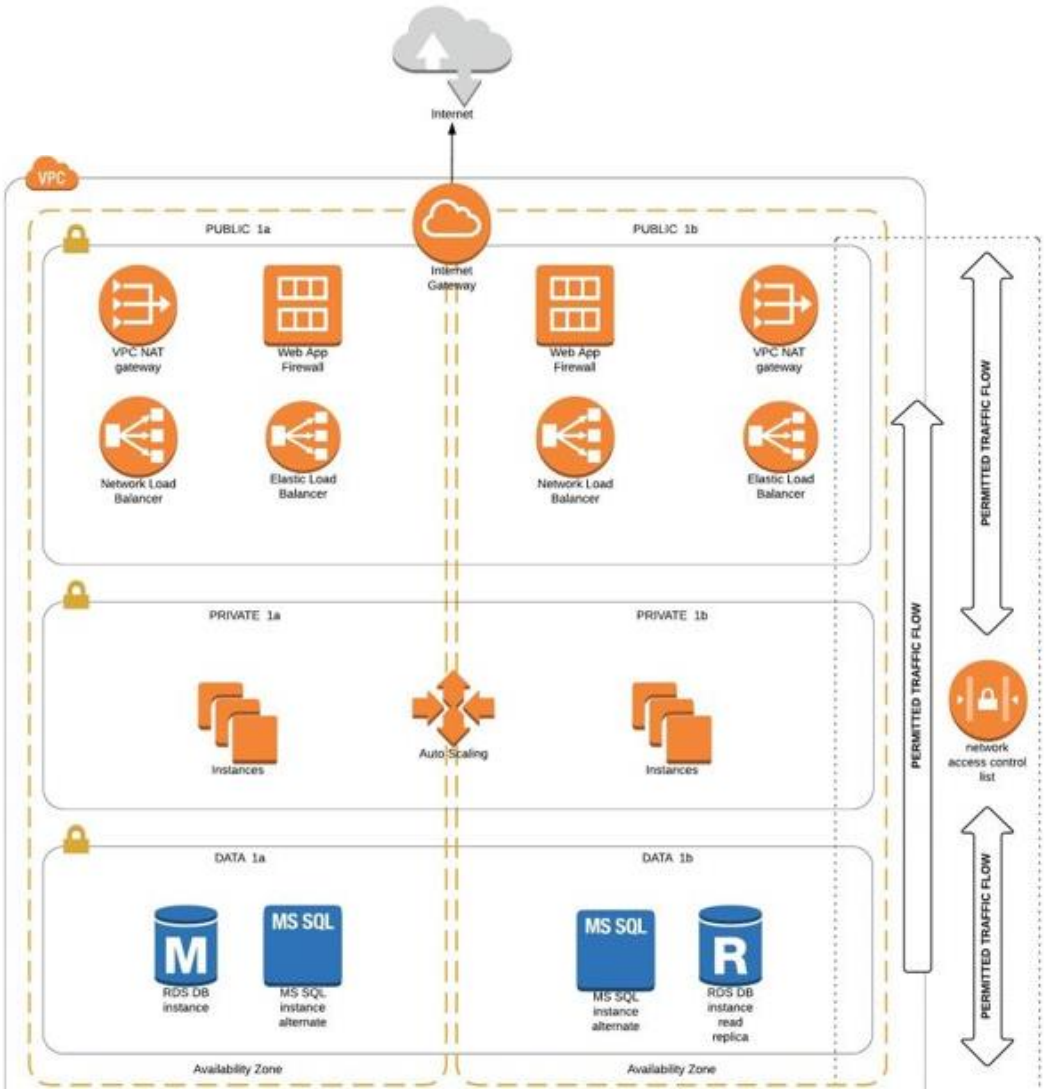
E-Mail: mark.brincat@shl.com

---

1. Introduction

SHL stands for great assessment. As the global leader in talent innovation we help organizations and their leaders address the most pressing talent priorities by providing an unparalleled view of their workforce. Our unrivalled assessment service, benchmark data, extensive and analytic technology enable companies to influence genuine organizational change and drive tangible business outcomes from having the right people in the right roles at the right time.

This document explains SHL's approach to information security and describes the processes and technologies used to protect information and information systems. It answers questions that our clients regularly ask to satisfy their legal and regulatory requirements.



2. Information Security Program

SHL's operations depend on complex, interconnected information technology systems and networks. To protect the confidentiality, integrity, and availability of these systems, networks, and the data that they store, process, and transmit, SHL has implemented a layered defense strategy. We rely on technology and human processes to safeguard our client's data at all layers of the enterprise.

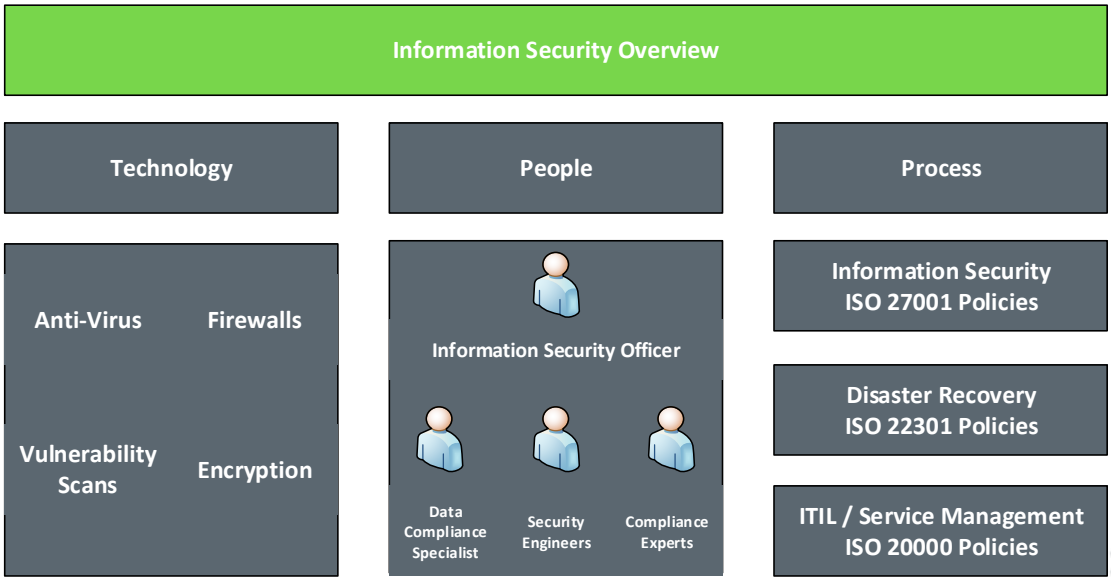
Our strategy is to balance the strength of our technical controls with their usability. Our strategy ensures appropriate controls are embedded within the process, starting with design and moving on to operations. The goal of the information security team is to counter the security threats to our client information we store, process, and transmit.

Our Staff

SHL Information Security Officer leads our information technology security team. It consists of a security engineering, IT security operations, identity and access management, policy and compliance, and business continuity and disaster recovery expertise. The team's certifications and involvement with industry forums demonstrate our proactive approach to understanding the current threats and protecting our environment against them.

All SHL staff are subject to the SHL Code of Conduct. The Code sets forth the laws and regulations that our staff need to follow in all countries in which we do business. All staff are required to acknowledge their consent to the Code and abide by its terms. The Code includes the Company-wide Data Protection and End User Acceptable Use Policy, which details each employee and contractor's responsibility around use, handling and security of all data, including client data, throughout our business processes.

SHL requires all staff to use our company assets in an effective, efficient, and ethical manner. Our commitment is to avoid risks to the company or an individual from improper activities as a result of inadvertent or deliberately improper use. To ensure all staff understand their responsibilities, we have an acceptable use policy in place and we issue the acceptable use policy to all our staff and contractors.



3. Third-Party Audits and IT Security Assessments

SSAE 16/SOC 2 Type II

SHL's commitment to a secure operating environment is demonstrated by our ongoing certification program. Our systems are located at secure third-party cloud facilities that provides high-availability, flexibility, scalability, and cost effectiveness to support SHL services. All AWS locations are SSAE 16/SOC 2 Type II compliant.

Further information about AWS compliance programmes can be found here.

Transfer of Data

To provide platform availability 24x7 SHL operates a follow the sun support model with support staff in the UK, USA, India and South Africa. This support outside of the EU is critical to supporting and maintaining our online assessment platform. Whilst this access is limited, we do recognise it is still considered a transfer under European Data Protection Law. SHL has the Intragroup Agreement in place, signed by all SHL affiliates, which contains the European Union (**EU**) Standard Contractual Clauses (**SCCs**) which have been approved by the EU data protection authorities for the transfer of data outside the EEA. We are also happy to enter into the SCCs with any clients. Our third party vendors and service providers are also required to sign up to SCCs in accordance with Article 46 of the General Data Protection Regulation. All SHL affiliates have the same technical, physical, and administrative security controls and are required to comply with our data protection policies and procedures, applicable laws, governing the collection and use of personal information.

Monthly Vulnerability Assessments

SHL employs a CREST certified organisation to perform third-party web application testing across key Internet-facing applications. In addition to common application vulnerabilities, these scan covers the OWASP Top Ten website security flaws as well.

3rd Party Penetration Testing

SHL have partnered with a Penetration Testing company to complete penetration tests on SHL Applications at least annually.

International Organization for Standardization (ISO)

ISO is an independent, nongovernmental membership organization—is the world's largest developer of voluntary international standards. ISO International Standards ensure that products and services are safe, reliable, and high quality. These standards are strategic tools that reduce costs by minimizing waste and errors and increasing productivity. They help companies access new markets, prevent trade barriers for developing countries, and facilitate free and fair global trade.

ISO 27001: Information Security

SHL understands that the confidentiality, integrity, and availability of information processed by the organization is of extreme importance to its current and prospective clients. Furthermore, the intellectual property SHL holds and the software products it develops are essential to the future success and growth of the company. SHL has developed and implemented an information security management system (ISMS) and has maintained certification to ISO 27001 since 2010

ISO 22301: Business Continuity

SHL's Business Continuity Management process identifies potential threats to the organization and the impact if these threats materialize. It requires that we build resilience by developing and implementing business continuity and disaster recovery plans. For these efforts, SHL's IT department has attained ISO 22301 certification, which assures our clients that we have robust best practices in place to continually deliver our products and services. SHL have maintained our ISO 22301 certification since 2014.

ISO 20000: Service Management

SHL's IT department is also ISO 20000 certified which demonstrates our ability to professionally maintain, support, and manage our IT services using best practices. ISO 20000-1 is a very broad standard that covers a variety of areas, such as Incident Management, Capacity Management, Internal Audit Process, Change Management, and Problem Management. SHL have maintained our ISO 20000 certification since 2014.

External Audit

At SHL, an external audit firm reviews controls annually as part of financial auditing. The control review includes, but is not limited to, logical access, change control, system documentation, data flow, and change and problem management.

As part of the SHL Information Security policy and as part of our ISO certifications, we complete external audits annually.

Internal Audit

Quarterly, our Internal Audit reviews IT controls throughout our Information Technology system and our business. These controls include perimeter device admin access and access controls, incident handling and corresponding service-level agreements, and physical access to restricted areas.

Vendor Assessment

SHL has strong governance controls to assess our vendor partners. We hold third-party vendors to the same high security standards as our own. The information security team incorporates a risk assessment at the beginning of every partner or vendor engagement. It performs vendor risk assessments according to the security profile of the services offered and data shared.

Vulnerability Scanning

SHL's information security team has established a disciplined, programmatic approach to discovering and mitigating threats and vulnerabilities. A multifaceted approach to threat and vulnerability analysis and management is critical because, as defenders, we are committed to protecting against all information attacks. Two types of vulnerability scans are performed across SHL: web application scans and network and systems scans.

Cyber Essentials Plus

Cyber Essentials Plus is a UK Government-backed, industry-supported certification scheme introduced in the UK to help organizations demonstrate operational security against common cyber-attacks. The independent assurance process works for Cyber Essentials Plus certification through an annual external assessment conducted by an accredited assessor.

It demonstrates the baseline controls SHL implements to mitigate the risk from common Internet-based threats, within the context of the UK Government's "10 Steps to Cyber Security".

CSA Security Trust Assurance and Risk (STAR) …. Security on the Cloud Verified.

In addition to SHL other security certifications SHL are now certified to CSA STAR Security Program - https://cloudsecurityalliance.org/star/registry/?name=SHL. The STAR program enables SHL to validate their cloud security and provide proof to current and future customers.

This provides further competitive advantage and demonstrates to our clients that following the migration to AWS our cloud security continues to meet the high standards we have set.

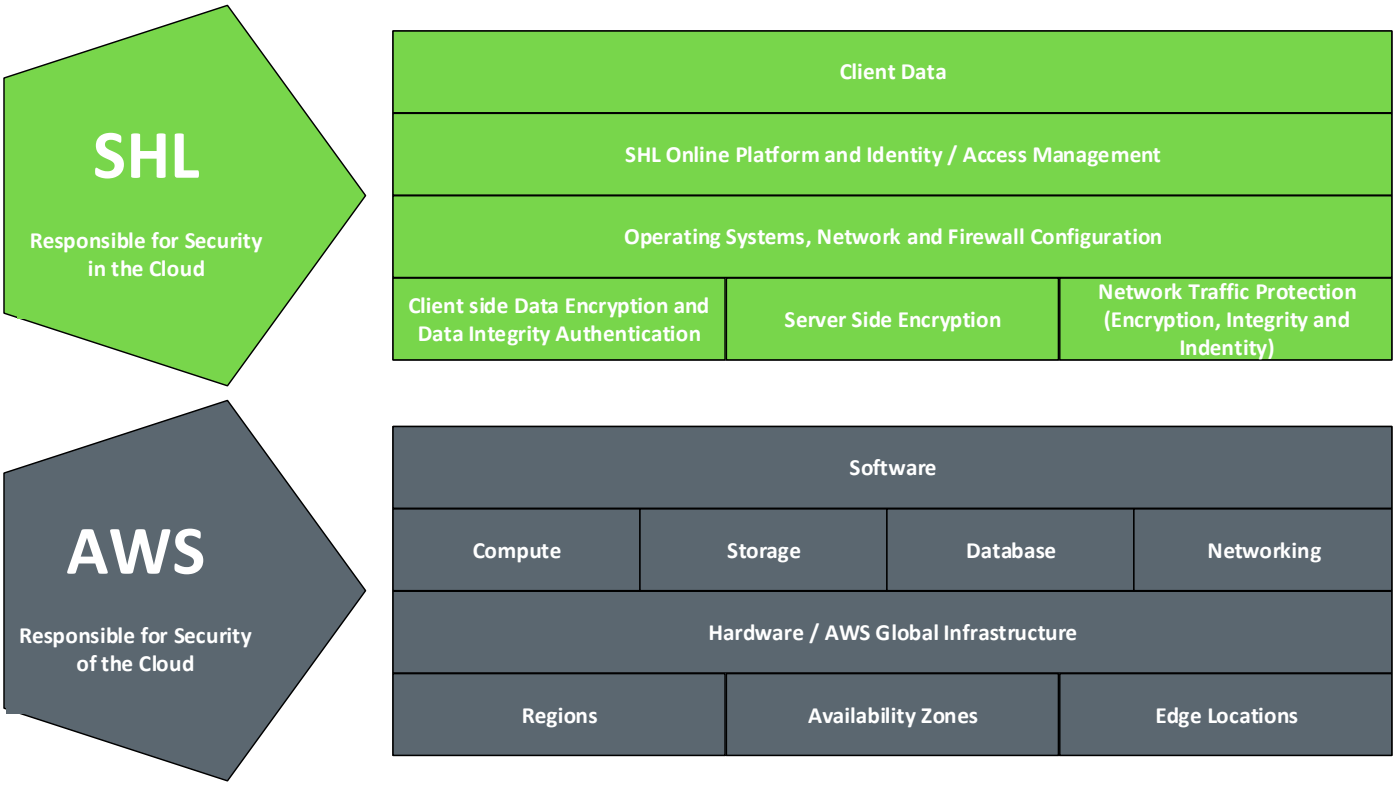
4. Data Centre Security

SHL utilises Infrastructure as a Service (IaaS) from AWS to provides its assessment services via a technology infrastructure and support services that provide world class:

- Availability,
- Security,
- Reliability,
- Performance, and
- Scalability.

SHL engineers infrastructure with reliability and availability in mind. We have redundant processing systems, databases, and networks so no single component can bring the system down. At the web service level, our redundancies allow us to sustain multiple failures before system performance degrades.

Information security policy covers awareness of threats from the environmental to the geopolitical.



Certification

All of AWS regions are both ISO 27001 and SSAE 16/SOC 2 Type II certified.

Further information about AWS compliance programmes can be found here.

SHL utilises the following AWS regions

Operating Region	AWS Data Site	AWS Backup Location
Europe, Middle East, India and Africa	EU: Frankfurt | EU-CENTRAL-1	EU: Ireland | EU-WEST-1
Americas (US, Canada, Central and South America	USA: Ohio | US-EAST-2	USA: N. Virginia | US-EAST-1
Australia and Asia	Australia: Sydney | AP-SOUTHEAST-2	EU: Ireland | EU-WEST-1
China	China: Ningxia | CN-NORTHWEST-1	China: Beijing | CN-NORTH-1
Global SHL Operational	Ireland | EU-WEST-1	

5. Information Risk Management

SHL maintains a comprehensive risk assessment and management capability. Our information security policy breaks down risk management into three key components: assessment, reduction, and monitoring. The policy focuses on identifying and documenting risks pertaining to all major business processes at SHL and, wherever feasible, implementing activities to reduce risk to an acceptable level. The process incorporates several aspects of the business, from information assets to personnel. Identified risks are reported internally and presented to the board of directors.

The information security team works closely with all internal departments and product groups, consulting with technical architects, project managers, developers, and process owners to ensure they perform a review and properly implement all security controls. The information security team owns, manages, and reviews any risk identified in this process.

The team performs IT risk assessments on systems and data products that process, store, or transmit information assets. Business unit managers employ risk assessment and analysis techniques to ensure correct controls are in place in their area of responsibility.

When an appropriate information owner or asset owner has been determined, the team mitigates risk based on an assessment that clearly indicates an unacceptable level of risk exists for the information assets under their control.

The team monitors risk at a frequency commensurate with the potential risk exposure of each business unit.

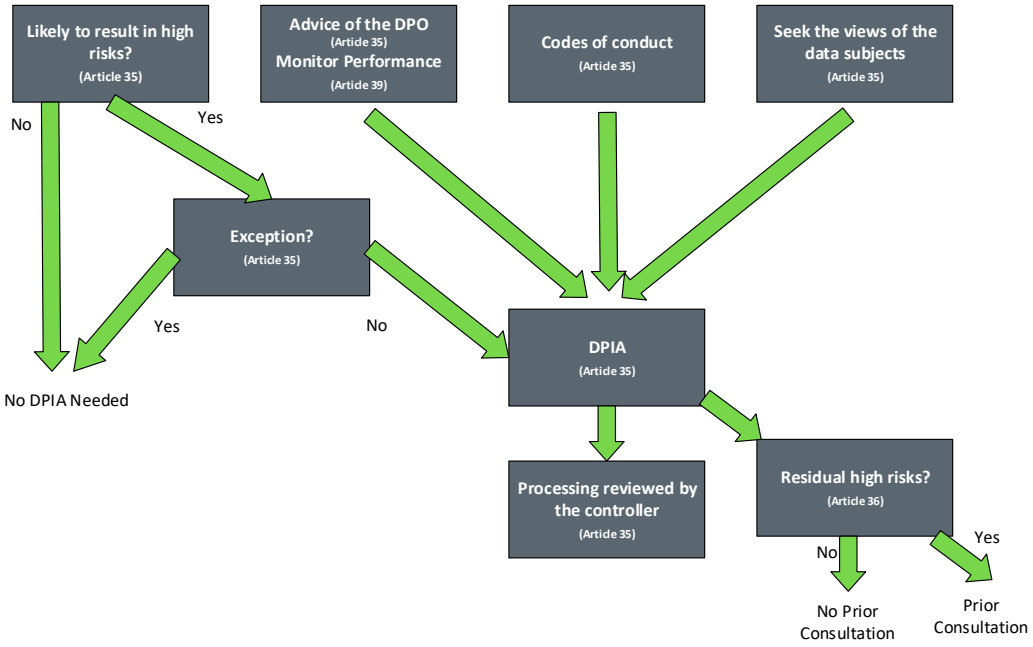
Risk Management Process
Illustrative

6. Data Protection Program

SHL recognizes the importance of having effective and meaningful privacy protections to govern the collection, use, analysis, processing, and disclosure of confidential information, including (but not limited to) personal information. Our data protection program is consistent with our obligations to our clients, and employees under all applicable data protection laws, including the EU General Data Protection Regulation, and the terms of our client contracts. All SHL entities have the same technical, physical, and administrative security controls and are required to comply with our data protection policies and procedures, applicable laws, and the terms of our client contracts. SHL has an Intragroup Agreement in place (signed by all SHL entities) containing the European Union ("EU") Standard Contractual Clauses, which have been approved by the EU data protection authorities for the transfer of data outside the European Economic Area.

SHL continues to maintain its Privacy Shield certification but SHL does not rely on EU-U.S. Privacy Shield to transfer data that originated in the EEA or the UK to the US.

SHL maintains a comprehensive and systematic monitoring of data protection practices for business continuity and ongoing changes to the business. SHL conducts Data Protection Impact Assessments on changes which may affect processing activities when the processing could result in a high risk to the rights and freedoms of data subjects following the structure below.



SHL maintains a personal data breach register for monitoring and identification of trends for continuous improvement activities. This includes a model which indicates where the use of the Incident Response Plan is necessary against the severity of the breach. Within the Incident Response Plan are the roles and responsibilities for registration and notification to a supervisory authority and, if appropriate, notification to data subjects affected in appropriate timescales.

A list of sub-processors SHL utilises to process client data is available in section 8.

With respect to our data protection and data use policy for other public facing activities, which are not directly covered by this document, please refer to our Privacy Policy at www.shl.com.

7. Data Storage Locations

The following table identifies the locations where the various SHL Client platforms store data:

Data Infrastructure			
Platform Operations and Services Delivery	SHL operates its infrastructure globally and determines the primary data storage location based on two criteria selected by the client: • The on-line assessment platform; and • The geographic instance of the selected on-line assessment platform Please see the data storage location chart below for specifics. ****IMPORTANT: This chart addresses data infrastructure and <u>storage</u> locations. Questions regarding processing of data for a particular client should be referred to the Legal Department.**		
System	**SHL Server**	**Production Data Location**	**Disaster Recovery Location**
TalentCentral	USA	USA	USA
	EU	Germany	Ireland
	CN	China	China
	APAC	Australia	Ireland
MFS	EU/USA/APAC	Germany	Ireland
iAssess	USA	USA	USA
	EU	Germany	Ireland
	CN	China	China
	APAC	Australia	Ireland
Mobilise	USA	USA	USA
	EU	Germany	Ireland
	CN	China	China
	APAC	Australia	Ireland
Development Coach	EU/USA/APAC	Germany	Ireland
SHL Online	EU/USA/APAC	Germany	Ireland
Sunstone	EU/USA/APAC	USA	USA

Brainbench	EU/USA/APAC	USA	USA

8. Sub Processors

The following sub processors are used by SHL.

Sub Processors			
	**IMPORTANT: This chart only applies to data storage locations. Any questions about the type of data stored please contact the SHL Legal team.		
Type	**Product**	**Description**	**Data Storage Location**
CRM	Salesforce	Store of marketing contacts and support cases	UK
Email	Microsoft Office 365	Emails to and from SHL (SHL Online Applications are sent directly from the platform within AWS)	USA and UK
Customer Contact Centre – Voice	New Voice Media	Phone system used for SHL Customer Support Centre	UK
CSAT Tool	Qualtrics	Customer Satisfaction survey data	UK
Marketing Tool	Eloqua	Sending marketing emails to contacts who have requested information	Canada
Hosting	AWS	Hosting of SHL systems.	Germany, Ireland, USA, Australia, China

9. Policies and Procedures

SHL's policies are closely aligned with international standard IS0 27001. This standard was originally developed to provide controls for best practices in information security and has evolved as a reference to maintain confidentiality, integrity, and availability of information systems.

Access Control

All information networks, regardless of connectivity and whether SHL-owned, leased, or contractor operated, must be protected from unauthorized access. Information networks include all intranets, extranets, local area networks, wide area networks, metropolitan area networks, and value-added networks. This policy applies to all individuals and software programs that access or administer access to information resources.

SHL information resources are essential to its success. Therefore, we grant controlled access to information resources based on business requirements. The overall strategy is that access is strictly forbidden unless explicitly granted. There is no implicit right of access.

Asset Management

The asset management policy at SHL defines the requirements for asset classification and controls. An asset is defined as any tangible or intangible item owned or controlled by SHL. This includes logical assets, such as intellectual property and data, and physical assets, such as equipment. This policy applies to all users of SHL assets.

SHL assets must be accounted for and controlled in a consistent manner. These assets are crucial to SHL's success and must be protected by the proper controls to minimize any risk of harm, disruption of services, or disclosure of sensitive information.

Capacity Management

For robust service delivery, information systems must meet anticipated capacity requirements at SHL. The system's development and operational teams are responsible for determining anticipated hardware requirements and capacity and for monitoring system capacity performance. This includes disk usage and size, network traffic load, load balancing, necessary processing power, and necessary memory requirements.

Data Retention and Destruction

Corporate information in all its forms is deemed to be a SHL asset. As with any asset, protection from theft, damage, destruction, modification, or unauthorized use is necessary to SHL's ongoing success. Any SHL information processing equipment that is to be disposed of or reused must undergo a cleansing process before release. The cleansing process

must consist of the destruction of the information residing on equipment, validation of the process, and testing to ensure no data is left on the equipment.

The data destruction policy defines the requirements for the destruction and disposal of electronic media in line with the requirements of the information security management system. The requirements for the disposal and destruction of paper records are defined within the information classification policy

Encryption

To safeguard SHL information, we use cryptography as feasible to reduce the risk of disclosure. The task includes configuring computers with SHL-approved encryption software and approving encryption products and algorithms to mitigate the risk of data exposure.

All SHL entities utilizing and supporting cryptography ensure they are in compliance with the encryption policy, ensure that data that is encrypted can be decrypted, and protects keys from misuse or compromise.

All three information classification levels—restricted, confidential, and public data—are encrypted whenever transmitted externally over any untrusted electronic communication system. Confidential and restricted data are encrypted for transmission within the internal network and externally to the extent operationally feasible.

Incident Management

SHL's incident management policy serves as a formal process for reporting, investigating, and analyzing all information security events, weaknesses, and incidents. The policy further ensures that lessons are learned so preventive controls can be identified and implemented.

In addition to the policy, SHL also has a comprehensive incident response process based on industry best practice.

Password Policy

At SHL, password complexity is enabled for all user and network accounts. Passwords expire every 90 days with a password history of the last 24 passwords used. Accounts lock after 10 failed password attempts in a predefined time period.

Problem Management

SHL has a problem management process based on ITILv3 foundations and best practices. SHL uses this process to diagnose the root cause of incidents, determine the resolution to those problems, and ensure the resolution is implemented through appropriate control procedures. Internal and external auditors monitor SHL's compliance with the problem management process.

Change Management

SHL has an ISO 20000 certified change management process based on ITILv3 foundations and best practices. We document and categorize change requests to monitor and implement hardware and software changes.

All submitted changes go through a weekly change advisory board meeting for review and approval and are captured and recorded. Internal and external auditors monitor SHL's compliance with the change management process.

Account Management

SHL automatically creates and disables unique user accounts based on an employee's status in our HR system. Access control follows the principle of least privilege. The employee's manager requests access to data, elevated privileges, and other special access through an additional access form. The account management team reviews the request and processes it after obtaining the appropriate approval.

SHL restricts access to confidential, sensitive, and personal data to individuals on a need-to-know basis, approval for which must be given by the individual's manager.

10. Software Development Life Cycle

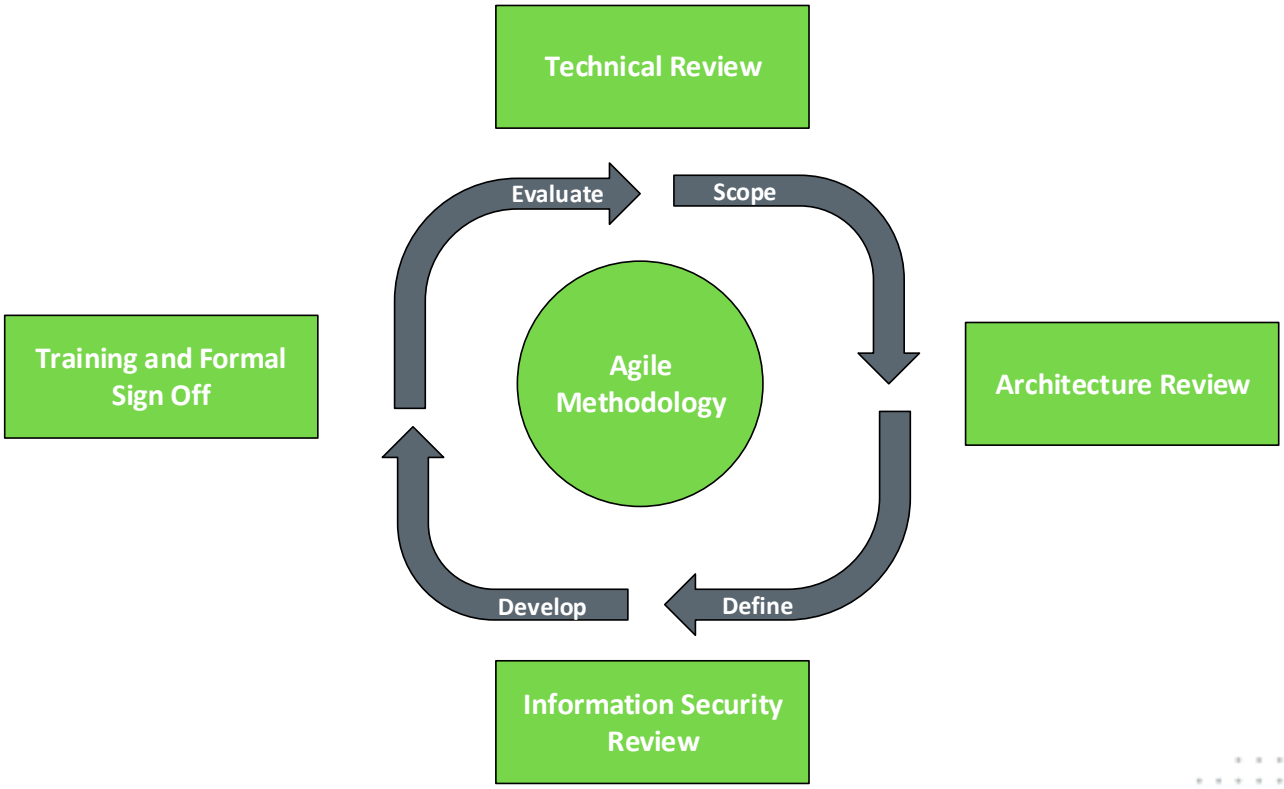
Agile development is an umbrella term for several of SHL's iterative and incremental software development methodologies. Agile methodology fundamentally incorporates iteration and continuous feedback to successively refine and deliver a software system. All processes involve continuous planning, testing, integration, and other forms of continuous evolution of both the project and the software. They are all lightweight (especially compared to traditional waterfall-style processes) and inherently adaptable, and they all focus on empowering people to collaborate and make decisions together quickly and effectively.

Security is integral to the development of SHL products. A software development life cycle follows a security review process that is part of our overall project management function. Security review includes technical review, architecture review, security checklists, and formal sign off. The security team defines and provides the standards and creates secure products for our clients.

We have a comprehensive security testing capability from infrastructure scanning to web application scanning. We conduct third-party web penetration tests to mitigate threats.

We provide appropriate training for our development staff in secure development, design, and testing of our products is provided on an ongoing basis.

Software Development Life Cycle
Illustrative



11. Business Continuity and Disaster Recovery

SHL maintains business continuity and disaster recovery plans and annually tests these plans. SHL's business continuity and disaster recovery program focuses on people, process, and technology throughout events and post-recovery. It also introduces key preventative dependency technologies such as fault tolerance, high availability, virtualization, stand by, and extreme replication environments. The integrated business continuity and disaster recovery program, in conjunction with other organizational information, has also become a key corporate asset and part of our value proposition.

SHL's business continuity policy aligns with the industry standard ISO 22301.

Business owners review and update business continuity plans annually or as business processes change. We base our business continuity and disaster recovery program on portions of a number of standards including ISO 22301, the Business Continuity Institute, ASIS SPC.1-2009, NFPA 1600, and the FFIEC IT guidelines. Business continuity plans for mission critical and mission essential business processes utilize business continuity teams—each operating remotely—to maintain business processes during and after incidents. The individual business process is responsible for determining the composition of the business continuity teams.

Business owners test selected platforms annually for recovery within a predefined service-level agreement. The system architecture teams develop a solution that leverages the high availability of the cloud.

12. Security Training and Awareness

SHL trains staff in its privacy and data security policies and procedures. Such training is conducted on an annual basis at a minimum. All staff are required to take online training modules that cover varying aspects of information security, physical security, privacy, and other security domains annually. New hires receive training within three months of joining SHL.

For new staff, these modules are part of the on boarding process. Existing staff must recertify every year. Human Resources handles course delivery and content, and consults domain subject matter experts for content and review. We outline our training below.

Preventing Discrimination and Harassment

All SHL staff have a right to expect fair and non-discriminatory treatment, a responsibility to uphold these standards themselves, and an obligation to take appropriate action when they believe these standards may have been violated. This training module helps SHL employees better understand and recognize discrimination and harassment and know the appropriate steps to take when they observe or learn of inappropriate conduct.

Global Anti-Corruption

We hold all SHL staff to strict requirements to align our business practices with the requirements of US law, UK law, and other rules governing bribery and corruption. This training module helps SHL employees identify situations that can raise bribery and corrupt practices concerns.

Global Data Protection

All SHL staff participate in annual data protection training to ensure that staff understand the legal requirements under the European Union General Data Protection Regulation as well as the data protection requirements of other jurisdictions, such as the US, Australia, Canada and South Africa, for the collection, use, storage and retention of personal information of our staff, clients and candidates.

Cyber-Security

We include all SHL staff in training to ensure that our commitment to data security and proper information practices are part of their understanding around handling client information. Our cyber-security training focuses on foundational concepts such as internal and external threats to systems and data, and what to do when a breach happens. Staff will uncover specific ways data and systems can be breached, and learn essential practices for passwords, email usage and technology to protect digital information and physical access.

13. Technical Security Controls

Server Protection

We deploy standard security builds throughout SHL's infrastructure. Our server builds are based on industry best practices. Server protection is in line with SHL's overall strategy of defense in depth. Protection encompasses server hardening, network security, system integrity monitoring, and auditing capabilities.

Workstation Protection

SHL uses industry standard products to protect workstations. The team deploys anti-virus software on all systems and installs full disk encryption and host-based intrusion preventions systems (IPS) with stateful firewalls on laptops. Every workstation has a password-protected screensaver.

Anti-Virus

All devices are run Anti-Virus / Anti-Malware software which covers the following aspects.

- Machine learning and artificial intelligence detect known and unknown ransomware
- Behavior-based indicators of attack (IOAs) prevent sophisticated fileless and malware-free attacks
- Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
- Threat intelligence prevention blocks activities known to be malicious

Intrusion Prevention System

SHL has signature and behavioral-based detections using IPS that are distributed at all Internet inbound and outbound connections. IPS tuning helps us ensure alerts are real and actionable.

Patch and Vulnerability Management

SHL reviews patches and vulnerabilities regularly and notifies the applicable teams. We provide action items and remediation activities where applicable. The team rates patches based on risk and exploitability. Based on these ratings, remediation time frames range from one week to one month.

Wireless Networks

We segment wireless networks as DMZ networks hosted on firewall enclaves independent of server production networks. In addition, wireless networks also utilize network admission control for role-based access. WPA2 Enterprise with AES-256 bit encryption is used to secure wireless connections.

Firewall Management

SHL follows a default deny policy for all inbound and outbound Internet connections. Upon request from a SHL business sponsor, explicit permit statements are enabled to permit access to systems and applications that provide services directly to remote staff or SHL clients. Permit statements in this context are always configured as specifically as possible. Permissive permit statements ensure end users and systems are able to access Internet systems using approved protocols.

Data Loss Prevention

SHL's data loss prevention policy prevents accidental or intentional leakage of sensitive information and client data from SHL's network, thus maintaining our clients' trust. It works in the background to ensure that sensitive information and client data is securely handled by using government-level encryption. This encryption also ensures data confidentiality if a device with sensitive or client data is lost or stolen.

Remote Access / Access to Internet

Remote Access VPN utilizes AES-256bit encryption and requires two-factor authentication before a user can connect. SHL uses the ZScaler VPN platform over SSL, providing secure access to applications.

Access to Internet is limited via Zscaler ZIA which allows SHL to apply restrictions to the categories of websites that users can connect to and also provides the additional protection

- IPS & Advanced Protection - Delivering full threat protection from malicious web content like browser exploits, scripts, and identify and block botnets and malware callbacks.
- Block zero-day exploits by analyzing unknown files for malicious behaviour.
- DNS Filtering and Security - Control and block DNS requests against known and malicious destinations.

Secure Communication

By default, all email traffic from SHL systems is encrypted using TLS.

SHL also utilises MS SharePoint and MS Teams to securely share information with clients.

Security Monitoring

SHL undertakes automated and centralized checking of systems, services, and applications to ensure the effectiveness of the systems. We implement and manage network management and security tools to monitor and maintain secure systems. We also implement multiple tools to monitor system uptime, confidentiality, integrity, and availability.

System and Data Backup

SHL systems run weekly full backups with incremental daily backups. Backups are encrypted when written to an S3 bucket within AWS region. Backups are transferred securely within AWS region to be used in the event of Disaster Recovery. Backups are stored for 45 days and then are deleted from the S3 bucket.

14. Supporting Documents

ISO 27001, ISO 22301, ISO 20000 Certificates

Our ISO 27001, ISO 22301, and ISO 20000 certificates are publicly available document and can be found in Appendix A, B, and C. The current certificates are addressed to our former parent company, The Corporate Executive Board Company and are in the process of being re-issued to SHL directly.

SSAE 16/SOC 2 Type II Report

Third-party certificates can be provided upon signing a non-disclosure agreement (NDA).

Web Application Scanning Reports

These documents are company confidential and can be provided upon signing an NDA.

Policies

Specific system policies are company confidential but can be provide selected policies upon signing an NDA.

High-Level Application Diagram

A high-level application diagram can be found in Appendix D.

Appendix A: ISO 27001 Certificate

bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that:

SHL Group Limited
1 Atwell Place
Thames Ditton
KT7 0NE
United Kingdom

Holds Certificate Number: IS 694554

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

The management of information security for the protection of assets in relation to the global provision of IT services. This is in accordance with the statement of applicability v2.1 dated 17/06/2019.

For and on behalf of BSI:

Andrew Launn, EMEA Systems Certification Director

Original Registration Date: 2018-10-19
Latest Revision Date: 2021-01-04

Effective Date: 2019-09-01
Expiry Date: 2022-08-31

Page: 1 of 2

...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsigroup.com/ClientDirectory

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

Appendix B: ISO 22301 Certificate

bsi.

Certificate of Registration

BUSINESS CONTINUITY MANAGEMENT SYSTEM - ISO 22301:2012

This is to certify that:

SHL Group Limited
1 Atwell Place
Thames Ditton
KT7 0NE
United Kingdom

Holds Certificate Number: BCMS 694556

and operates a Business Continuity Management System which complies with the requirements of ISO 22301:2012 for the following scope:

The Business Continuity Management System in relation to the global provision and continuity of IT services both internally and externally including delivery, service, support, maintenance and management. The development, management and maintenance of the BCMS.

For and on behalf of BSI:

Andrew Launn, EMEA Systems Certification Director

Original Registration Date: 2018-10-19
Latest Revision Date: 2020-06-02

Effective Date: 2020-07-18
Expiry Date: 2022-10-29

Page: 1 of 2

...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsigroup.com/ClientDirectory

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

Appendix C: ISO 20000 Certificate

bsi.

Certificate of Registration

IT SERVICE MANAGEMENT SYSTEM - ISO/IEC 20000-1:2018

This is to certify that:

SHL Group Limited
1 Atwell Place
Thames Ditton
KT7 0NE
United Kingdom

Holds Certificate Number: ITMS 694555

and operates an IT Service Management System which complies with the requirements of ISO/IEC 20000-1:2018 for the following scope:

The service management system of SHL supporting the internal provision of IT services from its global offices, in accordance with the service catalogue.

For and on behalf of BSI:

Andrew Launn, EMEA Systems Certification Director

Original Registration Date: 2018-10-26
Latest Revision Date: 2020-06-02

Effective Date: 2020-07-28
Expiry Date: 2023-07-27

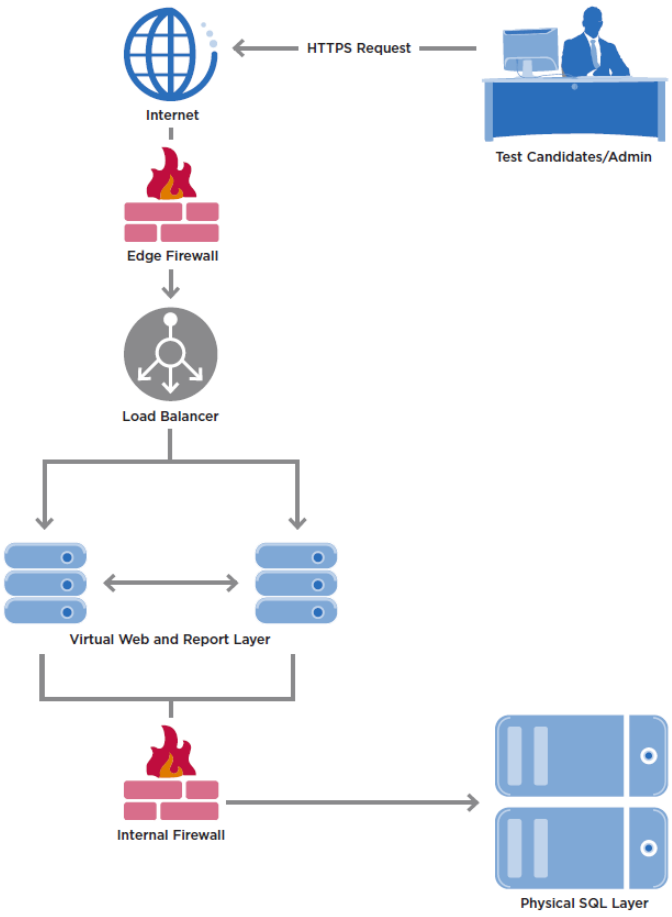
Page: 1 of 2

...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsigroup.com/ClientDirectory

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

Appendix D: High-Level Application Diagram



Review and Maintenance

This policy shall be reviewed by the Chief Technology Officer as is deemed appropriate but no less frequently than every 12 months.

Any changes to this policy shall be approved by the SHL Legal Department.

