dun & bradstreet

Information Security

Statement of Applicability for the UK & Ireland business

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
A.5 Information security Policies	**Management direction for information security**	**5.1**	**Objective:**	**To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.**
	Policies for Information Security	5.1.1	Yes	We have a set of policies that are approved by management that are referenced in this Statement of Applicability. We also have a high-level global framework and policy for Information Security to support our ISMS. It is adopted by our UK Leadership and applies to all team members and contractors in the UK.
	Review of the policies for information security	5.1.2	Yes	All our policies follow a standard format which includes details of the policy owner(s) coordinator(s) & approver(s). All policies reviewed annually or sooner if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
A.6 Organization of information security	**Internal organization**	**6.1**	**Objective:**	**To establish a management framework to initiate and control the implementation and operation of information security within the organization.**
	Information Security Roles and Responsibilities	6.1.1	Yes	Responsibility and accountability for the management of our global ISMS resides with our global Chief Security Officer and for the UK ISMS accountability is with the UK Managing Director with responsibility delegated to the Business Operations Leader. Individual assets have owners designated in the asset register.
	Segregation of Duties	6.1.2	Yes	Our Access Control Policy is to ensure that Conflicting duties and areas of responsibility are segregated.
	Contact with Authorities	6.1.3	Yes	We maintain contact with relevant law enforcement and regulatory bodies both in the normal course of our business and in exceptional circumstance to report security incidents or to maintain continuity of our business.
	Contact with Special Interest Groups	6.1.4	Yes	We are members of special security related interest groups and forums.
	Information Security with Project Management	6.1.5	Yes	We address information security in all projects, Information security implications are expected to be addressed and reviewed regularly in all projects.

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
	Mobile Devices and Teleworking	**6.2**	**Objective:**	**To ensure the security of teleworking and use of mobile devices.**
	Mobile Device Policy	6.2.1	Yes	Mobile devices (including Smart Phones and Tablets) are widely used in our organisation. The requirements for both company provided devices and employee owned devices are set out in our policies. Training is provided to reinforce understanding and compliance.
	Teleworking	6.2.2	Yes	Teleworking is common practice in our modern working environment. Our policies and training take into account the risks and associated controls required.
A.7 Human Resource Security	**Prior to Employment**	**7.1**	**Objective:**	**To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.**
	Screening	7.1.1	Yes	Background verification checks in line with our policy and procedure are carried out for all candidates for employment. The policy takes account of relevant laws and regulations; is proportional to the business requirements, the classification of the information to be accessed and the perceived risks to the business. We have contractual agreements with third party suppliers whose employees work at D&B premises are often referred to as contractors. Our supplier agreements with these third parties require their employees to comply with our Information Security policies and procedures.
	Terms & Conditions of Employment	7.1.2	Yes	The contractual obligations for employees and contractors engaged by Dun & Bradstreet are set out in the Terms & Conditions of Employment which all employees and directly employed contractors are required to sign before commencing employment. These terms and conditions also set out the continuing responsibilities for Information Security after employment ends. The Information Security obligations and ethical considerations required by D&B are reinforced in our Code of Conduct and Information Security Training materials. We have contractual agreements with third party suppliers whose employees work at D&B premises are often referred to as contractors. Our supplier agreements with these third parties require their employees to comply with our Information Security policies and procedures.

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
	During Employment	**7.2**	**Objective:**	**To ensure that employees and contractors are aware of and fulfil their information security responsibilities.**
	Management Responsibility	7.2.1	Yes	Being 'Data Inspired' is one of D&B's core values and the importance of data and information security is part of the culture of our business. All new employees are assessed against their terms & conditions of employment, their information security obligations and other criteria during their probationary period and throughout their employment. Management ensure that employees are trained in aspects of information security relevant to their role. We have a clear Whistleblowing process which is reinforced in our annual Code of Conduct training.
	Information Security Awareness, Education and Training	7.2.2	Yes	A program of general Information Security Awareness, Education & Training exists for all employees. Where there are role specific information security requirements, training needs are assessed and appropriate training arranged.
	Disciplinary process	7.2.3	Yes	We have a clear Disciplinary Policy and Procedure which sit along a Capability & Performance Improvement Policy and Procedure to handle circumstances where an employee who has committed an information security breach.
	Termination and Change of Employment	**7.3**	**Objective:**	**To protect the organization's interests as part of the process of changing or terminating employment.**
	Termination or Change of Employment Responsibilities	7.3.1	Yes	Processes exist to ensure employees are reminded of their obligations with regard to information security and the consequences of not meeting those obligations when they leave D&B. When employees change roles, the responsibility rests with the line manager to advise the employee of any role specific obligations.
A.8 Asset Management	**Responsibility for Assets**	**8.1**	**Objective:**	**To identify organizational assets and define appropriate protection responsibilities.**
	Inventory of assets	8.1.1	Yes	We have an Inventory of information security related assets contained in our UK Asset Register. It also references assets held on other inventories. Certain specific assets types such as software are managed by our Global Security team - specific policy is in place addressing requirements for those asset types.
	Ownership of Assets	8.1.2	Yes	All information security related assets (or groups of assets) have designated owners who are responsible for the asset throughout its lifecycle or owners for defined phases of the asset's lifecycle.
	Acceptable use of Assets	8.1.3	Yes	Acceptable use of Information Security related assets is defined in our Acceptable Use Policy and is reinforced through training and awareness courses.

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
	Return of Assets	8.1.4	Yes	Procedures are in place to ensure that Information Security related assets that are assigned to employees or contractors are returned when the contract with the employee or contractor ends.
	Information Classification	**8.2**	**Objective:**	**To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.**
	Classification Guidelines	8.2.1	Yes	Information is classified and labelled as set out in our Global Data Classification Policy. They guide asset owners and employees on the appropriate labelling of information assets.
	Labelling of Information	8.2.2	Yes	Information is classified and labelled as set out in our Global Data Classification Policy. They guide asset owners and employees on the appropriate labelling of information assets.
	Asset Handling	8.2.3	Yes	Our Acceptable Use Policy and Data Classification Policy together with our Data Handling & Destruction Standard define appropriate handling of assets & information.
	Media Handling	**8.3**	**Objective:**	**To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.**
	Management of Removable Media	8.3.1	Yes	The use, management and destruction of removable media is controlled by our Acceptable Use Policy and our Data Handling and Media Destruction Standard.
	Disposal of Media	8.3.2	Yes	Disk drives and use of USB ports for media storage devices are disabled as a standard and only enabled on exception where justification is provided and approved by GSR.
	Physical Media Transfer	8.3.3	Yes	A list of approved carriers is maintained by our GS&P team as part of our Third-Party Management & Due Diligence Policy.
A.9 Access Control	**Business Requirements of Access Control**	**9.1**	**Objective:**	**To limit access to information and information processing facilities.**
	Access Control Policy	9.1.1	Yes	Access to the network and systems is controlled by our Global Access Control Policy and Global Network Configuration Policy. User Requests are managed by our USR process controlling and limiting access to an as needed basis.
	Access to Networks and Network Services	9.1.2	Yes	
	Business Requirements of Access Control	**9.2**	**Objective:**	**To ensure authorized user access and to prevent unauthorized access to systems and services.**
	User Registration and De-Registration	9.2.1	Yes	There are global policies and standards in place, and a formal global user registration and de-registration procedure for granting and revoking access to all information technology systems and services.

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
	User Access Provisioning	9.2.2	Yes	There are global policies, standards and a formal user access provisioning process is implemented to assign and revoke access rights for all user types to all systems and services.
	Management of Privileged Access Rights	9.2.3	Yes	Allocation and use of privileges are restricted and controlled in line with our global policy.
	Management of Secret Authentication Information of Users	9.2.4	Yes	Allocation of passwords is controlled through a formal management process. Globally D&B operates a formal management process for the management and control of secret authentication information of users. For contractors and 3rd Party Vendors the contract/agreement covers confidentiality. Where access is granted to third parties it is limited in accordance with our policy.
	Review of User Access Rights	9.2.5	Yes	D&B operates a formal user registration and de-registration procedure for granting and revoking access to all information technology systems and services.
	Removal or Adjustment of Access Rights	9.2.6	Yes	D&B operates a formal user registration and de-registration procedure for granting and revoking access to all information technology systems and services.
	User Responsibilities	**9.3**	**Objective:**	**To make users accountable for safeguarding their authentication information.**
	Use of Secret Authentication Information	9.3.1	Yes	A Confidentiality Agreement is included in employee's terms and conditions of employment. Our policies and standards support this and use of secret authentication information is included in training materials. For contractors and 3rd Party Vendors the contract/agreement covers confidentiality.
	System and Application Access Control	**9.4**	**Objective:**	**To prevent unauthorized access to systems and applications.**
	Information Access Restriction	9.4.1	Yes	Access to information and application system functions by users and support personnel is restricted in accordance with the defined access control policy.
	Secure Log-on Procedures	9.4.2	Yes	Access to operating systems is controlled by a secure log-on policy.
	Password Management System	9.4.3	Yes	Systems for managing password is interactive and ensure quality password
	Use of Privileged Utility Programs	9.4.4	Yes	The use of utility programs that might be capable of overriding system and application controls is restricted and tightly controlled
	Access control to program Source Code	9.4.5	Yes	Access to program source code is restricted.

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
A.10 Cryptography	**Cryptography Controls**	**10.1**	**Objective:**	**To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.**
	Policy on the use of Cryptography Controls	10.1.1	Yes	D&B operate formal policies, standards and procedures on the use of cryptography controls for the protection of its information.
	Key Management	10.1.2	Yes	A policy, and associated procedures and standards, in relation to the use, protection and life cycle of cryptographic keys has been developed and implemented throughout the whole lifecycle.
A.11 Physical and Environmental Security	**Secure Areas**	**11.1**	**Objective:**	**To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.**
	Physical Security Perimeter	11.1.1	Yes	Physical perimeter security is defined by an managed in accordance with our Physical Security Policy. Additional documented information supports the execution of the policy. The premises and secure working areas are defined.
	Physical Entry Controls	11.1.2	Yes	Physical entry controls are set out in our Physical Security Policy. There is a visitor access procedure to support this policy.
	Securing Offices, Rooms and Facilities	11.1.3	Yes	Secured information processing faculties are identified and secured by access control systems in line with our policy and as set out in associated documents.
	Protecting against External and Environmental Threats	11.1.4	Yes	Protection of our facilities, in line with health and safety legislation requirements, is in place. Additional fire, heat and flood protection is active in sensitive secure areas housing essential equipment. Additional security measures are also in place at all our sites to help prevent malicious access.
	Working in Secure Areas	11.1.5	Yes	We have policies and procedures to ensure that access to secure areas is restricted on a specific needs basis and that special working procedures are in place and rigorously enforced.
	Delivery and Loading Areas	11.1.6	Yes	All deliveries in Marlow & London are made via our reception teams. In Cardiff postal deliveries are sorted by allocated team members.
	Equipment	**11.2**	**Objective:**	**To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.**
	Equipment Sighting and Protection	11.2.1	Yes	Equipment is sited or protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
	Supporting Utilities	11.2.2	Yes	Equipment is protected from power failures and other disruptions caused by failures in supporting utilities by ensuring suitable planning and architecture of infrastructure utilities.
	Cabling Security	11.2.3	Yes	Power and telecommunication cabling carrying data or supporting information services is protected from interruptions or damaged.
	Equipment Maintenance	11.2.4	Yes	Equipment is correctly maintained to ensure its continued availability and integrity.
	Removal of Assets	11.2.5	Yes	Equipment, information and software is not be taken off-site without prior authorization of their manager unless set out in policy.
	Security of Equipment and Assets Off-Premises	11.2.6	Yes	Security is applied to assets and equipment off-site, taking into account the different risks that arise outside the D&B premises.
	Secure Disposal or Re-Use of Equipment	11.2.7	Yes	Policy, process and procedures exist that ensure that all equipment reuse is managed and is disposed of securely.
	Unattended User Equipment	11.2.8	Yes	Policy, standards and training are in place to ensure that users log off or lock devices whenever equipment is left unattended so that passwords or PINs are required to reactivate sessions and that sessions should be terminated when no longer in use.
	Clear Desk and Screen Policy	11.2.9	Yes	Policy, standards and training are in place to ensure that users clear their desk of restricted information when unattended and log off or lock devices whenever equipment is left unattended so that passwords or PINs are required to reactivate sessions.
A.12 Operations Security	**Operational Procedures and responsibilities**	**12.1**	**Objective:**	To ensure correct and secure operations of information processing facilities.
	Documented Operating Procedures	12.1.1	Yes	Procedures, policies (containing procedures), training materials and other instructions / information is provided to those that need them to effectively fulfil the information security aspects of their roles. Where appropriate these documents are included in this SoA under the appropriate controls.
	Change Management	12.1.2	Yes	Policies and processes are documented to ensure that changes likely to impact information security are controlled
	Capacity Management	12.1.3	Yes	Use of resources is monitored, tuned and projections made of future capacity requirements to ensure the required system performance
	Separation of development, Testing and Operational Environments	12.1.4	Yes	Development, test and operational environments are separated by controlled access to reduce the risks of unauthorized access or changes to the operational system.

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
	Protection from Malware	**12.2**	**Objective:**	**To ensure that information and information processing facilities are protected against malware.**
	Controls against Malware	12.2.1	Yes	Where technically feasible, all D&B servers and workstations are required to have active anti-malware software that is configured in compliance with D&B corporate standards. Any server or workstation without active malware configured any-malware software may be blocked from network services until brought into compliance.
	Back-Up	**12.3**	**Objective:**	**To protect against loss of data.**
	Information Backup	12.3.1	Yes	Back-up copies of information and software are taken and tested regularly in accordance with the agreed back-up policy.
	Logging and Monitoring	**12.4.1**	**Objective:**	**To record events and generate evidence.**
	Event Logging	12.4.1	Yes	Audit logs recording user activities, exceptions and information security incidents is produced and kept for an agreed time period to assist future investigations and access control monitoring.
	Protection of Log Information	12.4.2	Yes	Logging facilities and log information is protected against tampering, unauthorized access and destruction.
	Administrator and Operator Logs	12.4.3	Yes	System Administrator/Operator activities is logged, protected from amendment by the same System/Operator Administrator and regularly reviewed.
	Clock Synchronization	12.4.4	Yes	The clocks of all relevant information processing systems are synchronized with an agreed single accurate time source.
	Control of Operational Software	**12.5**	**Objective:**	**To ensure the integrity of operational systems.**
	Installation of software on Operational Systems	12.5.1	Yes	We have policies and procedures in place to ensure the installation of software on production systems is appropriately controlled.
	Technical Vulnerability Management	**12.6**	**Objective:**	**To prevent exploitation of technical vulnerabilities.**
	Management of Technical Vulnerabilities	12.6.1	Yes	Technical vulnerabilities are identified and managed in line with our policies and processes.
	Restrictions on Software Installations	12.6.2	Yes	Only D&B approved, licensed and functionally required software is installed on end user devices.
	Information Systems Audit Considerations	**12.7**	**Objective:**	**To minimise the impact of audit activities on operational systems.**

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
	Information System Audit Controls	12.7.1	Yes	Global Security documents set out compliance requirements in all policies, standards, procedures, etc., so that implementers & management know what they will be measured against. Technical tests are included in the compliance section as well. GSR performs any number of scanning activities on systems, e.g., vulnerability scanning, compliance scanning, static code analysis, dynamic URL scanning, penetration testing as well as detective monitoring on servers and end point systems (e.g., laptops).
A.13 Communications Security	**Network Security Management**	**13.1**	**Objective:**	**To ensure the protection of information in networks and its supporting information processing facilities.**
	Network Controls	13.1.1	Yes	D&B maintain appropriate controls and procedures to ensure the consistent and secure operations of the network and related components.
	Security of Network Services	13.1.2	Yes	D&B ensure security is considered and addressed in all network service agreements.
	Segregation in Networks	13.1.3	Yes	Networks are segregated as much as practical to prevent access overlap and to minimise impact of any incident to a network.
	Information Transfer	**13.2**	**Objective:**	**To maintain the security of information transferred within an organization and with any external entity.**
	Information Transfer Policies and Procedures	13.2.1	Yes	Formal transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities. Security training re-enforces our policies.
	Agreements on Information Transfer	13.2.2	Yes	Agreements are in place between D&B Global and 3rd party Vendors and Business Partners.
	Electronic Messaging	13.2.3	Yes	Information involved in electronic messaging is appropriately protected.
	Confidentiality or Non-Disclosure Agreements	13.2.4	Yes	Confidentiality and non-disclosure agreements are established and used where appropriate to protect information.
A.14 System Acquisition, Development and Maintenance	**System Requirements of Information Systems**	**14.1**	**Objective:**	**To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.**
	Information Security Requirements Analysis and Specifications	14.1.1	Yes	Statements of business requirements for new and information technology systems, or enhancements to existing information technology systems specify the requirements for security controls.

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
	Securing Application Services on Public Networks	14.1.2	Yes	All systems and supporting infrastructure that engage in e-commerce is designed, developed and operated in a manner that appropriately protects the interests of D&B and its customers.
	Protection Application Services Transactions	14.1.3	Yes	Information involved in application service interactions is protected to ensure that its confidentiality, availability and integrity is, by design and overall architecture, protected.
	Security in Development and Support	**14.2**	**Objective:**	**To ensure that information security is designed and implemented within the development lifecycle of information systems.**
	Secure Development Policy	14.2.1	Yes	Development of software within the organisation is set out in our policy for secure application development. We have Support Service Agreements with other parts of our organisation to ensure this is applied where software is being developed. Third Parties are required to meet our standards as set out in our Third-Party Management Policy.
	System Change Controls Procedures	14.2.2	Yes	System changes are controlled by policies and implemented following process and procedure.
	Technical Review of Applications after Operating Platform Changes	14.2.3	Yes	When operating platforms are changed, business critical applications are reviewed and tested to ensure no adverse reactions to operations or security.
	Restrictions on changes to Software Packages	14.2.4	Yes	Changes to software packages are discouraged, limited to necessary changes and effective software change control.
	Secure System Engineering Principles	14.2.5	Yes	Software security standards are in place to ensure that systems are designed, developed, implemented, maintained and documented consistently in accordance with security requirements.
	Secure Development Environment	14.2.6	Yes	Secure development environments for system development and integration cover the entire system development lifecycle in line with our policy for secure application development.
	Outsourced Development	14.2.7	Yes	Where global contract is in place compliance with our global policies is established at a corporate level. Where outsourced development is managed from the UK, leaders provide suitable and adequate supervision and monitoring.
	System Security Testing	14.2.8	Yes	Systems security requirements and functionality are integrated into software test plans.
	System Acceptance Testing	14.2.9	Yes	Software change control, test procedures and system acceptance procedures are followed when new or amended hardware, software and relevant procedures are introduced to the production environment.

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
	Test Data	**14.3**	**Objective:**	**To ensure the protection of data used for testing.**
	Protection of Test Data	14.3.1	Yes	Data used for testing systems are stored and processed in a manner that ensures appropriate security controls and compliance with all applicable privacy requirements and where production environment sensitive data is used in a test environment it shall be redacted or otherwise obfuscated.
A.15 Supplier Relationships	**Information Security in Supplier Relationships**	**15.1**	**Objective:**	**To ensure protection of the organization's assets that is accessible by suppliers.**
	Information Security Policy for Supplier Relationships	15.1.1	Yes	Through agreements and contracts we require our vendors to meet Information Security requirements as set out in relevant policies.
	Addressing Security with Supplier Agreements	15.1.2	Yes	Appropriate arrangements are in place in relation to information security agreements with 3rd Party Vendors and Business Partners.
	Information and Communication Technology Supply Chain	15.1.3	Yes	Agreements with Vendors include requirements that address the information security risks associated with information and communication technology services and product supply chain.
	Supplier Service Delivery Management	**15.2**	**Objective:**	**To maintain an agreed level of information security and service delivery in line with supplier agreements.**
	Monitoring and Review of Supplier Services	15.2.1	Yes	D&B monitors, reviews and audits vendor service delivery, where required.
	Managing Changes to Supplier Services	15.2.2	Yes	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, is managed, taking into account of the criticality of business information systems and processes and re-assessment of risks.
A.16 Information Security Incident Management	**Management of Information Security Incidents and Improvements**	**16.1**	**Objective:**	**To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.**
	Responsibilities and Procedures	16.1.1	Yes	Management responsibilities and procedures are established to ensure a quick, effective, and orderly response to information security incidents.
	Reporting Information Security Events	16.1.2	Yes	We have procedures in place to ensure security events are reported and recorded. These procedures are supported with training courses and policy.
	Reporting Information Security Weaknesses	16.1.3	Yes	All employees, contractors and 3rd party users of information technology systems and services are required to report any observed or suspected weaknesses in information technology systems or services using the same mechanisms as for actual Security Events.

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
	Assessment of and Decision on Information Security Events	16.1.4	Yes	The assessment of incident security events and the decision to classify as an information security incident is defined in our policy and procedure.
	Response to Information Security incidents	16.1.5	Yes	The response to information security incidents are defined in policy and process documents.
	Learning from Information Security Incidents	16.1.6	Yes	We apply a learning and continual improvement approach to all IS incidents.
	Collection of Evidence	16.1.7	Yes	Policy and process set out the procedure for gathering and retaining evidence and the chain of custody.
A.17 Information Security Aspects of Business Continuity Management	**Information Security Continuity**	**17.1**	**Objective:**	**Information security continuity shall be embedded in the organization's business continuity management systems.**
	Planning Information Security Continuity	17.1.1	Yes	A managed process has been developed and is maintained for business continuity throughout D&B Globally including the UK and with relevant 3rd Party vendors that addresses the information security requirements needed for the organization's business continuity.
	Implementing Information Security Continuity	17.1.2	Yes	Plans have been developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required timescales following interruption to, of failure of, critical business processes. Events that cause interruptions to business processes are identified, along with the probability and impact of such interruptions and their consequences for information security.
	Verify, Review and Evaluate Information Security Continuity	17.1.3	Yes	Business Continuity Plans are tested and updated periodically to ensure that they are up to date and effective.
	Redundancies	**17.2**	**Objective:**	**To ensure availability of information processing facilities.**
	Availability of Information Processing Facilities	17.2.1	Yes	A managed process have been developed and maintained for establishing, documenting, implementing and maintaining processes, procedures and controls to ensure the required level of continuity for information security during an adverse, unplanned or emergency situation.
A.18 Compliance	**Compliance with Legal and Contractual Requirements**	**18.1**	**Objective:**	**To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.**
	Identification of Applicable Legislation and Contractual Obligations	18.1.1	Yes	Registers are maintained to capture relevant IS related statutory, regulatory and contractual obligations.

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
	Intellectual Property Rights (IPR)	18.1.2	Yes	Appropriate procedures are implemented to ensure compliance with statutory, regulatory, and other legal obligation requirements on the user of material in respect of which there may be intellectual property rights and on the use of proprietary software products
	Protection of Records	18.1.3	Yes	Policies are in place to ensure records are protected from loss, destruction and falsification, in accordance with statutory and regulatory and other legal obligation and business requirements
	Privacy and Protection of Personal Identifiable Information	18.1.4	Yes	Our Data protection and privacy policies, procedures and training support relevant statutory and regulatory and (if applicable) in other legal requirements.
	Regulations of Cryptographic Controls	18.1.5	Yes	Cryptographic Controls are in compliance with all relevant statutory and regulatory and other legal obligation requirements.
	Information Security Reviews	**18.2**	**Objective:**	**To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.**
	Independent Review of Information Security	18.2.1	Yes	Audits are conducted internally by persons independent of the function of management being audited. Our Global Enterprise Risk and Audit team who are independent of UKI management support the audit process.
	Compliance with Security Policies and Procedures	18.2.2	Yes	Leaders are responsible for ensuring compliance within their areas of responsibility. Non-compliance, corrective action and opportunities for improvement are also reviewed at Management Review Meetings.
	Technical Compliance Review	18.2.3	Yes	Information technology systems are checked for compliance with security implementation standards. ISMS leaders from GSR; DBIS and UK meet to share best practice, identify continual improvement opportunities and track changes.
Additional Controls	**Continual Improvement**	**D&B Control**	**Objective:**	**Continual Improvement**
	Learning from other D&B business entities & driving improvements to ISMSs	C01	Yes	ISMS leaders from GSR; DBIS and UK meet to share best practice, identify continual improvement opportunities and track changes.