Glossary

The Information Security Glossary contains commonly used terms and acronyms – used in industry standards such as the ISO 27000 framework and other legislative instruments – as well as within the documentation prepared for the University on this topic.

2-factor Authentication	Multifactor Authentication involving two factors – something known (e.g. a password or PIN) and something possessed (e.g. a token or smartcard) or a biometric attribute of the person being authenticated.
3-factor Authentication	Multifactor Authentication involving three factors – something known (e.g. a password or PIN) and something possessed (e.g. a token or smartcard) and a biometric attribute of the person being authenticated.
419	Section of the Nigerian penal code that was enacted to stop advance fee frauds originating in that country. It is now a common term for this type of scam.
Access control	A generic method of control designed to restrict access to an information asset, permitting authorised access whilst preventing unauthorised access.
Access matrix	Table relating types of user role (on one axis) to the IT systems, application functions and/or classes of data (on the other axis), showing the types of access (rights) permitted within the body of the matrix.
Access, Access rights, Access permissions	Ability of a user or program to interact with an information asset e. g. to read or write data, send messages over the network etc. Also the ability of a person to enter a building, room, cupboard etc. cf. Permissions
Accident, Accidental	Unplanned, chance happening or occurrence, not intended as deli. berate. Security incidents mostly result from chance events or accidents. cf. Sabotage
Account	Generalised term for userID, credential, identity, subject or entity within a directory service, representing an individual, group, system, device, function, service, etc. May also be termed accurately as a principal.
Accountable, Accountability	Ultimately answerable for the correct and thorough completion of a task or the protection of information assets. Accountability cannot be delegated, cf. Responsible.
ACL	Access Control List – specifies which entities, users or system processes are granted access to objects, such as information assets, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation. See also Discretionary ACL and System ACL.
ActiveX	Microsoft technology for interactive Web pages. Malicious ActiveX controls are considered as malware as they may potentially compromise systems: if browser security settings allow, even unauthenticated ("unsigned") ActiveX controls may access files on hard drives, for example.
Administrator	A system administrator, IT systems administrator, systems administrator, or sysadmin is a person with the responsibility to maintain and operate a computer system but may also refer to the elevated privileges associated with this role. Alternative generic account names, dependent upon the operating system, include root, toor, baron, avatar. See also Superuser, Root.
Advance fee fraud	Type of fraud in which the fraudster persuades a naïve victim to send money as 'advance fees' supposedly to secure a payment or service which never materialises. Commonly known as a 419 scam.
Adware	Annoying programs that display advertisements, offers, etc. Considered generally to be a form of malware, adware is often installed without consent and has undesirable

	effects that may compromise privacy.
AES	Advanced Encryption Standard – specification for the encryption of electronic data. AES uses a symmetric key where the same basic key is used for both encrypting and decrypting the data.
Alarm	Audio/visual warning that a critical condition requiring an urgent response (e. g. fire/smoke, intruder, flood) has occurred. See also Alert.
Alert	Warning that a critical system event has occurred. Alerts generally require less urgent responses than alarms and so are normally logged for later analysis and follow-up action.
Android®	An operating system for mobile devices, specifically tablets and smartphones.
Anonymity	A person's ability to use systems and networks without disclosing their identity. A form of privacy.
Antivirus	Software designed to minimise the risk of malware by detecting, preventing and/or removing various forms of malware infection such as viruses, worms, trojans, etc. May also control other potentially unwanted software designated by the University.
Asset	An item that has value to the University, such as money, physical possessions, facilities (machine or computer), people, environment and intangibles such as reputation
Asymmetric	See Cryptography
Attack	The manifestation of a Threat.
Attacker	The agent causing an attack (not necessarily human).
Attribution	The act of openly acknowledging the originator or owner of intellectual property to avoid claims of plagiarism and copyright abuse.
Audit	Structured process of examination, review, assessment and reporting by one or more competent people who are independent of the situation, system, process, function, etc. being audited.
Audit trail, Audit log	Chronological record of information documenting important events or stages in a business or IT process, such as the system security log, typically configured to record successful and failed logons, etc.
Authenticate, Authentication	Process by which an individual user, system or entity is positively identified by another, typically on the basis of something they know (e. g. a password) and sometimes something they have (e. g. a security token) or something they are (biometrics). The latter cases are sometimes referred-to as **Strong Authentication** or **Two-Factor Authentication**.
Authorise, Authorisation	The process of permitting access to a resource, system or asset. Permitted, accepted and/or agreed as being in the University's best interests.
Availability	One of the three core elements of information security, along with confidentiality and integrity. Availability concerns the requirement for information, IT systems, people and processes to be operational and accessible when needed.
Avatar	A representation of an individual, or system, maintained within, or linked to, an Identity and Access Management system (IAM). Avatars are used to represent an electronic identity – generally used for conferencing, gaming etc.
Axiom	A logical statement that is assumed to be true. In this context, a fundamental information security rule derived from the 39 control objectives defined in ISO/IEC 27002.
Backdoor	Secret function or credential allowing hackers to access a system without proper authorisation, bypassing most defences. Often includes keyloggers and rootkit functions.

Backup	Copy of data and/or programs from an IT system at a given point in time. Backups provide the ability to restore a system to a known state following an incident.
Baiting	A social engineering attack in which physical media (such as a USB flash memory stick) containing malware is left in close proximity to a targeted organisation.
BCP	Business Continuity Plan – enables one or more systems and/or business processes to be recovered in the event of a disruptive event that has caused the systems or business processes to cease operation. The plan will cover one or more scenarios of potential disruption. A Disaster Recovery (DR) Plan is also a Business Continuity (BC) Plan, but is usually taken to refer to recovery of one or more IT systems or services as opposed to the BC Plan including wider business processes and manual procedures. Within the University, the term Local Resilience Plan is also in use, having the same meaning as Business Continuity Plan.
BHO	Browser Helper Object – software component that is loaded and runs automatically when the browser is launched. Malicious BHOs may incorporate malware such as spyware.
BIA	Business Impact Assessment – a risk analysis process for reviewing the potential impact of security incidents affecting IT systems supporting business critical processes, in order to determine the associated availability requirements.
Biometric	Measurable physical characteristic of a person, such as a fingerprint, iris pattern, retinal pattern, facial shape or voice pattern, which can be used as an authentication factor to positively identify a person.
Blended Threat	A cyber-attack incorporating a combination of attacks against different vulnerabilities.
Bluetooth	Wireless networking protocol intended for short-range use over a few metres. May be capable of unauthorised interception over longer distances.
Bot	Short for ‘robot’. Networked computer – often compromised using a trojan – under the remote control of hackers. Also known as zombie.
Botnet	Networks of bots that may be used for illegal or nuisance activities such as spamming, carrying out DoS attacks or as launch pads for hacking other systems. Botnets comprising up to tens of thousands of compromised machines may be rented on the black market. Botnets are controlled via Command and Control (C&C) Servers.
Breach	Form of information security incident normally occurring as a result of deliberate action or inaction, as opposed to accidental causes.
Browser	A [web] browser is a software application for retrieving, presenting, and traversing information resources on the World Wide Web.
Buffer Overflow Attack	An attack where a buffer in some software, is overwhelmed by adding more data than it is designed to hold, which ends up by allowing the attacker to run custom code.
Business Critical	Systems which have been classified as a result of a risk assessment to rate highly in terms of the potential impact on the University’s business (i. e. teaching, learning, research and administration) in the event of downtime, using criteria such as operational disruption, financial loss, damage to reputation, etc.
BYOD	Bring Your Own Device – where employees are allowed to use their own laptops and mobile devices at work.
CA	Trusted body or system that digitally signs and issues digital certificates to authenticated users or systems in a PKI.
Certificate	See Digital Certificate.
Change control	Management process for proposing, reviewing and accepting or rejecting changes to a process, system and/or the associated documentation.

Change management	The totality of activities used to control, direct and document changes to the University and its associated IT systems, processes, etc.
Checkpoint	A static record or snapshot of the state of a computer system, program, database, etc. at one point in time to which the system may be rolled-back if necessary. See also Backup.
Ciphertext, Cyphertext	Encoded/scrambled information which can be reconstituted into the corresponding plaintext using a cryptographic algorithm and a key.
Click-jacking	Also known as a "UI redress attack" Multiple transparent or opaque layers (on a web page) trick the user into clicking on a button or link on a different page than the one they were intending. Thus, the attacker is "hijacking" clicks and routing them to other destination, most likely owned by a different application, domain, or both. Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.
CMDB	Configuration Management Data Base – a repository of information related to configuration items (CI) in the IT infrastructure.
Code of Practice	University Code of Practice as defined in the University Regulations.
Compensating Control	Control that limits the severity of a control deficiency and prevents it from rising to the level of a significant deficiency or, in some cases, a material weakness. Although compensating controls mitigate the effects of a control deficiency, they do not eliminate the control deficiency.
Compliance	State of conformance with information security objectives, controls etc. defined internally by the University in policies, standards, codes of practice, etc. and/or externally by third parties (e. g. laws, industry regulations and contractual terms). Compliance tends to relate to meeting the legislative requirement although the differentiation is not strictly applied within the University.
Compromise	To undermine or attack. See Attack and Incident.
Concern	Stakeholders' interest in an asset such as availability, reliability, security etc.
CONFIDENTIAL	Class of information that is sensitive and therefore needs to be protected to a reasonable extent. It is intended for limited distribution within the University or to specially designated third parties, on a need-to-know ('default deny') basis. See the Information Classification Standard [5]
Confidentiality	One of the three core elements of information security, along with availability and integrity. Confidentiality essentially concerns secrecy or privacy.
Configuration Item, CI	The fundamental structural unit of a Configuration Management system. Examples: individual requirements documents, hardware, software, models, plans, and people.
Configuration Management	A subset of change management activities specifically relating to changes to IT systems configurations, e. g. the implementation of new programs/hardware, new versions or altered parameters.
Conformance	Meeting the requirement of a management system (e.g. ISMS), generally to achieve a minimum standard for official accreditation.
Contingency	Inherently unexpected or unpredictable situation such as a physical disaster (a bomb, plane crash, flood or fire), a serious fraud, virus/worm outbreak etc. that other controls have failed to prevent. The outcome is contingent (dependent) on the exact nature of the incident and the situation at the time.

Contingency plan	Pre-emptive approach for managing and organising resources to cope as well as possible with a contingency situation. Whereas the nature of the process to be followed during/after an incident depends on the specific situation, contingency plans support the efficient coordination and management of resources under any circumstances.

Control	An administrative, procedural, technical, physical or legal means of preventing or managing the impact upon an asset of an information security event or incident. The following types of control exist:
	• Preventative – prevents impact upon an asset.
	• Detective – detects impact upon an asset.
	• Reactive – reacts to impact on an asset, includes:
	  ○ Corrective – actively reduces impact.
	  ○ Recovery – restores an asset after impact.
	Controls may reduce information security threats or impacts, although most reduce vulnerabilities.

Control objective	Describes the anticipated business purpose or benefit of an information security control. Encapsulates the risk in business terms.
Cookie	Small text file sent by a website to a browser and later retrieved to track web browsing habits. With insecure browser settings, different sites may share the information in cookies, raising privacy issues.
Copy protection	Technique to restrict the ability of users to access, use or manipulate software and other information assets except on the original distribution media e. g. using a dongle or other forms of cryptography.
Copyright	Legal protection giving the originator/owner of original materials rights over the copying and use of the materials, for example through software licenses. A form of intellectual property rights.
Corrective control	A control that repairs or reduces the impact on an asset.
COTS	Commercial Off The Shelf – refers to package as opposed to bespoke software, typically distributed to the general public through retail outlets in shrink-wrapped packages with generic license agreements.
CPS	Certification Practice Statement – a formal document defining a given PKI.
CPS	See Certification Practice Statement
Crack, Cracker, Cracking	Hacker with malicious intent who breaks into networks and systems without the owners' permission or consent. Someone who modifies software to remove or disable copy protection and digital rights management features. A means to recover an encrypted password, or the software for this purpose.
Credential	Something an entity, user or system presents to prove (authenticate) their true identity e. g. a passport, password or security token.
CRL	Certificate Revocation List – a published list of digital certificates that have been revoked by the Certification Authority and are therefore invalid.
CRL	See Certificate Revocation List
Cryptography, cryptographic, 'crypto'	The practice of techniques for securing communication in the presence of third parties, i. e. to transform readable plaintext into unreadable ciphertext and vice versa. **Symmetric**: the keys to encrypt and decrypt are the same; **Asymmetric**: the key used to encrypt the data differs (although is related to) the key to

	decrypt. See Certificate, Private Key, Public Key, PKI
Custodianship	Temporarily taking responsibility for an Asset.
Cyber Security	Protection against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.
Cybercrime	Criminal activity performed using computers and/or the Internet. Includes actions ranging from downloading illegal music to stealing from banks. Cybercrime also includes non-monetary offenses, such as creating and distributing malware or posting sensitive or restricted information publicly.
Cybersecurity	Almost synonymous with **Information Security** but focussed on electronic information assets and related threats, vulnerabilities and mechanisms.
DACL	Discretionary Access Control List – an access control list (generally controlled by the owner of an object) that specifies the access that particular users or groups have to the object
Data	The lowest level of abstraction that applies to information or the electronic representations of information held within a computer system. Data may be said to realise or implement information in a physical or electronic form.
Data miner	Form of malware that covertly collects information on Web users, for example secretly recording data submitted on electronic forms.
DDoS	Distributed Denial of Service – a type of DoS attack using multiple (numerous) attacking systems to amplify the amount of network traffic, thereby flooding and perhaps swamping the target systems or networks.
Default allow	Access control principle stating that information should only be withheld from individuals if it requires special protection. Also termed 'need-to-withhold'.
Default deny	Access control principle stating that information should only be released to authenticated individuals if they have a legitimate purpose or reason for using the information, and are authorised to do so. Also termed 'need-to-know'.
Defence-in-depth	Control principle whereby multiple overlapping or complementary 'layers' of control are applied, all of which would have to be breached in order to impact the protected information assets.
Detective control	Control that detects impact on an asset.
Dialer	Form of malware which tries silently to connect to a premium rate phone number using the computer's modem. See also war dialer.
Digital certificate	File containing information about a user or system along with their public key plus a digital signature from the Certification Authority to authenticate the whole certificate. In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind a public key with an identity – information such as the name of a person or an organisation, their address, and so forth. The certificate can be used to verify that a public key belongs to a specific entity. See PKI.
Digital fingerprint	See Digital signature
Digital signature	Cryptographic hash of a message, constructed with the sender's private key, used to 'seal' the document thus revealing any subsequent changes, for integrity purposes, and authenticating it.
Directory	A system that stores, organises and provides access to information regarding users, entities or systems and their credentials.
Disaster Recovery	A Disaster Recovery (DR) Plan is a Business Continuity (BC) Plan, but is usually

[DR]	taken to specifically refer to recovery of IT services.
Discretionary	Optional, i. e. provided or used at someone's discretion. Refers to controls that are not mandated by the information security architecture.
Discretionary Access Control	A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).
Division of Responsibilities	Control requiring the involvement of more than one individual to complete a business process e. g. data entry performed by a member of staff with review and authorisation performed by a supervisor or manager. Normally reinforced by controlled access to the corresponding system functions. Reduces the possibility of fraud, barring collusion between the individuals, and data entry errors. Also known as separation or segregation of duties.
DMZ	De-Militarised Zone – a special network segment between the outer network perimeter and the inner University network, within which proxy servers and firewalls help to isolate the internal and external networks.
Dongle	Copy protection device used to 'unlock' (allow access to) software for use on the particular computer into which it is plugged.
DoS	Denial of Service – a type of information security incident in which availability is impacted, for example by deliberately or accidentally overloading the system or network, thereby interfering with legitimate business processing. See also DDoS.
DPO	Data Protection Officer, responsible under the Data Protection Act (DPA).
DR **D-R**	Disaster Recovery – arrangements to restore IT services supporting critical business functions, often from an alternate location, following a major incident affecting the primary production systems and data.
DRM	Digital Rights Management – technical controls using cryptography to permit or deny certain types of use of Intellectual Property, according to the copyright owner's wishes. Access control technologies that are used by hardware manufacturers, publishers, copyright holders and individuals to limit the use of digital content and devices. The term is used to describe any technology that inhibits use of digital content that is not desired or intended by the content provider. The term does not generally refer to other forms of copy protection, which can be circumvented without modifying the file or device, such as serial numbers or keyfiles.
Dual-control	Form of control requiring the actions of more than one person, for example when two soldiers have to insert and simultaneously turn their keys in order to launch a missile. See Division of Responsibilities
Electronic Identity	An electronic representation of an individual, or system, used for Authentication and Access Control. A person may have more than one electronic identity. Electronic identities are usually maintained using an Identity and Access Management (IAM). See UserID.
Elevated privileges	Enhanced access privilege. See privilege
Emergency intervention	Situation in which a competent support person is specifically authorised by management to modify a system directly, typically through a privileged emergency credential, bypassing the normal system access controls and code migration processes in order to resolve an urgent production issue.
Encryption	Application of cryptography to make information unintelligible, i. e. translating plaintext into ciphertext using a prescribed algorithm and a key.

Exemption	Temporary, approved relaxation of security policy requirements, provided that compensating controls are implemented (where possible). The person requesting an exemption (normally the owner) remains formally accountable for the residual risk resulting from non-compliance with policy. See waiver.
Failover	Manual or automated process for transferring resilient IT services between redundant equipment, campuses and/or network routes, improving availability.
Failsafe	Concept used mainly in safety-critical or high-security system and process designs, whereby a control failure leaves the system/process in an inherently safe or secure condition, even if that impairs availability.
Fair use	Copyright laws generally permit limited use of copyright materials without the copyright owner's explicit permission. Such fair use exceptions typically allow quoting and summarising of non-substantial parts of copyright materials and small-scale copying for research and educational purposes.
Fault	Problem with information processing or communications systems including definite or suspected security incident, system failure, program error/bug, malware/virus, other undesirable system operation, etc.
FIPS 140-2	Federal Information Processing Standards (FIPS) are US government security standards issued by the National Institute of Standards and Technology (NIST) and the 140 series covers cryptography. FIPS 140-2 is a validation certificate issued by NIST that certifies compliance with the standards.
Firewall	Specialised router specifically configured as a gateway to control logical access to the attached network segments, nodes and devices.
Firmware	Software embedded in a hardware device, typically an EEPROM (Electrically Erasable Programmable Read Only Memory) chip. A computer's BIOS (Basic Input Output System) is an example: BIOS firmware normally checks the machine's hardware for faults and loads the boot loader part of the main operating system. Any malware in firmware is likely to have complete control of the system since it is inherently trusted by the operating system and other software.
Flood	In terms of computer networks, flooding inundates or swamps a network or device. See DoS.
FOSS	Free Open Source Software – free to use but usually still subject to a license.
Fraud	Theft or similar crime involving deliberate deception by a fraudster.
Fuzz Testing, "Fuzzing"	Providing invalid, unexpected, or random data to the inputs of a computer program to test its resilience to attack. See Penetration test.
Generic Account	An account, or UserID, which is not attributed to an individual. See Service Account.
Governance	Comprises the entire management framework or structure for controlling and directing the University, including information security and other controls.
Guest	A generic, non-privileged account or security principal (including a group) with minimal system access. Also called "nobody".
Hacker, Hacking, Hack	Originally, the term applied to someone who was obsessively fascinated by technology. In common use, hacker has gradually come to mean someone who deliberately breaks into networks and systems although cracker is technically more accurate.
Hacktivism, Hacktivist	Hacking, phreaking, or otherwise using technology to achieve a political or social goal. Major hacktivist groups that have achieved notoriety include Anonymous and LulzSec.
Hardware	Tangible IT asset. Hardware has a financial book value, generally less than its replacement cost due to depreciation (wear and tear). Hardware typically has even greater value to its owner thanks to supporting/enabling important business processes.

Harm	Damage that can happen to an asset such as undesired exposure of stored information or unavailability of a service. Harm is usually quantified as Impact.
Hash	Characteristic value produced by passing a string or file through a so-called 'one-way encryption' function. The original string or file cannot be recreated with any certainty from the hash value but its validity can be verified by recalculating and comparing the hash against a previously calculated and securely stored hash value.
Hold file	Transactions that fail integrity or other checks are commonly flagged or placed in this special holding area for manual inspection, instead of being processed. Also known as a suspense file.
IAM	Identity and Access Management – system that contains and manages electronic identities including security-related data but also preferences and other relevant data.
Identity theft	Type of fraud in which the fraudster falsely assumes the victim's identity, typically as a prelude to stealing financial or other assets. Often involves theft or falsification of credentials used to assert the holder's identity.
Impact	Changing the value of an asset by reducing its availability, integrity or confidentiality. A measure or description of the effect or outcome of an incident. A measure of the seriousness of Harm.
In the wild	Describes malware that is being actively and widely exploited, as opposed to that which has only ever been seen in the laboratory or in very limited-scope incidents. "General release"
Incident	Situation where an attack occurs and causes a business impact.
Industrial espionage	The use of unethical, illicit, surreptitious and often illegal "spying" techniques to gather sensitive information from competitors, either directly or via common business partners or other third parties. An extreme form of competitive intelligence.
Information asset	A physical or virtual artefact containing data that realises information. This includes documents, emails, databases etc. Information itself is abstract but is instantiated in the form of information assets.
Information Asset Owner	The designated person held accountable for the proper protection of one or more information assets such as business applications and data sets. They approve appropriate information security controls for the assets, authorise access and monitor the effectiveness of the controls.
Information Security	The protection of confidentiality, integrity and availability of information in all its forms including electronic (see **Cybersecurity**) and physical.
Information Security Architecture	The complete set of information security controls limiting the risks associated with a given IT system or infrastructure. Should ideally be documented in the security design.
Information Security Design	Documentation describing the key information security risks, control objectives and controls required in a computer system, in other words the information security architecture. May comprise one or more dedicated security design documents or may be distributed across various system architecture, design, development and operations documents, policies, standards, guidelines, procedures, change records, etc.
Information Security Event	An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
Information Security Incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations or threatening information security.
Information Security Management	The function responsible for day-to-day management of information security, managing technical, procedural and physical controls, systems, processes, standards etc. Led by the Information Security Officer.

Information Security Policy Manual	The University's overarching policy defining the overall objectives and structure for information security management, also known as the ISMS.
Information Security, InfoSec	The preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Insider threat	Information security threat arising from University members.
Integrity	Property of completeness and accuracy of information. Protected through controls such as referential integrity, data entry validation, digital signatures, honesty, ethics and trust. One of the three core elements of information security, along with confidentiality and availability.
IP	Intellectual Property – proprietary information (typically) that legally belongs to someone and may be protected by IPR.
IPR	Intellectual Property Rights – the rights of the legal owner of intellectual property (IP) to determine how the information is used and/or copied by others, for example through software licensing/copyright, patent, trademark or contract law.
ISMS	Information Security management System – the overall management system comprising governance, policies, standards, procedures, guidelines, etc. through which information security is directed and controlled.
ISO	1. International Standards Organisation. 2. Information Security Officer – responsible for Information Security at the University.
ISO/IEC 27000-family ("ISO27k")	A growing collection of ISMS international best practice standards being produced under the auspices of a joint ISO/IEC committee.
ISO/IEC 27001:2005 ("ISO 27001")	International standard "Specification for an Information Security Management System", originally known as BS 7799 Part 2. This is the standard against which ISO/IEC 27002 users may choose to have their ISMS certified.
ISO/IEC 27002:2005 ("ISO 27002")	International standard "Code of Practice for Information Security Management", originally known as BS 7799 Part 1 and then ISO/IEC 17799. Proposes a reasonably comprehensive set of information security control objectives and a selection of best practice information security controls.
ISSG	Information Security Steering Group – the University oversight or governance committee responsible for Information Security.
IT Services	Department responsible for managing computing and telecommunications services to the University.
JANET	Joint Academic Network – a private computer network dedicated to connecting all further- and higher-education organisations in the UK, as well as the UK Research Councils.
Journaling	Database security/control method in which steps leading up to a commit point are saved temporarily until the commit is complete, enabling the sequence to be reversed or recreated if interrupted by an incident, for instance a power failure or coincident change.
Key	See Private Key, Public Key, PKI
Keyfile	A data file which contains cryptographic or license keys. See also PKI.
Keylogger	Malware that secretly records the keystrokes. There are hardware and software versions. Hardware keyloggers are inserted into the keyboard cable or connector where they may appear to be interference suppressors, or are fitted inside the keyboard or computer. Software keyloggers are typically installed by trojans.

Least privilege	Information security principle involving restrictions in the level of privileges, permissions, capabilities or rights assigned to an individual person, function or system, consistent with their authorised and intended purpose.
Local Resilience Plan	See Business Continuity Plan
Lock	Physical security device requiring a physical key, electronic key card, PIN code or similar to release a door, etc. Also a database integrity control which essentially prevents simultaneous data changes being made by different computer processes or users.
Log	An historical record of events, recorded in a data file for subsequent review and analysis. Logs should be secured against unauthorised modification (tampering) or access (if confidential) and retained for as long as is necessary to complete the review and analysis, or according to legal and/or business requirements identified in the Information Retention Policy. See audit trail.
Logic bomb	Form of malware designed to lay dormant but self-activate at some point e. g. at a certain time (i. e. a time bomb), when a certain user logs in, when a particular combination of events occurs (e. g. the programmer is removed from the payroll) and cause some malicious action (e. g. shutdown the system, modify or delete data).
Logical access control	Automated information security control protecting electronic information assets (data/software, directories, disks, tapes etc.) against access by unauthorised users, programs or systems.
Malware	Portmanteau of "malicious software" meaning programs written and circulated with malicious intent such as viruses, worms, trojans, rootkits, logic bombs, etc.
Mandatory Access Control	Access control by which the operating system constrains the ability of a subject or initiator to access or generally perform a specific operation on an object or target. In practice, a subject is usually a process or thread; objects are constructs such as files, directories, TCP/UDP ports, shared memory segments, etc. Subjects and objects each have a set of security attributes. Whenever a subject attempts to access an object, an authorisation rule (enforced by the operating system) examines these security attributes and decides whether the access can take place. Any operation by any subject on any object will be tested against the set of authorisation rules (aka policy) to determine if the operation is allowed. Mandatory access schemas are generally applied at an organisational level compared with discretionary access which is specified by the information asset owner.
Member	Member of the University as defined in the University Regulations.
Mobile code	Programs that transfer between systems and execute, performing specific functions with little or no user interaction.
MoSCoW	Requirements prioritisation scheme: • **M – must** be met. • **S – should** be met if possible (high priority). • **C – could** be met in future if time and resources permit. • **W – won't** be met now but may be considered in the future.
Multifactor authentication	Form of user authentication in which different types of credential are required (e.g. a secret password plus a security token plus a biometric). Multiple passwords recalled and entered by single person do not qualify as multifactor authentication, whereas passwords recalled and entered by more than one person (one form of dual-control) do.
Need-to-know	Alternative name for the principle of default deny.
Need-to-withhold	Alternative name for the principle of default allow.

N-factor Authentication	See Multifactor Authentication.
Non-interactive account	Type of account intended for automated system activity and file ownership by computers, systems and applications, rather than by people.
OPEN	Class of information that is not sensitive and therefore may be published or distributed externally. See the "Information Classification Standard" [5], also PUBLIC
Outage	IT service interruption caused either by a planned activity (such as scheduled maintenance) or an unplanned incident.
PAN	Principal Account Number – the main account number on a payment or credit card as defined in PCI-DSS.
Passphrase	A secret phrase or saying that is either used directly as a long and hence strong password, or is used to recall one (e. g. using initial letters of the words to a song or poem).
Password	A secret string of characters that should only be known by one person and can therefore be used to authenticate them. A type of credential.
Patent	Legal protection for novel inventions that have been properly registered with the relevant patent authorities. A form of IPR.
Payload	The resultant (usually destructive) function of malware that performs unauthorised activity, such as deleting or modifying files, etc.
PCI-DSS	Payment Card Industry Data Security Standard – a commercial contract that the University is party to through their activities relating to accepting credit and debit card payments.
Penetration test	Officially authorised/sanctioned/requested test of the University's information security controls by competent and trustworthy experts. The scope may include network, physical and/or other information security controls and specific systems or locations.
Perimeter	The outermost physical and/or logical boundary around a collection of assets, such as the network perimeter dividing the University's internal network from JANET, the Internet and other external networks.
Personal data, personal information	Information associated with an identifiable individual person. This term is explicitly defined in national data protection laws with minor but important differences between countries.
Phreaking, Phreaker	The activity of a culture of people who study, experiment with, or explore telecommunication systems, such as equipment and systems connected to public telephone networks.
PIN	Personal Identification Number – a numeric password used on systems with numeric keypads instead of full alphanumeric keyboards. PIN is often misused as a synonym for password
Pirate	Someone who commits piracy e. g. by making, using, selling or otherwise distributing illegal copies of copyright material, whether deliberately or inadvertently.
Plagiarism	Theft (copying and using) of another person's IP without properly acknowledging or attributing it to them.
Plaintext	Information that a sender wishes to transmit to a receiver. cf. Ciphertext.
Policy	A University Policy as defined in the University Regulations.
Polymorphic virus	Type of computer virus which changes (morphs or mutates) as it infects successive systems/files, making detection and disinfection challenging.
Preventative control	Control that prevents impact on an asset.

Principal	An entity that can be authenticated by a computer system and authorised for specific functions. Security principals are generally individual users, groups, processes, services, devices, etc. See Account
Principle	Fundamental or philosophical basis on which information security controls are based. Often encapsulated by phrases such as 'default deny', 'defence in depth', 'shared responsibility' and 'least privilege'.
Privacy	Right to confidentiality regarding sensitive information about individuals or groups.
Private key	The secret member of a public-private key pair in an asymmetric cryptography system or PKI.
Privilege, Privileged	Attribute of certain accounts, principals, programs etc. that allows the users or programs to bypass logical access controls and execute functions that are normally forbidden to ordinary (non-privileged) accounts, for example, data backups need to copy all the files to be backed up, even if they are not owned by the backup user. See Administrator, Root
Privileged User Role	Whereas non-privileged user roles define minimal rights of access to networks, systems and data for most users, Privileged User Roles define more powerful access rights that can bypass normal security controls and are therefore only allocated to highly trustworthy members with additional procedural and/or technical controls.
Program Source Library [PSL]	Controlled directory or database containing human-readable source code files cf. program library.
Proprietary	Valuable and normally sensitive commercial information such as trade secrets, customer lists and competitive information. See CONFIDENTIAL
Public key	The non-secret member of a public-private key pair in an asymmetric cryptography system or PKI, normally published within a digital certificate.
Public Key Infrastructure [PKI]	Asymmetric cryptographic system using public and private key pairs. cf. Symmetric
PVLAN	Private VLAN that is isolated from others through the use of traffic encryption.
RAT	Remote Administration Tool – software that provides hackers with a back door into an infected system to snoop or take control.
RBAC	Role Based Access Control – access control scheme whereby principals are granted certain system access rights according to the roles they are required to perform, the idea being that roles change less frequently than users.
Reactive control	Control that reacts following impact upon an asset.
Recovery control	Control that restores an asset after impact.
Referential integrity	Set of integrity controls incorporated into relational database management systems to help prevent inconsistencies, for example in the links between related tables.
Remote Diagnostic Port	Dedicated console or management port giving privileged access for technical support to a device such as a telephone exchange, server, storage subsystem, router, firewall, gateway etc.
Rights	Capabilities granted or denied to principals by system managers, supervisors or administrators. See Permissions and clarification section.
Risk	The combination of the probability of an event and its consequences – the likelihood of a Threat exploiting a Vulnerability and the resulting Impact upon Assets.
Risk assessment, Risk analysis	Structured process for examining information security threats, vulnerabilities and impacts relating to a given system or situation, in order to determine whether additional controls are required. The specific terms "risk assessment" or "risk analysis" may refer to different extents of examination ('analysis' normally implies more depth).

Risk management	The process of managing defined risks by mitigating them, accepting them or transferring them to third parties (e.g. insurance companies).
Role	The responsibility for performing specific behaviour.
Root	1. See Administrator, Superuser 2. Gain root or superuser access (particularly to Android and Linux/Unix
Rootkit	Hacker toolset typically containing trojans and utilities to take and keep control of a compromised computer system. Often includes hacked versions of normal system programs with backdoors and other covert functions. Usually hidden deep in the system "kernel" or device drivers, hence hard to detect and eradicate.
RPO	Recovery Point Objective – following a serious incident requiring the invocation of disaster recovery arrangements, defines the point prior to which all data should have been restored (e. g. previous hour, previous working day, previous week etc.).
RTO	Recovery Time Objective – defines the absolute maximum ('worst case') acceptable duration of non-availability of systems due to incidents, which therefore determines the corresponding need for suitable resilience and disaster recovery arrangements.
Sabotage	Deliberate, wilful and unauthorised damage to IT facilities, systems, network devices/connections, deletion, insertion or disclosure of data etc. in order to cause a Denial of Service or other impact.
Sandbox	An architectural pattern where data or binary code is stored in a secure area to be examined safely or protected from external access.
Security Administration	Information security function responsible for administering userIDs, passwords, access to applications etc.
Security Principal	See Principal
Security token	Hardware device used as a credential, for example a smart card or key fob containing a cryptographic processor and/or display. May also relate to the notional representation of a security principal or credential within a system.
SEI	Software Engineering Institute a US federally funded body run by Carnegie Mellon University (CMU).
Service	The externally visible functionality which is meaningful to the environment and is realised by systems or business behaviour.
Service Account	A generic, often privileged, account under which a background process runs.
Shared responsibility	Information security principle stating that all members are collectively responsible for maintaining adequate security measures.
Smartphone	Mobile device combining the features of a phone with those of a personal digital assistant [PDA], such as media players, email, browsers, wireless connectivity, cameras, and also touch-sensitive screen technology. See Android, iOS
Snapshot	A backup technique that creates a read-only copy of a file, usually by manipulating the storage allocation mechanism within a file system so that changes are forced into new blocks of storage rather than updating in place.
SOA	Service Oriented Architecture – a technical architecture consisting of cooperating services where the implementation of the services is hidden from the consumers, whether people or systems.
Social engineering	Hacking or Fraud technique or form of attack involving the manipulation of people through a combination of deception and persuasive or assertive behaviour. May also be combined with other threats.
Spam	Unsolicited email (generally sent in bulk and commercial in nature).

Spear phishing	A precisely targeted phishing attack, usually aimed at individuals or well-defined groups.
Spoof, Spoofing	Attempt by an unauthorised entity to gain access to a system by posing as an authorised user, i. e. impersonation
Spyware	Type of malware which covertly 'spies' on the user, for example, sending information about the programs run, Websites visited or data submitted, to a remote system or user.
SQL injection attack	A form of attack on a database driven web application in which the attacker executes unauthorised SQL commands to exploit insecure code.
Stakeholder	Person who has a legitimate interest, or stake, in an Asset.
Standing data	Reference items that are relatively static and unchanging (e. g. bank account numbers) compared to more volatile user data (e. g. bank account balances).
Stealth virus	Virus that hides by intercepting disk access requests. When a basic antivirus program tries to search the disk, the virus conceals itself by removing or changing program names, file names etc. in the information fed to the antivirus program. See also rootkit.
Superuser	Special user account possessing unbounded elevated privileges, used for system administration. Depending on the operating system, the actual name of this account might be: root, administrator, avatar, supervisor, etc.
Symmetric (cryptography)	Cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption/decryption, or signature creation/verification). Symmetric cryptography is sometimes called "secret-key cryptography".
Sysadmin	See Administrator
System	A collection of elements organised to accomplish a defined objective or Mission. The term is recursive and may also refer to a component or a 'system of systems'. These elements include products (hardware, software, and firmware), processes, people, information, techniques and facilities. The mechanism that delivers a service to the customers.
System Access Control List (SACL)	In contrast to the DACL, which specifies object access granted for listed trustees, Microsoft describes the System Access Control List as a means to control how access to an object is audited.
System files	Files containing executables and data that are part of, or owned by, an operating system. Users and applications are usually blocked from accessing these files.
Technical standard	IT Services technical standards, including security standards, referring to industry standards, hardware, software etc.
Test environment	Computer environment comprising systems, networks, devices, data and supporting processes that are used for testing (checking and/or exercising) application systems prior to being released for use in production (cf. development).
Third party	Independent person or external organisation not directly employed by the University.
Threat	A potential cause of harm to an asset. A Threat exploits a Vulnerability to Impact an Asset.
Time bomb	See logic bomb.
Timeout	1. Function that automatically suspends and password-locks a computer session after a certain time without user activity. 2. Also, an expiration time limit for a process.
Trojan	Contraction of "Trojan horse program" that may appear to the user to offer a useful function or to do nothing, but in fact contains hidden malicious functions, typically

	allowing remote control of the system by hackers. A form of malware.
Trustee	An entry in an access control list to which permissions or rights are granted (or denied). See Discretionary ACL and System ACL.
Two Factor Authentication ("2FA")	Simplest form of multifactor authentication, for example, requiring a password in addition to the current value displayed on a security token in order to authenticate a user.
Unauthorised	Not permitted, accepted or agreed by management as being in the University's best interests.
UNIX, Unix, Un*x	An operating system; trademarked as UNIX, but within the University, a general term for one of its derivatives or any operating system which resembles it.
User Role	Logical access rights are standardised by defining and assigning the minimal rights necessary for users in certain job functions to perform their roles within the University (see also Privileged User Role).
UserID	User Identifier – a label used to tag a user and their activities on an IT system so that they may be controlled by logical access controls, recorded in log files etc. Also known as a username, logon name, account, credential, etc.
VDI	Virtual Desktop Infrastructure – where the client application actually runs on a server and the local device is just used as a 'dumb' terminal showing an image of the application screen only.
Virus	Computer program that self-replicates and automatically spreads between systems. Usually contains a payload. A form of malware.
Virus hoax	Chain letter or social media spreading a false virus (malware) warning. Hoaxes can cause alarm and waste time but are not normally harmful, although some that advise users to delete, rename or replace files can cause problems (a form of social engineering).
VLAN	Virtual Local Area Network – a broadcast LAN domain containing one or more hardware devices, usually associated according to the specific ports on LAN switches to which they are connected (see also PVLAN).
VPN	Virtual Private Networking – the application of cryptography to create a secure "tunnel" between IT systems over an unsecured or untrustworthy network (such as the Internet).
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more Threats.
Waiver	Formal documented exemption from security requirements, including documentation of the circumstances, decision process/rationale, extent and compensating controls.
War dialer	Hacking or penetration testing software that automatically calls a range of phone numbers in an attempt to locate vulnerable modems, fax machines, voicemail systems etc.
Web bug	Tracking hyperlink within a Web page that refers the user's browser to a particular file on the Web, typically a tiny one-pixel image. When the user's browser reads the page, interprets the code and retrieves the file, the web server records the network access by the user's address in its log, potentially compromising the user's privacy.
Whaling	Cyber-attacks targeted specifically at senior executives and other high-profile targets.
Worm	Networking program that exploits network connections to spread between systems and often performs unauthorised functions such as sending unsavoury emails or spam, DoS attacks etc. A form of malware.
X. 509 Certificate	A digital certificate of specified format, binding an entity to a public key. The X. 509 standard was issued on 03 July 1988.

XSS	Cross Site Scripting – a web hacking technique in which websites with inadequate data entry validation are made to return malware to a browser for execution (e. g. to manipulate or disclose their supposedly private cookies or other local data). Abbreviated to "XSS" to distinguish it from CSS: Cascading Style Sheet.
Zero-day threat	A cyber attack against an unknown operating system or application vulnerability.
Zombie	See bot.

Ontology

The ontology provides a basic set of concepts and relationships that can be used to reason about information security and upon which a controlled vocabulary may be constructed.

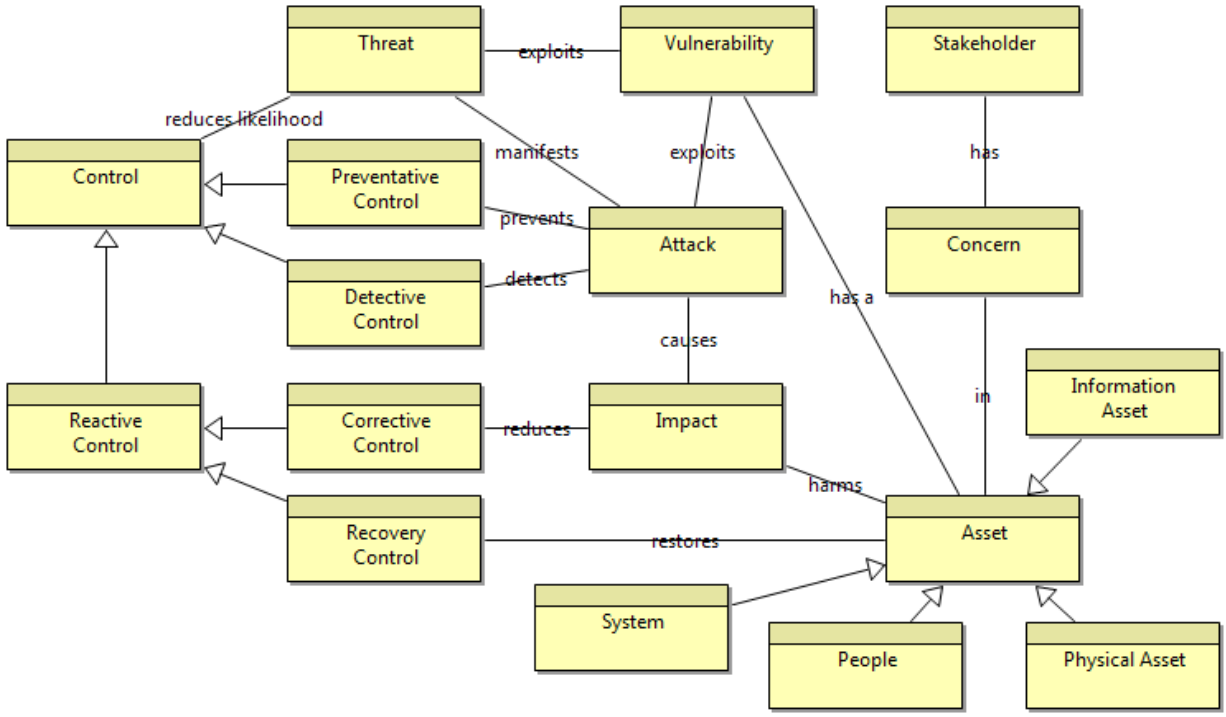

Figure 1 Basic Ontology for Information Security Risk Analysis and Management

Asset	Business Object	Anything that has value to the organisation or its customers, including physical assets, information, systems and people in their role as participants in a System.
Attack	Business Object	An event that is a manifestation of a Threat to an Asset
causes	Association	**Attack** causes **Impact**
Concern	Business Object	Stakeholders interest in an Asset
Control	Business Object	An administrative, procedural, technical, physical or legal means of preventing or managing the impact upon an asset of an information security event or incident. This can be: Preventative, Detective, Reactive (Corrective / Recovery). Controls may reduce information security threats or impacts, although most focus on vulnerabilities.
Corrective Control	Business Object	A control that repairs or fixes the impact on an asset
Detective Control	Business Object	Control that detects impact on an asset.

detects	Association	**Detective Control** detects **Attack**
exploits	Association	**Threat** exploits **Vulnerability**
exploits	Association	**Vulnerability** exploits **Attack**
harms	Association	**Impact** harms **Asset**
has	Association	**Stakeholder** has **Concern**
has a	Association	**Asset** has a **Vulnerability**
Impact	Business Object	Measure of harm or effect upon an Asset.
in	Association	**Concern** in **Asset**
Information Asset	Business Object	An asset that contains information e.g. database, email, document, book.
manifests	Association	**Threat** manifests **Attack**
People	Business Object	People viewed as 'human assets' for the purpose of risk analysis and management.
Physical Asset	Business Object	Physical assets including land, buildings, vehicles
Preventative Control	Business Object	Control that prevents impact on an asset.
prevents	Association	**Preventative Control** prevents **Attack**
Reactive Control	Business Object	Control that reacts following impact upon an asset.
Recovery Control	Business Object	Control that restores an asset after impact.
reduces	Association	**Corrective Control** reduces **Impact**
reduces likelihood	Association	**Control** reduces likelihood **Threat** Reduce the likelihood of a Threat manifesting.
restores	Association	**Recovery Control** restores **Asset**
Stakeholder	Business Object	Interested party.
System	Business Object	A combination of interacting elements organised to achieve a defined objective, including hardware, software, processes, people, information, techniques, facilities and any other type of Asset.
Threat	Business Object	A person, situation or event (whether deliberate or accidental in nature) that is capable of exploiting a vulnerability to impact an asset.
Vulnerability	Business Object	Weak or missing information security control, or an inherent weakness in an Asset.

Disambiguation

Authentication vs. Authorisation

Authentication is the process of verifying identity, or asserting that the entity is whom or what they claim to be. Authorisation is the method of granting access based on the confirmed identity.

Authentication is performed at logon while Authorisation, sometimes referred-to as 'access control', is granting access to resources after logon. Authentication is performed centrally while authorisation is usually the responsibility of individual applications.

Malware, Virus, Trojan, Rootkit, Worm, etc.

Malware is a contraction for "malicious software" although malware could encompass firmware and hardware. It is the general term applied to viruses, trojans, rootkits, spyware, adware, scareware, keyloggers, ransomware and crimeware, etc. Malware can also be known as a "computer contaminant" in a legal context.

The first malware was a computer virus, i. e. a program that replicates itself and spreads accordingly. Worms are similar to viruses in that they self-replicate but they do not attach themselves to existing computer programs. Worms generally disrupt network operations, even if only by consuming excessive bandwidth, whereas viruses almost always corrupt or modify files on a target computer.

Trojan horses, commonly called trojans, are programs that masquerade within other programs, causing unexpected (unwanted) results when executed. Rootkits are specialised trojans designed to subvert standard operating systems thus hiding their existence.

Trojans now make up approximately 90% of all malware.

In the industry, we have seen a transition in the last decade from "antivirus" to "antimalware" measures within the accompanying software marketing.

Principles, Axioms, Policies, Standards, Guidelines

The ISO27k Implementers Forum provides the following pyramidal representation of the relationship between these terms:

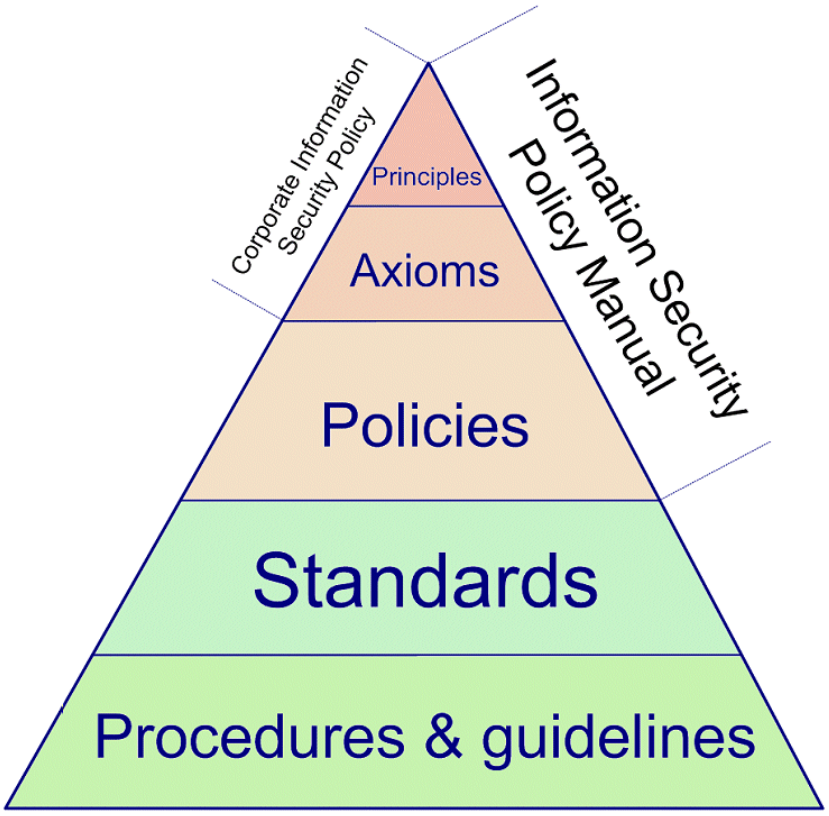

Figure 2: ISO27k ISMS Documentation Pyramid

The General Conditions of Use [1] together with the Information Security Policy [2], and other policies such as the Data Protection Policy [3], constitute the Information Security Policy Manual while the Information Security Policy

by itself is the Corporate Information Security Policy in terms of ISO27k. This scheme takes into account the special status of the General Conditions of Use as a Code of Practice as defined in the University Regulations.

Standards, prepared by the Information Security Officer and ratified by the ISSG, define the requirements and rules pertaining to individual topics while procedures and guidelines will be issued by IT Services as and when appropriate.

Security principles are rooted in the University's Enterprise Architecture Framework (EAF) and all IT projects are required to comply and state how compliance is achieved and justify exceptions. The principles are as follows:

ID	Principle	Rationale
SEC1	**Accountability** All user and system interactions and access to information must be attributable to authenticated (reliably identified) people, organisations or systems.	The University must maintain traceability and non-repudiation of responsibility for access and changes for legal and moral reasons.
SEC2	**Least Privilege** When allowing access to a resource, assign the minimum necessary privileges to complete the job in hand.	Reduce the possibility that users or systems will abuse the privileges granted them to make unforeseen changes or gain unauthorised access.
SEC3	**Defend in Depth** Do not rely on a single control but erect a succession of barriers that an intruder must overcome before gaining access.	No single security mechanism can be guaranteed unbreakable, therefore good practice is to implement multiple overlapping controls where it is possible to do so.
SEC4	**Assume Insecure Communications** Data is vulnerable while in transit and must be adequately protected to preserve its confidentiality, integrity and availability..	Internal networks should be considered hostile environments for data and mitigated by authentication, encryption and other controls.
SEC5	**No Security by Obscurity** Security must be designed-in and not rely on hiding information.	Security should not be compromised by the release of network diagrams, system specifications or CMDB.
SEC6	**Transparency** Controls should not impair the ability of the University to function or unnecessarily restrict the availability of information.	Security controls should promote the availability of information subject to protection of its confidentiality and integrity.

Axioms are derived from these principles and incorporated into the security documents.

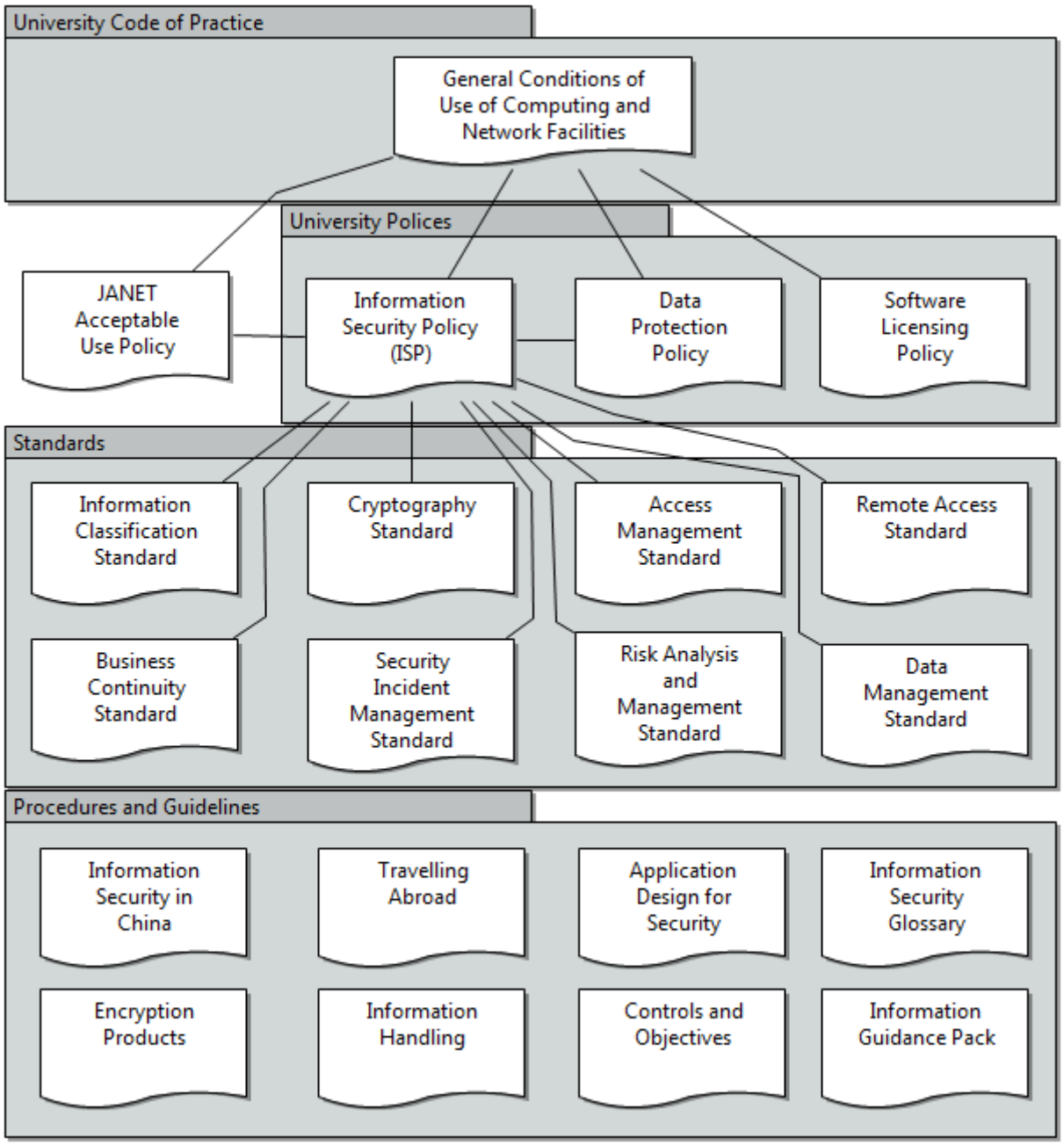

Figure 3 Information Security Document Set

System vs. Service

Although often used interchangeably, these two terms are strictly defined for use within the University and this documentation set.

A ‘service’ refers to a bundle of functionality that is delivered, or realised, using one or more systems. The ‘system’ is often transparent, or invisible, to the customers, or consumers, of a service.

Note that, in technical contexts such as ‘service oriented architecture’ (SOA), the consumers of a service may themselves be systems rather than people. All consumers of services must reliably identify themselves (authentication) so that they can be granted access (authorisation) to information in accordance with University security policies.

Account, User, userID, Credential, Principal, Subject, Object, Entity, Identity, ID

While the glossary seeks to differentiate these terms, they are often interchangeable. These terms vary according to the operating system, application or developer and so care must be taken to establish the precise definition within its contextual usage.

Abilities, Permissions, Rights, Privileges, and Capabilities

As with the previous terms, there is often an overlap from system to system.

However, in the strictest terms within Microsoft systems, rights refer to logon capabilities (such as authenticating as a background service, an interactive user, or a task), permissions relate to object access capabilities (e. g. Read, Write, SendAs, etc.), and privileges relate to elevated capabilities including overriding permissions (such as backing up a file without holding Read permission). 'Abilities' is a largely deprecated Microsoft term, a combination rights and privileges.

Unless the context demands a strict usage of one of these terms, "capability" will be used as a generic reference in this documentation set.

References

1. University of Birmingham General Conditions of Use of Computing and Network Facilities — http://www. it. bham. ac. uk/policy/
2. University of Birmingham Information Security Policy — http://www. it. bham. ac. uk/policy/
3. University of Birmingham Data Protection Policy — http://www. legalservices. bham. ac. uk/dppolicy
4. University of Birmingham Freedom of Information Guidelines — http://ww. foi. bham. ac. uk
5. University of Birmingham "Information Classification Standard" — http://www. it. bham. ac. uk/policy/
6. University of Birmingham "Cryptography Standard" — http://www. it. bham. ac. uk/policy/

Bibliography

Sources for this glossary include:

- The ISO/IEC 27000-series ("ISO27k") standards, and various other information security standards, many of which are listed at ISO27001security. com. The original work is shared by the ISO27k implementers' forum under the Creative Commons Attribution-Non commercial-Share Alike 3. 0 License [http://creativecommons. org/licenses/by-nc-sa/3. 0].
- Wikipedia [http://en. wikipedia. org]
- The SANS Institute Glossary of Security Terms [http://www. sans. org]
- Dictionary of Information Security by Rob Slade (2006)
- Other information security and computing dictionaries, such as "Internet Security Dictionary" by Vir V Phoha, (2002) and "The Encyclopaedia of Networking and Telecommunications" by Tom Sheldon (2001).