SyOPs Glossary of Terms

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	20/10/2016
V 1.1	Andrew Clarke	Definitions for malware, new roles and best practice CIA/Governance definitions	11/02/2020

Document Approval

This document requires the approval from BUL as defined in the ISMS Compliance document.

Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security officer

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. Purpose

This document sets out a glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

2. Abbreviations and Definitions

2.1 General Terms

1 CIA – Confidentiality, Integrity, Availability - known as the CIA triad, is a guideline for information security for an organisation.

2 Confidentiality - Confidentiality is a characteristic that applies to information. To protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorised entities. In this context, entities include both individuals and processes.

3 Integrity - Within the narrow context of information security, the term integrity means to protect the accuracy and completeness of information.

4 Availability - Availability is a property or characteristic. Something is available if it is accessible and usable when an authorised entity demands access.

5 Information Security Management System (ISMS) - ISMS – Is a management system that uses a framework of resources to achieve an organisation's objectives. The management system includes policies, procedures, documents, records, plans, guidelines, agreements, contracts, processes, practices, methods, activities, roles, responsibilities, relationships, tools, techniques, technologies, resources, and structures that organisations use to protect and preserve information, to manage and control information security risks, and to achieve business objectives. In terms of information security, a management system allows an organisation to:

- 5.1 satisfy the information security requirements of customers and other stakeholders;
- 5.2 improve an organisation's plans and activities;
- 5.3 meet the organisation's information security objectives;
- 5.4 comply with regulations, legislation and industry mandates; and
- 5.5 manage information assets in an organised way that facilitates continual improvement and adjustment to current organisational goals.

6 Information assurance – Information assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. CIA underpins everything we do in all spheres and information assurance and is measured using an IA Assessment Framework (IAAF), which details the measures required to achieve the desired maturity levels for operations, resilience, privacy, and business continuity.

7 Cyber Security - Cyber security is part the broader information security controls. Cyber security, as a part of Information security, refers to the practice of ensuring ***'confidentiality,' 'Integrity,' and 'availability' (CIA)*** *of all information held digitally.*

8 Information Security – Information security ensures the confidentiality, availability and integrity of information. Information security involves the application and management of appropriate controls that involves consideration of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimising consequences of information security incidents.

9 Network security - Network security is an organisation's strategy that enables guaranteeing the security of its assets including all network traffic. It includes both software and hardware technologies. Access to the network is managed by effective network security,

which targets a wide range of threats and then arrests them from spreading or entering in the network. Network security is an integration of multiple layers of defences in the network and at the network. Network Security is governed by the Cyber and Information Security Policies and controls are implemented by each network security layer.

10 Information asset - Information is an asset that, like other important business assets, is essential to an organisation's business and, consequently, needs to be suitably protected. Information can be stored in many forms, including: digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees.

11 Zero Trust - Zero trust security is a Cyber security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

12 Safe Data Haven - Safe Data Haven is a secure IS repository used to store particular research data, intellectual property, personal data and University Confidential information for access exclusively by approved colleagues. Strict safeguards control who can access University information stored within a safe data haven. A safe data haven provides secure file transfer and an adherence to store and use data within a secure system.

13 SyOPs - "Security Operating Procedures".

14 DRU - "Document Reproduction Unit".

15 BUL - Brunel University London.

16 Third party sub-contractors are those organisations who provide services to Brunel University London sub-contractors relating to this contract. The term 'said parties' relates to individuals, sub-contractors and third party sub-contractors who will be involved in the processing of University information.

17 ICS - "Information Classification System" Assets or protectively marked data.

18 The University Brunel University. Any reference to 'a university' is generic to a higher education institution.

19 Unit of the University. This term is to be read to incorporate any department, college, institute, group, etc., of the University (whether academic, administrative or service-related), and any relevant subdivision with any degree of autonomy.

20 Senior Officer of a unit of the University. The classic example would be a Head of Department, but the term will encompass management of subdivisions and the leader of a team with specific information related duties. This term may be qualified (e.g., the Senior Officer of a teaching unit of the University).

21 BACUP - Brunel Acceptable Computer Use Policy.

22 Escrow - The lodgement of materials with a third party in order to provide continuity of service in the event of a default or disaster. A prime example of our use of escrow would be the use of a computing company to store up-to-date copies of source code and other items for a critical software product so that we may make amendments following the default (bankruptcy, etc.) of a supplier. A decision to use escrow will be risk-based, and is usually concentrated upon smaller suppliers.

23 Key Escrow - In this series of documents, we use the term to describe the lodgement within the University of encryption/decryption keys for an information asset of the University, which must be stored in encrypted form. This lodgement will be in a central repository independent of the day-to-day management of the asset, and will allow emergency access to the encrypted data by duly authorised users within the normal population of users of the asset, in the event of death, incapacity or other extended inaccessibility of regular key holders.

24 RFC – Request for Change – a change request highlighting and amendment to a service(s) that must be approved by CAB before implementing.

25 RMADS - Risk Management Accreditation Document Set.

26 Management - The term management refers to all the activities that are used to coordinate, direct, and control organisations. In this context, the term management does not refer to people. It refers to what managers do.

27 Management system - A management system is a set of interrelated or interacting elements that organisations use to establish policies and objectives and all the processes they need to ensure that policies are followed and objectives are achieved. These elements include structures, programs, procedures, plans, documents, records, methods, tools, techniques, technologies, roles, responsibilities, relationships, agreements, and resources. There are many types of management systems. Some of these include information security management systems, quality management systems, environmental management systems, business continuity management systems, food safety management systems, risk management systems, disaster management systems, emergency management systems, and occupational health and safety management systems. The scope or focus of a management system could be restricted to a specific function or section of an organisation or it could include the entire organisation. It could even include a function that cuts across several organisations.

28 Objective - An objective is a result you wish to achieve. Objectives can be strategic, tactical, or operational and can apply to an organisation as a whole or to a system, process, project, product, or service. A variety of words can be used to express objectives. These include words like target, aim, goal, purpose, or intended outcome.

29 Organisation - An organisation can be a single person or a group that achieves its objectives by using its own functions, responsibilities, authorities, and relationships. It can be a company, corporation, enterprise, firm, partnership, charity, or institution and can be either incorporated or unincorporated and can be either privately or publicly owned. It can also be a single operating unit that is part of a larger entity.

30 Trusted information communication entity - A trusted information communication entity is an autonomous organisation that supports the exchange of information between members of an information sharing community.

31 Competence - Competence means being able to apply knowledge and skill to achieve intended results. Being competent means having the knowledge and skill that you need and knowing how to apply it. Being competent means that you know how to do your job.

32 Conformity - Conformity is the "fulfilment of a requirement". To conform means to meet or comply with requirements. There are many types of requirements. There are information security requirements, customer requirements, contractual requirements, regulatory requirements, statutory requirements, and so on.

33 Consequence - A consequence is the outcome of an event. A single event can have a range of certain or uncertain consequences and these consequences can influence how well an organisation achieves its objectives. In addition, initial consequences can escalate through knock-on effects.

34 Context - An organisation’s context includes all of the internal and external issues that are relevant to its purpose and the influence these issues could have on its ability to achieve the objectives and outcomes that its ISMS intends to achieve. An organisation’s internal context includes its approach to governance, its contractual relationships, and its capabilities, culture, and standards. Governance includes the organisation’s structure, policies, objectives, roles, accountabilities, and decision-making process; and capabilities include its knowledge and its human, technological, capital, and systemic resources. An

organisation's external context includes stakeholder values, perceptions, and relationships, as well as its social, cultural, political, legal, regulatory, technological, economic, natural, and competitive environment. In short, context includes all the internal and external factors and forces that your information security management system must be able to cope with. ISO IEC 27001 2013 expects you to consider your organisation's internal and extern al context when you define the scope of its information security management system and when you plan its development.

2.2 Authorities

35 Brunel University Council – contribution to and approve the mission, vision and strategic direction of the University.

36 Brunel University Executive Board.

37 CESG Communications-Electronics Security Group.

38 HMG Her Majesties Government.

2.3 Roles and Responsibilities

39 CISA - Cyber, Information Security and Applications.

40 SIRO - "Senior Information Risk Owner" is the Brunel University London Head of Security and Emergency Planning and is accountable for the Brunel University London providing board level representation for all security and operational matters.

41 ISM - "Cyber & Information Security Manager" completes a number of roles such as Security Controller and interim Site Security Liaison Officer (SSLO) and will be delegated overall day to day security responsibility for all aspects of security (e.g. personnel vetting, physical, technical, procedural, DPA, etc.) relating to Brunel University London. The ISM reports directly to the SIRO.

42 SC - "Security Controller".

43 SM - "Systems Manager" will be responsible for all aspects of IT related system management and administration.

44 SSLO - "Site Security Liaison Officer" is the individual responsible for the secure operations within their nominated location (Kingston Lane, Boat House) and will be the first point of contact for all staff within these locations. The SSLO will be responsible for the physical security for their nominated location and the secure operational of all equipment pertaining to those locations etc.

45 ISG - Information Steering Group.

46 ISOP - Information Security Oversight Panel.

47 ISWP - Information Security Working Party.

48 PWG – Practitioners Working Group.

49 CAB – Change Advisory Board – Board to approve Change Requests.

50 Council - Council has ultimate accountability for information security activities within the University. More specifically, it protects institutional reputation by being assured that clear regulations, policies and procedures that adhere to legislative and regulatory requirements are in place, ethical in nature, and followed.

51 Executive Board - Has responsibility for leading and fostering a culture that values, protects and uses information for the success of the University and benefit of its members. Defining the University's information security risk appetite in the context of the prevailing legal, political, socio-economic and technological environment and external standards and ensuring that a fit for purpose and adequately resourced information security framework is in place including this policy document as a reference document. The Executive Board is ultimately accountable for information security governance and INFOSEC risk as a whole.

52 Infrastructure Strategy Committee - The Infrastructure Strategy Committee (ISC) is a forum for operational and executive consideration of University-wide digital and information services strategy.

53 Cyber and Information Security and Applications Steering Group (CISA) - The Cyber, Information Security and Applications Steering Group purpose is to drive the programme of Cyber & INFOSEC strategic projects forward and deliver the capability development outcomes and benefits as set out in the Cyber & INFOSEC strategy paper.

54 Digital Strategy Board (DSB) replaces the CISA board and functions.

55 Chief Information Officer (CIO) & SIRO - The CIO undertakes the role of Senior Information Risk Owner (SIRO) for the University. The role of the SIRO is to take ownership of the University's information risk, act as an advocate for information risk on the Executive Board.

56 Chief Information Security Officer (CISO) - The Chief Information Security Officer is a security leadership role with a core responsibility to drive and deliver the University's Cyber & Information Security Strategy, implement the Information Security Management System (ISMS) and take ownership of the University's information risk.

57 Information Asset Owners - Information Asset Owners (IAOs) are Directors and Heads of Departments held accountable for the protection of particular Information Assets. Some examples of Data Owners include the Registrar and student data; The CFO for financial data and the HR Director for employee data. Within colleges, this role will fall to the Director of College Operations or the Institute Director of Operations for research.

The IAOs are responsible for ensuring that information risk is managed appropriately and for providing assurances to the Senior Information Risk Owner (SIRO).

Information Asset Owners must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'.

IAOs are responsible for:

- Leading and fostering a culture that values, protects and uses information for the success of the University and benefit of its staff and students
- Knowing what information comprises or is associated with the asset, and understands the nature and justification of information flows to and from the asset
- Knowing who has access to the asset and why, whether it be system or information to ensure access is monitored and compliant with policy
- Understanding and addressing risks to the asset, and providing assurance to the SIRO

58 IAC – Information Asset Custodian are IT services and / or locally appointed persons (Head of IT Infrastructure and Operations, Head of Development and Application Services, College and Department IT officers) responsible for the technical environments. A system administrator or Information Asset Custodian is a person who has technical control over an information asset dataset. Usually, this person has the administrator or root account or equivalent level of access. This is a critical role and it must be executed in accordance with the access guidelines developed by the IAOs.

IACs and are responsible for:

- Implementing appropriate physical and technical controls, to protect the confidentiality, integrity and availability of University data.
- Applying the 5 cyber security controls specified by the Cyber Essentials scheme.
- Understanding and reporting on security risks and how they impact the confidentiality, integrity and availability of University Data.
- Ensuring the relevant ISMS patching and configuration policy is adopted within the centralised IT teams and reported on regularly to provide risk exposure status.

- Ensuring comprehensive disaster recovery architecture is maintained and operations are in place for such.
- Investigating and resolving information security incidents in conjunction with the Cyber & INFOSEC Manager and CISO.
- Supporting appropriately authorised forensic investigations overseen by Governance, Information, & Legal Services, the CIO or CISO.
- Ensuring compliance with required RPOs and RTOs during business continuity events.
- Motivating, organising, mentoring, and directing department managers and staff regarding the security of information assets and cyber risks.
- The corrective action plans and remediation activity from internal and external audits, and other observed vulnerabilities.

In most cases, the Information Asset Custodian is not the Information Asset Owners.

59 Data Users also have a critical role to protect and maintain BUL information systems and data. For the purpose of information security, a Data User is any employee, contractor or third-party provider who is authorised by the Data Owner to access information assets.

60 Data Protection Officer (DPO) - The Data Protection Officer (DPO) is a leadership role required by the General Data Protection Regulations (GDPR) and the data Protection Act 2018 (DPA 2018). The Data Protection Officer is responsible for overseeing the data protection strategy and its implementation to ensure compliance with GDPR.

61 Stakeholder - A stakeholder is a person or an organisation that can affect or be affected by a decision or an activity. Stakeholders also include those who have the perception that a decision or an activity can affect them.

62 IT System Administrator is a collective term to refer to any of the following:

- Server/Application Administrator
- Network Administrator
- Firewall Administrator
- Mobile Administrator

2.4 Security and Incident Terms

63 DS - “Disclosure Scotland” will be the minimum security clearance level for all Brunel University London personnel with access to University Assets or protectively marked information.

64 InfoSec – Information Security.

65 “Incident Team” is the team of people who will investigate any reported incidents.

66 “Incident Handler” is an individual who will deal with a specific incident and manage all actions taken in response to the incident. The Incident Handler is appointed by the “Incident Team” leader.

67 Incident management plan - Clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process.

68 Nonconformity - Nonconformity is a nonfulfillment or failure to meet a requirement. A requirement is a need, expectation, or obligation. It can be stated or implied by an organisation or interested parties.

69 Nonrepudiation - Nonrepudiation techniques and services are used to provide undeniable proof that an alleged event actually happened or an alleged action was actually carried out and that these events and actions were actually carried out by a particular entity and actually had a particular origin. Nonrepudiation is a way of guaranteeing that people cannot later deny that an event happened or an action was carried out by an entity.

70 Policy - A policy statement defines a general commitment, direction, or intention. An information security policy statement should express management's formal commitment to the implementation and improvement of its information security management system (ISMS) and should include information security objectives or facilitate their development.

71 Procedure - A procedure is a way of carrying out a process or activity. Procedures may or may not be documented. ISO IEC 27001 and 27002 sometimes asks you to document a procedure and sometimes it leaves it up to you to decide.

72 Audit - An audit is an evidence gathering process. Evidence is used to evaluate how well audit criteria are being met. Audits must be objective, impartial, and independent, and the audit process must be both systematic and documented. Audits can be internal or external. Internal audits are referred to as first-party audits while external audits can be either second or third party. They can also be combined audits (when two or more management systems of different disciplines are audited together at the same time).

73 Audit scope - The scope of an audit is a statement that specifies the focus, extent, and boundary of a particular audit. The scope could be specified by defining the physical location of the audit, the organisational units that will be examined, the processes and activities that will be included, and the time period that will be covered.

74 Threat - A threat is a potential event. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because the incident may harm an organisation or system.

75 Security implementation standard - A security implementation standard is a document that describes the officially or formally authorised ways in which security can be achieved or realised. Third party - A third party is any person or body that is recognised as independent of the people directly involved with an issue.

76 ISMS project - ISMS projects include all of the work that organisations do to implement information security management systems (ISMSs).

77 Governance of information security - The governance of information security refers to the system that is used to direct and control an organisation's information security activities.

78 Information security The purpose of information security is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable.

79 Information security continuity - Information security continuity refers to an integrated set of policies, procedures, and processes that are used to ensure that a predefined level of security continues during a disaster or crisis (when disruptive incidents occur or adverse situations exist). Continuity is achieved by identifying potential threats and vulnerabilities, by analysing possible impacts, and by taking steps to build organisational resilience.

80 Information security event - An information security event is a system, service, or network state, condition, or occurrence that indicates that information security may have been breached or compromised or that a security policy may have been violated or a control may have failed.

81 Information security incident - An information security incident is made up of one or more unwanted or unexpected information security events that could possibly compromise the security of information and weaken or impair business operations.

82 Information security incident management - Information security incident management is a set of processes that organisations use to deal with information security incidents. It includes a detection process, a reporting process, an assessment process, a response process, and a learning process.

83 Information sharing community - An information sharing community is a group of people or a group of organisations that agree to share information.

2.5 Risk, Business Continuity, Disaster Recovery Planning and Disposal Terms

84 ARP - Activity Recovery Plans.

85 ADISA - Asset Disposal & Information Security Alliance.

86 BC - Business continuity - Strategic and tactical capability of the Brunel University London to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level.

87 BCM - Business Continuity Management - Holistic management process that identifies potential threats to an Brunel University London and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building Brunel University London resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

88 BCML - Business continuity management lifecycle - Series of business continuity activities which collectively cover all aspects and phases of the business continuity management programme.

89 BCP - Business Continuity Plan - Documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an Brunel University London to continue to deliver its critical activities at an acceptable pre-defined level.

90 BCS - Business continuity strategy - Approach by an Brunel University London that will ensure its recovery and continuity in the face of a disaster or other major incident or business disruption.

91 BIA - Business Impact Analysis - Process of analysing business functions and the effect that a business disruption might have upon them.

92 BIL - Business Impact Level.

93 CBP - Critical business process - Identified as part of the Business Impact Analysis as one of the first business processes to be recovered.

94 CFIA - Component Failure Impact Analysis - A study that attempts to predict the impact resulting from a failure of a component of a system.

95 CMT - Crisis Management Team.

96 CRP Component Recovery Plans.

97 CSIRT – Computer Security Incident Response Team.

98 DR - Disaster Recovery.

99 IAS Information Assurance Standard.

100 IL Impact Level (1-5).

101 IRT - Incident Response Team.

102 ERT Emergency Response Team - The emergency response team is a team of business professionals trained and prepared to respond to an emergency incident such as natural disasters and/or an interruption of business operations.

103 Exercise - Activity in which the business continuity plan(s) is rehearsed in part or in whole to ensure that the plan(s) contains the appropriate information and produces the desired result when put into effect.

104 ITRP - IT Recovery Plans.

105 MTPOD - Maximum Tolerable Period of Disruption - The Maximum Tolerable Period of Disruption or MTPOD is the “duration after which an Brunel University London’s viability will be irrevocably threatened if product and service delivery cannot be resumed.

106 Risk - Something that might happen and its effect(s) on the achievement of objectives. According to ISO 31000, risk is the “effect of uncertainty on objectives” and an effect is a positive or negative deviation from what is expected. The following paragraph will explain what this means. ISO 31000 recognises that all of us operate in an uncertain world. Whenever we try to achieve an objective, there’s always the chance that things will not go according to plan. Every step has an element of risk that needs to be managed and every outcome is uncertain. Whenever we try to achieve an objective, we don't always get the results we expect. Sometimes we get positive results and sometimes we get negative results and occasionally we get both. Because of this, ISO 31000 wants us to reduce uncertainty as much as possible. Information security risk is often expressed as a combination of two factors: probability and consequences. It asks two basic questions: what is the probability that a particular information security event will occur in the future? And what consequences would this event produce or what impact would it have if it actually occurred? Information security risks often emerge because potential security threats are identified that could exploit vulnerabilities in an information asset or group of assets and therefore cause harm to an organisation.

107 Risk acceptance - Risk acceptance means that you’ve deliberately decided that you can live with or tolerate a particular risk or that you're prepared to take a particular risk. Accepted risks should be monitored and periodically reviewed. While risk acceptance is normally part of the risk treatment decision making process it can occur outside of this process.

108 Risk analysis - Risk analysis is a process that is used to understand the nature, sources, and causes of the risks that have been identified and to estimate the level of risk. Risk analysis results are used to carry out risk evaluations and to make risk treatment decisions. How detailed your risk analysis ought to be will depend upon the risk, the purpose of the analysis, the information you have, and the resources available.

109 Risk assessment - Overall process of risk identification, analysis and evaluation Risk assessment is a process that is, in turn, made up of three processes: risk identification, risk analysis, and risk evaluation. Risk identification is a process that is used to find, recognise, and describe the risks that could affect the achievement of objectives. Risk analysis is a process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. Risk evaluation is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable.

110 Risk communication and consultation - Risk communication and consultation is a dialogue between an organisation and its stakeholders. Discussions could be about the existence of risks, their nature, form, likelihood, and significance, as well as whether or not risks are acceptable or should be treated, and what treatment options should be considered. This dialogue is both continual and iterative. It is a two-way process that involves both sharing and receiving information about the management of risk. However, this is not joint decision making. Once communication and consultation is finished, decisions are made and directions are established by the organisation, not by stakeholders.

111 Risk criteria - Risk criteria are terms of reference and are used to evaluate the significance or importance of an organisation’s risks. They are used to determine whether a specified level of risk is acceptable or tolerable. Risk criteria should reflect your organisation’s values, policies, and objectives, should be based on its external and internal context, should consider the views of stakeholders, and should be derived from standards, laws, policies, and other requirements.

112 Risk evaluation - Risk evaluation is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a risk or a specified level of risk is

acceptable or tolerable. Risk evaluation results are used to help select risk treatment options.

113 Risk identification - Risk identification is a process that involves finding, recognising, and describing the risks that could affect the achievement of an organisation's objectives. It involves discovering possible sources of risk in addition to the events and circumstances that could affect the achievement of objectives; it also includes the identification of possible causes and potential consequences. You may use historical data, theoretical analysis, informed opinion, expert advice, and stakeholder input to identify your risks.

114 Risk management - The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects Risk management refers to a coordinated set of activities, methods, and techniques that organisations use to deal with the risk and uncertainty that influences how well they achieves their objectives. Risk management process A risk management process is one that systematically uses management policies, procedures, and practices to establish context, to communicate and consult with stakeholders, and to identify, analyse, evaluate, treat, monitor, and review risk.

115 Risk owner - A risk owner is a person or entity that has been given the authority to manage a particular risk and is accountable for doing so.

116 Risk treatment - Risk treatment is a risk modification process. It involves selecting and implementing one or more treatment options. Once a risk treatment option has been implemented, it becomes a control or it modifies an existing control. You have many risk treatment options. You can avoid the risk, you can reduce the risk, you can remove the source of the risk, you can modify the consequences, you can change the probabilities, you can share the risk with others, you can simply retain the risk, or you can even increase the risk in order to pursue an opportunity.

117 Residual risk - Residual risk is the risk left over after you've implemented a risk treatment option. It's the risk remaining after you've reduced the risk, removed the source of the risk, modified the consequences, changed the probabilities, transferred the risk, or retained the risk.

118 Level of risk - The level of risk is its magnitude. It is estimated by considering and combining consequences and likelihoods. A level of risk can be assigned to a single risk or to a combination of risks.

119 Likelihood - Likelihood is the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively (using mathematics).

120 RPO - Recovery Point Objective - The Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time, it is the point in time to which you must recover data as defined by the University. This is generally a definition of what an Brunel University London determines is an "acceptable loss" in a disaster situation

121 RTO - Recovery Time Objective - The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

122 SEAP - Security Equipment Approval Panel.

123 Service Continuity Team - The team responsible for managing risks that could seriously affect IT services. IT service continuity management ensures that the IT service provider can always provide minimum agreed service levels, by reducing the risk to an acceptable level and planning for the recovery of IT Services.

124 SPF - Security Policy Framework.

125 WEEE Hasardous Waste Regulations, the Waste, Electrical and Electronic Equipment Directive.

2.6 Virus and Malware Terms

126 Adware - Software that automatically plays, displays, or downloads advertisements to a computer, often in exchange for the right to use a program without paying for it. The advertisements seen are based on monitoring of browser habits. Most adware is safe to use, but some can serve as spyware, gathering information about you from your hard drive, the websites you visit, or even your keystrokes. Certain types of adware have the capability to capture or transmit personal information.

127 Antivirus Software - A type of software that scans a computer's memory and disk drives for viruses. If it finds a virus, the application informs the user and may clean, delete, or quarantine any files, directories, or disks affected by the virus. The term antimalware is preferred because it covers more threats.

128 Browser Hijacker - A type of malware that alters your computer's browser settings so that you are redirected to websites that you had no intention of visiting. Most browser hijackers alter browser home pages, search pages, search results, error message pages, or other browser content with unexpected or unwanted content.

129 Dat Files - Also known as a data file, these files are used to update software programs, sent to users via the Internet. .DAT files contain up-to-date virus signatures and other information antivirus products use to protect your computer against virus attacks. .DAT files are also known as detection definition files and signatures.

130 Keylogger - Software that tracks or logs the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. This is usually done with malicious intent to collect information including instant messages, email text, email addresses, passwords, credit card and account numbers, addresses, and other private data.

131 Malware - A generic term used to describe any type of software or code specifically designed to exploit a computer or the data it contains, without consent. Malware includes viruses, Trojan horses, spyware, adware, most rootkits, and other malicious programs.

132 Phishing - A form of criminal activity using social engineering techniques through email or instant messaging. Phishers attempt to fraudulently acquire other people's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Typically, phishing emails request that recipients click on the link in the email to verify or update contact details or credit card information. Like spam, phishing emails are sent to alarge number of email addresses, with the expectation that someone will act on the information in the email and disclose their personal information. Phishing can also happen via text messaging or phone.

133 Ransomware - Malicious software created by a hacker to restrict access to the compute system that it infects and demand a ransom paid to the creator of the malicious software for the restriction to be removed. Some forms of ransomware may encrypt files on the system's hard drive, while others may simply lock the system and display messages to coax the user into paying.

134 Spam - An unwanted electronic message, most commonly unsolicited bulk email. Typically, spam is sent to multiple recipients who did not ask to receive it. Types include email spam, instant messaging spam, web search-engine spam, spam in blogs, and mobile phone-messaging spam. Spam includes legitimate advertisements, misleading advertisements, and phishing messages designed to trick recipients into giving up personal and financial

information. Email messages are not considered spam if a user has signed up to receive them.

135 Spyware - Spyware spies on a user's computer. Spyware can capture information like web browsing habits, email messages, usernames and passwords, and credit card information. Just like viruses, spyware can be installed on a computer through an email attachment containing malicious software

136 Trojan - Malicious programs disguised as legitimate software. Users are typically tricked into loading and executing it on their systems. One key factor that distinguishes a Trojan from viruses and worms is that Trojans don't replicate.

2.7 Computing specific Terms

137 The term “Workstation” pertains to both desktop and laptop computers.

138 The term “Data Centre” (DC) relates to the Brunel University London System located within the Data Centres.

139 RMADS - “Risk Management Accreditation Documentation Set” defines the Security Standards and Procedures which will ensure that the Brunel University London System protects the confidentiality, integrity and availability of the information it stores and transmits

140 MU - “Mobile User” will be Users, who will not necessarily have access to the University System, but need to adhere to strict security policies if holding University Confidential data on a Mobile machine,

141 OS - “Operating System”

142 OU - “Active Directory Organisational Unit”

143 SAN - “Storage Area Network”

144 LAN - “Local Area Network”

145 WSUS - “Windows Server Update Services

146 BUDN - Brunel University Data Network - The network of storage, servers, computers and like devices which provide electronic services for or at the University, whether owned, leased or otherwise acquired by the University, or owned by a third party for the purposes of transacting academic or corporate business of the University.

147 Username. Unique identifier for an authorised user’s personal and sole use for access to all information systems and services of the University. All Brunel documentation should use this term, rather than variants found elsewhere (login ID, user ID, etc.).

148 DSL - The Definitive Software Library identifies and holds a copy of all the software installed in the IT environment. This includes not just operating systems and applications, but also device drivers and any associated documentation.

149 Access control - Access control includes both access authorisation and access restriction. It refers to all the steps that are taken to selectively authorise and restrict entry, contact, or use of assets. Access authorisations and restrictions are often established in accordance with University and security requirements.

150 Asset - An asset is any tangible or intangible thing or characteristic that has value to an organisation. There are many types of assets. Some of these include obvious things like machines, facilities, patents, and software. But the term can also include less obvious things like services, information, and people, and characteristics like reputation and image or skill and knowledge.

151 Attack - An attack is any unauthorised attempt to access, use, alter, expose, steal, disable, or destroy an asset. Attribute An attribute is any distinctive feature, characteristic, or property of an object that can be identified or isolated quantitatively or qualitatively by either human or automated means.

152 Data - The term data is defined as a collection or set of values assigned to measures or indicators. A measure is a variable made up of values and an indicator is a measure or variable that is used to evaluate or estimate an attribute or property of an object.

153 Vulnerability - A vulnerability is a weakness of an asset or control that could potentially be exploited by one or more threats. An asset is any tangible or intangible thing or characteristic that has value to an organisation, a control is any administrative, managerial, technical, or legal method that can be used to modify or manage risk, and a threat is any potential event that could harm an organisation or system.

154 Accountability - To make an entity accountable means to assign actions and decisions to that entity and to expect that entity to be answerable for those actions and decisions. Therefore, accountability is the state of being answerable for the actions and decisions that have been assigned.

155 Analytical model - An analytical model is an algorithm or calculation that combines one or more base or derived measures with a set of decision criteria. Analytical models are used to facilitate and support decision making.

156 Authentication - Authentication is a process that is used to confirm that a claimed characteristic of an entity is actually correct. To authenticate is to verify that a characteristic or attribute that appears to be true is in fact true.

157 Authenticity - Authenticity is a property or characteristic of an entity. An entity is authentic if it is what it claims to be.

158 Base measure - A base measure is both an attribute or property of an entity and the method used to quantify it.

159 Continual improvement - Continual improvement is a set of recurring activities that are carried out in order to enhance the performance of processes, products, services, systems, and organisations.

160 Control - In the context of information security management, a control is any administrative, managerial, technical, or legal method that is used to modify or manage information security risk. Controls can include things like practices, processes, policies, procedures, programs, tools, techniques, technologies, devices, and organisational structures. Controls are sometimes also referred to as safeguards or countermeasures. ISO IEC 27001 part 6.13 expects you to select the controls that your organisation needs in order to implement its risk treatment options and carry out its risk treatment plan. Your list of controls will make up your Statement of Applicability. See ISO IEC 27001 2013 Annex A and ISO IEC 27002 2013 for a list of security control options.

161 Control objective - An information security control objective is a statement that describes what your information security controls are expected to achieve.

162 Correction - A correction is any action that is taken to eliminate a nonconformity. Corrections do not address causes (corrective actions address causes).

163 Corrective action - Corrective actions are steps that are taken to eliminate the causes of existing nonconformities in order to prevent recurrence. The corrective action process tries to make sure that existing nonconformities and potentially undesirable situations don’t happen again.

164 Decision criteria - Decision criteria are factors like thresholds, targets, or patterns. Decision criteria are used to determine whether action should be taken or whether further investigation is required before decisions can be made. Decision criteria are also used to evaluate results and to describe confidence levels.

165 Derived measure - A derived measure is a measure that is defined as a mathematical function of two or more values of base measures (a base measure is both an attribute of an entity and the method used to quantify it).

166 Documented information - The term documented information refers to information that must be controlled and maintained and its supporting medium. Documented information can be in any format and on any medium and can come from any source. Documented information includes information about the management system and related processes. It also includes all the information that organisations need to operate and all the information that they use to document the results that they achieve (aka records). In short, the term documented information is just a new name for what used to be called documents and records. But this change is significant. In the past, documents and records were to be managed differently. Now the same set of requirements are to be applied to both documents and records.

167 Effectiveness - Effectiveness refers to the degree to which a planned effect is achieved. Planned activities are effective if these activities are actually carried out and planned results are effective if these results are actually achieved.

168 Efficiency - Efficiency is a relationship between results achieved (outputs) and resources used (inputs). Efficiency can be enhanced by achieving more with the same or fewer resources. The efficiency of a process or system can be enhanced by achieving more or getting better results (outputs) with the same or fewer resources (inputs).

169 Event - An event could be one occurrence, several occurrences, or even a non-occurrence (when something doesn't happen that was supposed to happen). It can also be a change in circumstances. Events are sometimes referred to as incidents or accidents. Events always have causes and usually have consequences.

170 External context - An organisation's external context includes all of the factors and forces that exist beyond its own boundaries that influence how it tries to achieve its objectives. It includes its external stakeholders, its local, national, and international environment, as well as key drivers and trends that influence its objectives. It includes stakeholder values, perceptions, and relationships, as well as its social, cultural, political, legal, regulatory, financial, technological, economic, natural, and competitive environment.

171 Guideline - In the context of this standard, guidelines are the steps that are taken to achieve objectives and implement policies. Guidelines clarify what should be done and how.

172 Indicator - An indicator is a measure or variable that is used to evaluate or estimate an attribute or property of an object. Indicators are often derived from analytical models and are used to address information needs.

173 Information need - An information need is an insight that is necessary or required in order to solve problems, to manage risks, and to achieve goals and objectives.

174 Information processing facilities - An information processing facility is any system, service, or infrastructure, or any physical location that houses these things. A facility can be either an activity or a place and it can be either tangible or intangible.

175 Information system - An information system is any set of components that is used to handle information. Information systems include applications, services, or any other assets that handle information.

176 Internal context An organisation's internal context includes all of the factors and forces within its boundaries that influence how it tries to achieve its objectives. It includes its internal stakeholders, its approach to governance, its contractual relationships, and its capabilities, culture, and standards. 1 Governance includes the organisation's structure, policies, objectives, roles, accountabilities, and decision making process; and capabilities include its knowledge and its human, technological, capital, and systemic resources.

177 Measure - A measure is a variable made up of values. When measurement is carried out, a value (quantity) is assigned to a variable. Measurement - Measurement is a process that is

used to determine a value. In the context of information security management, measurement is a process that is used to obtain information about the effectiveness of an information management system (ISMS) and the controls that it uses. Measurement functions, analytical models, and decision criteria are used to evaluate measurement results and to decide whether action should be taken or whether further investigation is required before decisions can be made.

178 Measurement function - A measurement function is an algorithm or a calculation that combines two or more base measures. (A base measure is both an attribute or property of an entity and the method used to quantify it.)

179 Measurement method - A measurement method is a logical sequence of generic operations that uses measurement scales to quantify attributes. Measurement methods use either objective or subjective techniques to quantify attributes.

180 Measurement results - A measurement result addresses an information need and consists of one or more indicators together with details that explain how these indicators are to be interpreted.

181 Monitoring - To monitor means to determine the status of an activity, process, or system. In order to determine status, you may need to supervise and to continually check and critically observe the activity, process, or system that is being monitored.

182 Object - In this context, an object is any item that has attributes which can be characterised through measurement. Measurement is a process or method that is used to obtain information about the effectiveness of an information management system (ISMS) and the controls that it uses.

183 Outsource - When an organisation makes an arrangement with an outside organisation to perform part of a function or process, it is referred to as outsourcing. To outsource means to ask an external organisation to perform part of a function or process usually done in-house.

184 Performance - A performance is a measurable result that is achieved by an activity, process, product, service, system, or organisation. This definition allows us to consider performance measurements. It allows us to think about the measurement of organisational performance, process performance, product performance, service performance, systemic performance, and so on. Such measurements can be either quantitative or qualitative.

185 Process - A process is a set of activities that are interrelated or that interact with one another. Processes use resources to transform inputs into outputs.

186 Record - Records provide evidence that activities have been performed or results have been achieved. Records always document the past.

187 Reliability - Reliability is a property of something and means consistency. Something is reliable if it behaves consistently or produces consistent results.

188 Requirement - A requirement is a need, expectation, or obligation. It can be stated or implied by an organisation, its customers, or other interested parties. A specified requirement is one that has been stated (in a document for example), whereas an implied requirement is a need, expectation, or obligation that is common practice or customary.

189 Review - A review is an activity. Its purpose is to determine how well the thing being reviewed is capable of achieving established objectives. Reviews ask the following question: is the subject of the review a suitable, adequate, effective, and efficient way of achieving objectives?

190 Review object - A review object is the item or thing being reviewed.

191 Review objective - A review objective is a statement that describes what a review is intended or expected to achieve.

192 Scale - A scale is an ordered set of values. Scales can be distinguished from one another based on how values on the same scale are interrelated. There are at least four types of scales: nominal, ordinal, interval, and ratio. Nominal scales use categories as values (e.g. female vs. male), ordinal scales rank values (1st, 2nd, 3rd, 4th, etc.), interval scales use equal quantities as values (e.g., dates and temperatures), and ratio scales use values that specify how much or how many (e.g. duration and length). Ratio scales are possible because they exploit the fact that sometimes it makes sense to use zero as a value. Being able to use a zero value allows you to do calculations and to say that something is twice as far as something else or takes three times as long as something else, for example.

193 Unit of measurement - A unit of measurement is a particular quantity or magnitude that is used as a standard for comparing measurements of the same kind. A standard unit of measurement is one that has been defined and adopted by convention, by agreement, or officially established by law.

194 Validation - Validation is a process. It uses objective evidence to confirm that the requirements which define an intended use or application have been met. Whenever all requirements have been met, a validated status is achieved. The process of validation can be carried out under realistic use conditions or within a simulated use environment.

195 Verification - Verification is a process that uses objective evidence to confirm that specified requirements have actually been met. Verification is sometimes referred to as compliance testing.