2012 Resilience Benchmarking Glossary of Key Terms

Anti-virus

Application software deployed at multiple points in an IT architecture
It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected

SOURCE: Information Systems Audit & Control Association (ISACA), (2012), Glossary, http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

Audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

SOURCE: National Institute of Standards and Technology (NIST), (2001), SP 800 – 32 Introduction to Public Key Technology and the Federal KPI Infrastructure, http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf

BCM – Business Continuity Management

Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

SOURCE: International Organisation for Standardisation, (2012), ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements

BCMPG – Business Continuity Management Practice Guide

Standard and leading practices identified during the Tripartite Resilience Benchmarking exercise in a format which shares the practices and lessons with the wider sector.

SOURCE: Resilience Benchmarking Support Group (2012)

BCP – Business Continuity Plan

A clearly defined and documented plan for use at the time of a business emergency, event, incident and/or crisis. Typically a plan will cover all key personnel, resources, services and actions required to manage the *BCM* process.

SOURCE: Tripartite Authorities, (2008), Resilience Benchmarking Project Discussion Paper

BIA – Business Impact Analysis

Process of analysing activities and the effect that a business disruption might have upon them.

SOURCE: International Organisation for Standardisation, (2012), ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements

Biannually

Occurring twice a year.

SOURCE: http://oxforddictionaries.com

Biennially

Taking place every two years.

SOURCE: http://oxforddictionaries.com

BAU – Business as Usual

The organisation's ability to meet its business as usual objectives and maintain levels of staffing and transaction volumes as they would be during normal operations.

SOURCE: Adapted from the MWE 2011 Glossary of Acronyms

BS25999

A British standard developed to define requirements for a management systems approach to business continuity management based on good practice for use in large, medium and small organisations operating in industrial, commercial, public and voluntary sectors.

SOURCE: BS25999-2:2007

BYOD – Bring Your Own Device

Bring your own device (BYOD) is an alternative strategy allowing employees, business partners and other users to use a personally selected and purchased client device to execute enterprise applications and access data.

SOURCE: Gartner IT Glossary 2012 - http://www.gartner.com/it-glossary

Cash Flow and Liquidity

The ability of the organisation to manage and control the risks associated with market positions by ensuring that funds and securities are available to meet obligations and hedge risks.

SOURCE: Tripartite Authorities, (2005), Resilience Benchmarking Project Discussion Paper

CERT – Computer Emergency Response Team

An organisation that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

SOURCE: SANS Institute, (2012), http://www.sans.org/

CMT – Crisis Management Team

A *Crisis Management Team* typically consists of senior members of staff and is the team responsible for managing the organisation's strategic and/or tactical response to a *major operational disruption* or crisis incident.

SOURCE: Tripartite Authorities, (2011) MWE 2011 Glossary of Acronyms

Core Firms

For the purpose of benchmarking, *core firms* are firms which, as part of their business, provide key market infrastructure functionality, the failure of which could impact significantly on other firms in the market. It does not include those entities whose main or sole function is the provision of financial infrastructure services (see *financial infrastructure providers*).

SOURCE: Tripartite Authorities, (2008), Resilience Benchmarking Project Discussion Paper

Controls / Key Controls

The methods, policies, and procedures - manual or automated - that are adopted by an organisation to ensure the safeguarding of assets, the accuracy and reliability of management information and financial records, the promotion of administrative efficiency, and adherence to standards.

SOURCE: Glossary of Terms (updated 25/05/2010), CERT - http://www.cert.org/resilience/download/d.html

Critical Business Functions

The functions (internal or outsourced), without which the organisation would be unable to achieve its business objectives. For the purposes of benchmarking, they are defined as *wholesale payments, trade clearing, securities settlement, cash flow and liquidity, trading, custody and other critical systems.*

SOURCE: Tripartite Authorities, (2008), Resilience Benchmarking Project Discussion Paper

Critical Systems
The systems that support *critical business functions* (internal or outsourced) without which the organisation would be unable to achieve its business objectives.

SOURCE: Adapted from Tripartite Authorities, (2011) MWE 2011 Glossary of Acronyms

Custody
The holding of financial assets and *securities* in safe keeping, including the provision to clients of *settlement* and reporting services for all classes of financial instruments.

SOURCE: Tripartite Authorities, (2005), Resilience Benchmarking Project Discussion Paper

Cyber Attack / Cyber – attack
An attack, via *cyberspace*, targeting an organisation's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment / infrastructure; or destroying the integrity of the data or stealing controlled information.

SOURCE: Committee on National Security Systems (CNSSI), (2010), CNSSI – 4009 National Information Assurance Glossary, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

Cyber Resilience
See *Technology and Cyber Resilience*.

Cyber Security
The ability to protect or defend the use of cyberspace from cyber-attacks.

SOURCE: Committee on National Security Systems (CNSSI), (2010), CNSSI – 4009 National Information Assurance Glossary, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

Cyber Space
Cyber space is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.

SOURCE: http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy

Data Centre
A large group of networked computer servers typically used by organisations for the remote storage, processing or distribution of large amounts of data.

SOURCE: Oxford Dictionaries, (2012), http://oxforddictionaries.com

DR – Disaster Recovery

An IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The scope may overlap that of an IT Service Continuity Plan; however, the DR Plan is narrower in scope and does not address Business Impact Analysis. Also referred to as IT Disaster Recovery.

SOURCE: National Institute of Standards and Technology (NIST), (2001), SP 800 – 34 Contingency Planning Guide for Federal Information Systems, http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Disaster Recovery Service

Services (including data recovery, work area recovery and individual technologies and processes), to enable an organisation to return to an agreed level of business as usual following business or technology disruption affecting the organisation.

SOURCE: Resilience Benchmarking Support Group, (2012)

DoS – Denial of Service

An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.

SOURCE: National Institute of Standards and Technology (NIST), (2001), SP 800 – 61 Computer Security Handling Guide, http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

DDoS – Distributed Denial of Service

A Denial of Service technique that uses numerous hosts to perform the attack.

SOURCE: National Institute of Standards and Technology (NIST), (2001), SP 800 – 61 Computer Security Handling Guide, http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

Encryption

Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

SOURCE: SANS Institute, (2012), http://www.sans.org/

Evaluation System

Automated process responsible for assessing a new or changed IT service to ensure that risks have been managed and to help determine whether to proceed with the change.

SOURCE: Adapted from ITIL v3, Service Design (2007)

Exercise
Process to train for, assess, practice, and improve performance in an organisation.

SOURCE: International Organisation for Standardisation, (2012), ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements

Financial Infrastructure Providers
Key UK-based exchanges, clearing houses, settlement banks and payment system operators.

SOURCE: Tripartite Authorities, (2008), Resilience Benchmarking Project Discussion Paper

Hosting Pattern
Where and how technology is organised and 'housed'. Examples include in-house data centres, managed data centres, 3rd party data centres, number of data centres which the technology is spread across or synchronised technology etc.

SOURCE: Resilience Benchmarking Support Group, (2012)

Horizon Scanning
The systematic examination of potential threats, opportunities and likely future developments which are at the margins of current thinking and planning.

SOURCE: Defra, (2005), http://horizonscanning.defra.gov.uk/

IDS – Intrusion Detection System
Hardware or software product that gathers and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organisations) and misuse (attacks from within the organisations.)

SOURCE: Committee on National Security Systems (CNSSI), (2010), CNSSI – 4009 National Information Assurance Glossary, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

IMP – Incident Management Plan
A 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.

SOURCE: British Standards Institute, (2007), BS25999-2:2007 Business Continuity Management Specification

Incident
Situation that might, be or could lead to, a disruption, loss, emergency or crisis.

SOURCE: International Organisation for Standardisation, (2012), ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements

Invocation
Act of declaring that an organisation's business continuity arrangements need to be put into effect in order to continue delivery of key products or services.

SOURCE: International Organisation for Standardisation, (2012), ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements

IPS – Intrusion Prevention System
Any device (hardware or software) that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful.

SOURCE: Symantec, (2010), http://www.symantec.com/connect/articles/intrusion-prevention-systems-next-step-evolution-ids

ISO22301
A standard produced by the International Organisation for Standardisation which specifies requirements for setting up and managing an effective business continuity management system.

SOURCE: International Organisation for Standardisation, (2012), ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements

ITSCM – IT Service Continuity Management
The process responsible for management of risks that could seriously affect IT services. ITSCM ensure 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. ITSCM should be designed to support *Business Continuity Management*.

SOURCE: ITIL v3 Service Design (2007)

ITSCP - IT Service Continuity Plan
A plan defining the steps required recovering one or more IT services. The plan will also identify the triggers for invocation, people to be involved, communications, etc. It may also be referred to as Recovery Plan, Technical Recovery Action Plan (TRAP) or a derivative of one of these forms.

SOURCE: ITIL v3 Service Design (2007)

KPI's – Key Performance Indicators / KRI's – Key Risk Indicators

A metric used to help manage a process, IT service or activity. Many metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the process, IT service or activity. KPIs should be selected to ensure that efficiency, effectiveness and cost effectiveness are all managed.

SOURCE: ITIL v3 Service Design (2007)

Major Change

An addition, modification or removal that could have a *significant* effect on IT services and / or business operations.

SOURCE: Resilience Benchmarking Support Group, (2012)

Major Incident

The highest category of impact for an incident which results in *significant* disruption to the business.

SOURCE: ITIL v3 Service Design (2007)

Major Operational Disruption

An incident having a widespread and severe impact on multiple organisations and that requires the implementation of special arrangements for continued operation of *critical business functions*. Also see major incident.

SOURCE: Resilience Benchmarking Project Discussion Paper, (2008)

Malware

A term derived from 'malicious software', a common name for all kinds of unwanted software such as *viruses*, worms and Trojans.

SOURCE: Tripartite Authorities, (2011) MWE 2011 Glossary of Acronyms

Manual Work Around

A workaround that requires manual intervention. Manual Workaround is also used as the name of a recovery option in which the business process operates without the use of IT services. This is a temporary measure and is usually combined with another recovery option.

SOURCE: ITIL v3, Service Design (2007)

Market Data

Quote and trade-related data associated with equity, fixed-income, financial derivatives, currency etc. which is numerical price data reported from trading venues e.g. stock exchanges.

SOURCE: Resilience Benchmarking Support Group, (2012)

Monitoring System
Automated repeated observation of a configuration item, IT service or process to detect events and to ensure that the current status is known.

SOURCE: Adapted from ITIL v3, Service Design (2007)

MOD – Major Operational Disruption
An incident having a widespread and severe impact on multiple organisations and that requires the implementation of special arrangements for continued operation of *critical business functions*.

SOURCE: Tripartite Authorities, (2008), Resilience Benchmarking Project Discussion Paper

Multi-layered Anti-virus
A combination of multiple layers of anti-virus and sometimes spyware programs used to protect an organisation's systems and data from attack.

SOURCE: Resilience Benchmarking Support Group, (2012)

Near Miss
Events or situations which have the potential to result in an actual loss (or gain), but which are narrowly avoided or minimised.

SOURCE: Adapted from FSA, (2011) Enhancing frameworks in the standardised approach to operational risk – Guidance note

Other Critical Systems
Systems (other than *wholesale payments, trade clearing, securities settlement, cash flow and liquidity, trading, custody*) identified through the *business impact analysis* that support *critical business functions* (internal or outsourced), without which the organisation would be unable to achieve its business objectives.

SOURCE: Resilience Benchmarking Support Group, (2012)

Outsourced
An external service provider to manage IT services.

SOURCE: ITIL v3, Service Design (2007)

Patches
A release or update to software designed to fix problems with, or update, a computer program or its supporting data.

SOURCE: Resilience Benchmarking Support Group, (2012)

Pen Testing - Penetration Testing
A live test of the effectiveness of security defences through mimicking the actions of real life attackers.

SOURCE: Information Systems Audit & Control Association (ISACA), (2012), Glossary, http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

Policy
Intentions and direction of an organisation as formally expressed by its *top management*.

SOURCE: International Organisation for Standardisation, (2012), ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements

Recovery Plans
A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster.

SOURCE: Information Systems Audit & Control Association (ISACA), (2012), Glossary, http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

Remote Access
The ability to access technology and systems over a network from a location which is not a production or recovery site e.g. working from home via a secure method.

SOURCE: Resilience Benchmarking Support Group, (2012)

Resilience
In the context of Technology and Cyber Resilience Benchmarking see *Technology and Cyber Resilience*.

Risk and Control Assessments
A control risk self-assessment is a method / process by which management and staff of all levels collectively identify and evaluate risk and controls with their business areas. This may be under the guidance of a facilitator such as an auditor or risk manager.

SOURCE: Information Systems Audit & Control Association (ISACA), (2012), Glossary, http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

Risk Assessments
Overall process of risk identification, risk analysis and risk evaluation.

SOURCE: International Organisation for Standardisation, (2012), ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements

RPO – Recovery Point Objective
Point to which information used by an activity must be restored to enable the activity to operate on resumption (can also be referred to as maximum data loss).

SOURCE: International Organisation for Standardisation, (2012), ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements

RTO – Recovery Time Objective
Period of time following an incident within which a product, service or activity must be resumed or resources must be recovered.

SOURCE: International Organisation for Standardisation, (2012), ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements

Securities
Instruments that signify an ownership position in a corporation, a creditor relationship with a corporation or governmental body, or other rights to ownership.

SOURCE: Tripartite Authorities, (2008), Resilience Benchmarking Project Discussion Paper

Service Delivery
Normally, a reference to the five management processes described in the IT Infrastructure Library 'Service Delivery' volume, i.e., Service Level, Capacity, IT Service Continuity and Availability Management, plus Financial Management for IT Services.

SOURCE: ITIL v3 Service Design (2007)

Settlement
The process of transferring ownership after a trade has been carried out.

SOURCE: Tripartite Authorities, (2008), Resilience Benchmarking Project Discussion Paper

Securities Settlement Systems
A system which permits the holding and transfer of securities, either free of payment or against payment (delivery versus payment) or against another asset (delivery versus delivery). It comprises all the institutional and technical arrangements required for the settlement of securities trades and the safekeeping of securities. The system can operate on a real-time gross settlement, gross settlement or net settlement basis. A

settlement system allows for the calculation (clearing) of the obligations of participants.

SOURCE: Organisation for Economic Co-operation and Development (OECD) 2005 - http://stats.oecd.org/glossary/detail.asp?ID=6793

Significant
Sufficiently great or important to be worthy of attention; noteworthy

SOURCE: Oxford Dictionaries, (2012), http://oxforddictionaries.com

SLA – Service Level Agreement
An agreement between an IT service provider and a customer. The SLA describes the IT service, documents service level targets, and specifies the responsibility of the IT service provider and the customer. A single SLA may cover multiple IT services or multiple customers.

SOURCE: ITIL v3 Service Design (2007)

Supplier
See *Vendor*.

Technology and Cyber Resilience
In the context of this benchmarking, Technology and Cyber Resilience are properties of digital networks, the internet, infrastructure and services which are used to store, modify and communicate information that support the business and its ability to resist intentional and unintentional threats and respond and recover.

SOURCE: Adapted from EastWest Institute (2011) Russia-U.S. Bilateral on Cyber Security: Critical Terminology Foundations. EWI: New York. http://www.ewi.info/cybersecurity-terminology-foundations

Testing
Procedure for evaluation; a means of determining the presence, quality, or veracity of something.

SOURCE: International Organisation for Standardisation, (2012), ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements

Third Party
A person, group, or business that is not part of the service level agreement for an IT service, but is required to ensure successful delivery of that IT service.

SOURCE: ITIL v3 Service Design (2007)

Top Management
Person or group of people who direct and control an organisation at the highest level.

SOURCE: International Organisation for Standardisation, (2012), ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements

Trade Clearing
The process of clearing whereby the mutual obligations of the market participants are calculated for the exchange of *securities* and cash.

SOURCE: Tripartite Authorities, (2008), Resilience Benchmarking Project Discussion Paper

Trading
The act of a buyer and seller coming together and agreeing to exchange a given security (or contract in the case of derivatives) at an agreed price and point in time. Trading can be executed via an exchange-provided trading system, or over the counter.

SOURCE: Tripartite Authorities, (2008), Resilience Benchmarking Project Discussion Paper

Tripartite Authorities
HM Treasury, the Bank of England and the Financial Services Authority (FSA).

SOURCE: Tripartite Authorities, (2008), Resilience Benchmarking Project Discussion Paper

Vendor
An individual or company providing a service to a department or the organisation as a whole.

SOURCE: European Network and Information Security agency (ENISA) http://www.enisa.europa.eu

Virus
An unauthorised programme that inserts itself into a computer system and then propagates itself to other computers via networks or disks.

SOURCE: European Network and Information Security agency (ENISA) http://www.enisa.europa.eu

VPN – Virtual Private Network
An arrangement whereby a secure, apparently private network is achieved using *encryption* over a public network, typically the internet.

SOURCE: Oxford Dictionaries, (2012), http://oxforddictionaries.com

Wholesale Payments

Payment transactions, usually of large value and high-priority, made by corporate and financial institutions. These can include the discharging of obligations both with respect to non-financial instruments and in relation to the transfer of securities and other financial instruments in other parts of the financial infrastructure.

SOURCE: Tripartite Authorities, (2008), Resilience Benchmarking Project Discussion Paper