ICT readiness for business continuity

Webinar 3 Information Sheet

Information and Communications Technology (ICT) Readiness for Business Continuity / Disaster Recovery

This webinar discussed the concept of business continuity and the role ICT can perform in ensuring readiness for dealing with disruptions. It outlined 4 key steps in business continuity planning - Prevent, Prepare, Respond and Recover. It demonstrated those steps and discussed relevant ISO standards.

Business continuity planning

Business continuity planning (BCP) is a process that organizations undertake to prepare for an unexpected event and build in organizational resilience - to ensure an effective response, minimised impact, and a faster recovery. A BCP should include arrangements for prevention, preparation, response, and recovery to build resilience in the face of disruption.

There are so many possibilities to think of in business continuity that it can be difficult to get a clear idea of how to plan for the potential disruptions and how to manage them. As with many large problems, its often best to break them down into bite-sized pieces. Think of what disruptions may occur and what would be their impacts. Consider what would be your objectives and requirements for recovery. Then, break the process down into parts. In the webinar, we use: **Prevent, Prepare, Restore and Recover**. Once the whole concept is broken down like that, it is easier to get your BCP started.

More about relevant ISO standards

For those that are looking to develop an Information Security Management System (ISMS) based on ISO 27001, the most relevant controls listed in that standard are Annex A 5.29 and 5.30. These are summarised below:

ISO 27001 Annex control A 5.29 Information security during disruption

There are many events that may disrupt normal business operations. They include:

- Natural disaster / adverse weather events
- War or military action
- Terrorist attack
- Criminal act

- Civil disturbance
- IT systems failure
- Cyber attack
- The unexpected loss of key workers
- Supply chain failure
- Infrastructure failure
- Pandemic

These are just some of the many possible examples. If such an event occurs, it can cause operational disruption. This control requires organisations to maintain information security at an appropriate level during such a disruption.

ISO 27001 Annex control A 5.30 ICT readiness for business continuity

Information and Communications Technology (ICT) is a key element of all modern organizations, and the readiness of ICT is an important element of broader business continuity management. This control requires an organisation to ensure that its ICT is ready, to ensure business continuity objectives and requirements are met.

ISO 27002 Information security controls

This standard provides guidance on each of the 93 controls listed in ISO 27001 Annex A – including the 2 listed above.

ISO 27031 - Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity

This standard expands on the control 5.30 in ISO 27001 and 27002. It provides guidance on the concepts and principles behind the role of ICT in ensuring business continuity. It suggests a structure or framework, identifies and specifies various aspects of an ISMS for improving ICT readiness for business continuity, and enables an organisation to measure its readiness in the face of disruption.

ISO 22301 - Security and resilience - Business continuity management systems

In the light of recent events, governments, regulators, and business clients will increasingly want to be confident of resilience in their supply chains. More and more, they will seek assurance that key suppliers have implemented an appropriate level of business continuity planning. That resilience may be achieved with a Business Continuity Management System (BCMS) and may be demonstrated by the BCMS being independently certified. Fortunately, there is an international certification standard that specifies requirements for a BCMS, and that standard is ISO 22301.

The most recent (2019) version of ISO 22301 is based on ISO's common high-level clause structure and terminology used in the current generation of ISO management system standards. These have also been applied to various other standards such as ISO 9001 (Quality), ISO 45001 (OH&S), ISO 14001 (Environment), and of course, ISO 27001 (Information Security).

Whilst individual standards add additional, discipline-specific requirements, there is clearly scope for business continuity to form part of an integrated management system (IMS).

Web Sites and resources		
ISO 22301:2019 web page	**https://www.iso.org/standard/75106.html**	ISO 22301:2019 Security and resilience — BCMS - includes an abstract and preview
ISO 27031:2011 web page	**ISO/IEC 27031:2011 - Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity**	Once again, this ISO web page includes an abstract and preview. Although quite old, this standard was reviewed and confirmed in 2020 and is therefore, still current.
Queensland Government Business Continuity Planning Template	**https://www.publications.qld.gov.au/dataset/business-continuity-planning-template/resource/63f7d2dc-0f40-4abb-b75f-7e6acfeae8f3**	Free template to download (263kB DOCX file)
Qudos model business continuity plan template	**https://qudos-software.com/CHDE/QudosModelBusinessContinuityPlan.docx**	Free template to download (65kB DOCX file)
Chubb cyber index	**https://chubbcyberindex.com/#/splash**	This Index provides real-time access to global data on current cyber threats and how you can protect your company against them.
ACSC Cyber Incident Response Plan – Guidance	**https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf**	Free to download (1.98MB PDF file)
ACSC Cyber Incident Response Readiness Checklist	**https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Readiness%20Checklist_A4.pdf**	Free template to download (1.18MB PDF file)
ACSC Cyber Incident Response Plan	**https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Cyber-Incident-Response-Plan-Template.docx**	Free template to download (1.52MB DOCX file)

Previous webinars and information sheets	**Industry support workshops | State Development, Infrastructure, Local Government and Planning** At the site, click the link for 'Learn about cyber security'.	The webinar recordings and information sheets are now live on the State Development website.
ACSC (Australian Cyber Security Centre)	**https://www.cyber.gov.au/**	Federal Government unit that provides cyber security guidance to individuals, businesses and organisations.
ACSC Small Business Cyber Security Guide	**Small Business Cyber Security Guide | Cyber.gov.au**	This guide includes basic security measures to help protect your business against common cyber security threats.
NIST Cyber security framework	**https://www.nist.gov/cyberframework**	NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce and is a well-respected source of information. This cyber security framework consists of standards, guidelines and best practices to manage cybersecurity risk.
Qudos Information Security blog articles	**https://qudos-software.com/qudos-blog-articles-about-iso-management-systems/**	Includes a series of blog articles on information security in plain English.
Main Presenter		
Alan M Jones	**jonesa@qudos-software.com**	