Information security in the use of cloud services

Webinar 2 Information Sheet

Information security in the use of cloud services

When your computer hardware and software are on-premise, it's up to your business to manage and update it as needed. As such, from an information security perspective, on-premise IT infrastructure presents a high level of responsibility.

Cloud computing allows for parts of that infrastructure to be outsourced remotely or 'ín the cloud'. While it offers many advantages, there are some information security risks that need to be considered and addressed.

Cloud computing services are often referred to by various ''as a service'' names:

- **IaaS (Infrastructure-as-a-service)**
- **PaaS (Platform-as-a-service)**
- **SaaS (Software-as-a-service)**

They are collectively known simply as cloud services.

In IaaS, the vendor provides you with storage and other data centre facilities. You access and control various elements of the infrastructure.

PaaS is primarily used by software developers and programmers.

SaaS is perhaps the mostly widely used cloud service. In this case, the vendor provides you with access to a complete software application that you use via your web browser.

In the webinar, the emphasis was on SaaS. It focused primarily on the four important elements of:

- **Acquisition of cloud services.**
- **Use of cloud services.**
- **Management of cloud services.**
- **Exit from cloud services.**

For those that are looking to develop an ISMS (Information Security Management System) based on ISO 27001, the most relevant control listed in that standard is Annex A 5.23. Appropriately also named **Information security in the use of cloud services**, it requires processes to be established for the life-cycle of cloud services – from acquisition through to exit from them. Although that is the most obvious reference, there are many other clauses and controls in ISO 27001 that also have relevance to the use of cloud services.

The 3rd webinar in the series is all about **ICT readiness for business continuity**. It is scheduled for **5 October 2023.**

Web Sites and resources		
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.
ACSC Publication 'Cloud Computing Security for Tenants'	**https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/cloud-security-guidance/cloud-computing-security-tenants**	A publication is designed to assist organisations to perform a risk assessment and use cloud services securely.
ACSC Publication	**https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/cloud-security-guidance/cloud-computing-security-considerations**	This publication provides an overview of cloud computing and associated benefits. Most importantly, this publication provides a list of thought provoking questions to help organisations understand the risks, and assist in their assessment.
ACSC Guide to email account security (Outlook)	**https://www.cyber.gov.au/acsc/view-all-content/guidance/how-check-your-email-account-security-outlook**	This step-by-step guide will explain how to check the security of your email account.
ACSC Essential Eight	**https://www.cyber.gov.au/acsc/view-all-content/essential-eight**	While no set of mitigation strategies are guaranteed to protect against all cyber threats, organisations are recommended to implement eight essential mitigation strategies from the ACSC's Strategies to Mitigate Cyber Security Incidents as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.

Queensland Government

Scamwatch	**https://www.scamwatch.gov.au/**	Scamwatch is run by the Australian Competition and Consumer Commission (ACCC). It provides information to consumers and small businesses about how to recognise, avoid and report scams.
Previous webinars	[Industry support workshops	State Development, Infrastructure, Local Government and Planning](#)	Web page with links to previous webinars delivered by Qudos on behalf of Queensland Government in late 2022. The webinars took a plain English approach to helping business to learn about information security, learn how to protect against cyberattacks, and then systemise their approach for maximum long-term benefit.
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.
Qudos article 'Information security in the use of cloud services'	**https://qudos-software.com/information-security-cloud-services/**	Developed to complement this webinar. Publication date: 25 August 2023.
Main Presenter		
Alan M Jones	Email **jonesa@qudos-software.com**	Main presenter: CEO, Qudos Management. Provider of information security management system software and consultancy services.

Queensland Government