WHITE PAPER

Assessing cloud vendors for data security

Frontier
software

www.frontiersoftware.com

The cloud phenomenon is here. An ever increasing number of organisations are moving their IT framework and data to a cloud solution. They are doing so to maximise the potential of such solutions, in terms of flexibility, agility, efficiencies and cost savings. The trend toward cloud adoption means that significant amounts of sensitive data already reside there and the volume will continue to increase.

Nefarious actors have identified data stored on the cloud as a potential source of income and cases of data compromise have already occurred. The breadth of data theft is enormous, but encompasses personally identifiable information; a trigger point requiring organisations to report data breaches.

This whitepaper seeks to offer organisations a framework around which to base their assessments of third-party vendors who offer a cloud solution. The whitepaper is a guide to enable IT and operations professionals to discuss and identify what is important to them when considering cloud solutions.

Data protection and security are always major concerns when an organisation is considering a cloud solution; especially when considering the sensitive HR and Payroll data held by employers.

When assessing hosted payroll and HR vendors, it's important to ensure they apply industry best practices to the treatment and protection of your organisation's data. Vendors must be able to demonstrate the steps they take to protect data from security threats, both internal and external.

An essential defence in any vendor's arsenal is an "International Organisation Standardization" (ISO) accreditation. Expect your vendor to have ISO 27001 accreditation, an international standard for data security. It shows the vendor has a serious commitment to managing information security, based on risks to the organisation's information assets.

Achievement of the accreditation requires significant work to be done by a vendor. The ongoing in-depth auditing processes required for ISO certification include a systematic examination of risks and vulnerabilities and a comprehensive plan of information security controls.

Besides ISO 27001, vendors should also hold ISO 9001 accreditation. ISO 9001 is a quality management standard that requires an organisation to meet its own requirements and those of regulators. The standard is based on a plan-do-check-act methodology which helps organisations deliver results that meet its requirements and deliver continuous improvements.

Another accreditation to consider is ISO 20000, the internationally acknowledged standard for high quality service management.

Combined, accreditations such as the ones above, ensure you are dealing with a vendor with high levels of security-driven processes and controls.

As a purchaser of hosted services, an organisation must seek a vendor with a proven, secured and security-driven operation comprising hardened facilities equipped with established technologies and support.

Alongside ISO accreditation, consider vendors who also offer ISAE/ASAE 3402 compliance. For organisations seeking a vendor, ISAE/ASAE 3402 offers peace of mind that service processes and procedures are to a world standard and are annually assessed.

Ascertaining accreditations is a first step toward vendor selection. Also required is a closer examination of the physical security of data held on your behalf. As a minimum, make sure your vendor can satisfy the following requirements:

- ✓ World-class data protection and encryption for sensitive workforce data;
- ✓ Built-in solution and database protection designed to prevent unauthorized access to information, including layers of redundancy, encryption, network and web firewalls, intrusion detection, and user authentication;
- ✓ Dedicated information security staff, possessing industry determined and evaluated skill sets in information security and related best practices;
- ✓ A proactive and regularly tested business continuity plan and protection strategy that provides fully redundant power subsystems, protection against fires, natural disasters, power outages, sabotage, theft and/or civil disruption;
- ✓ Frequent, (every few hours and/or daily) backups of customers' data sent to an alternate facility;
- ✓ Continuous, automatic monitoring for viruses to ensure privacy and data integrity;

- ✓ Live-state heartbeat infrastructure monitoring;
- ✓ Embedded Web Application Firewall (WAF) as a core feature to all implementations;
- ✓ A Security Operations Centre (SOC) and Security Information and Event Management (SIEM) to monitor and analyse potential threats in real time.

Vendors committed to data security should offer Sarbanes Oxley (SOC) SOC2/SOC3-level controls to extend and supplement their ASAE 3402 governance controls. This would enable them to ensure that their system and your data:

- Is protected against unauthorised access
- Is available for operation and use as agreed
- Is designated confidential and protected accordingly
- Provides only for access models which drive your business confidences
- Provides complete, accurate, timely access in adverse conditions
- Is governed by privacy principles that ensure personal data is collected, used, retained and/or destroyed in conformity with your privacy commitment.

The next thing to consider is the physical location of your data. Vendors may choose to host data in their own dedicated computer and data storage infrastructure. Others may opt to do the same, but use a data centre to maintain the quality and security of infrastructure. Others may opt for a combination and still others may opt to house your data offshore, with no stringent data sovereignty controls.

Vendors should also be able to demonstrate a commitment to external audits of data security arrangements. By regularly engaging industry-accepted experts to review and bolster its protection model, organisations also benefit from an evaluation of their current effectiveness and identification of opportunities to apply new and market-leading web application firewall capabilities.

Once accreditation, process, control, audit and physical security concerns have been addressed, you need to consider the vendor themselves as a possible source of breach. Consequently, a detailed review of data access controls needs to be undertaken so that you are clear about who can access your data and for what purpose. Vendors should be able to document and demonstrate an employee-wide commitment to data security, via training and education programs that are rolled out company-wide.

An organisation cannot be too careful when assessing the data security practices of a potential vendor. A company such as Frontier Software is regularly assessed by some of the largest Australian brands and is well-placed to satisfy even the most stringent security review. Offering all of the minimum and additional requirements discussed above, Frontier Software secures its clients' data via:

- Data backup and recovery using a tailored multi-point recovery model
- Rapid access data storage via de-duplexing technology
- Hourly, end of day, end of week, end of month archiving and recovery
- Compulsory restoration testing
- Flexibility in performing point-in-process or point-in-time back up requirement
- User validation, application-layer governed authorisation
- Network and web application firewalls
- Discrete environment availability and recovery
- Hardware redundancy
- Strong change management
- Geographically dispersed data hosting facilities
- Continuous monitoring of environment to ensure confidentiality, integrity and availability and safety.

When assessing your potential vendors, don't rest until you have confidence in their structures and methodologies because a breach could affect both business longevity and reputation – not to mention the potential threat to individuals.

If a vendor can show that they meet the requirements discussed above, you can feel much more confident about securing your data in the cloud. In a world where data collection, storage and its use will be governed by extremely strict policies such as The Privacy Act (1989) Australia and the General Data Protection Regulation (GDPR), it's not only a wise consideration, it's obligatory.

Cloud Vendor Selection Checklist

	Item	
1	ISO 27001 Information Security	☐
2	ISO 9001 Quality	☐
3	ISO 20000 IT Service Management	☐
4	ASAE 3402 Assurance Engagements	☐
5	Data protection and encryption	☐
6	Database	☐
	- Layers of redundancy	☐
	- Encryption	☐
	- Network and web firewalls	☐
	- Intrustion detection	☐
	- User authentication	☐
7	Dedicated information security staff with industry assessed skill sets	☐
8	Regularly tested business continuity plan	☐
9	Fully redundant power systems	☐
10	Fire protection	☐
11	Natural disaster protection	☐
12	Power outage protection	☐
13	Sabotage protection	☐
14	Theft or civil disruption protection	☐
15	Frequent off-site data backup	☐
16	Continuous automatic virus monitoring	☐
17	Livestate heartbeart infrastructure monitoring	☐
18	Embedded web application firewall	☐
19	Security Operations Centre (SOC)	☐
20	Security Information Event Management (SIEM) process.	☐
21	Regular external audits of data security.	☐
22	Geographic location of data centre	☐
23	Vendor has documented internal data access controls	☐
24	Vendor has internal data security training for all staff.	☐