softsource VBRIDGE
computing a better way

BESTPRACTICE
CERTIFICATION
ISO27001
INFORMATION SECURITY
MANAGEMENT SYSTEM

ISO27001 CERTIFICATION

Softsource vBridge are proud to have extended the vBridge ISO27001 certification (achieved in 2020) to now encompass the entire company.

ISO 27001 certification is an internationally recognised standard that ensures we comply with recommended processes, technologies and behaviors that decrease the likelihood of security breaches. It's the only auditable standard that deals with the overall management of information security and is widely regarded globally as the gold standard.

Ensuring high standards of security risk management are a core fundamental principle of the services delivered by Softsource vBridge. We are proud of our security posture and invest significant time, effort, and capital in ensuring that we deliver high standards of security for our clients – failures in security can be catastrophic for our clients and we take that responsibility very seriously.

Security Risk Management

Security Risk management is part of our DNA. The ISMS comprises good-practice risk management activities to proactively identify, assess, and respond to security risks. The process formalises risk management by tracking of risks, assigning responsibility to individuals for monitoring and managing risks (instead of leaving it to chance), and establishing a risk treatment plan for identified threats and vulnerabilities.

We have a formalised Risk Council that meets regularly to review all risks, mitigations, treatments and controls. Our Risk Council includes board members, executive leadership, and operational experts within our teams. Central to our Risk Management Framework is the continuous monitoring and communication of risk with appropriate business stakeholders.

Our Risk Treatment process follows a four-step, 'Plan', 'Do', 'Check', 'Act' cycle and includes, as a minimum, a 12 monthly review of all risks and mitigations with their respective owners.

Security risk conversations are active within and across the organisation and all team members know how to raise risks or newly identified potential issues.

What does our ISO27001 certification mean to you?

ASSURANCE

That your information is being handled and protected in a secure manner.

IMPROVED CONFIDENTIALITY

ISO 27001 requires strict controls on access to sensitive information, which can help prevent data breaches and unauthorised access.

ENHANCED AVAILABLITY

By implementing measures to ensure the availability of critical systems and information, ISO 27001 helps ensure that customers have access to the information they need when they need it.

ACCOUNTABILITY

As part of our ISO 27001 Certification, we are required to complete annual external surveillance each year along with a full external audit by an accredited ISO certification body. This again provides assurance that we are delivering to our ISMS and that we can demonstrate compliance with our policies.

PEAC E OF MIND

We complete a minimum of one penetration test per year against our platform. Working with security test experts our Information Security Manager defines the planned approach. Along with external attacks we also ensure that penetration testing occurs from within our security perimeter, with limited access credentials to, for example, identify internal weaknesses.

OUR PEOPLE

Our team are an essential and effective part of our security program and efforts. All team members complete NZ Ministry of Justice vetting as part of our employment process. Our teams are regularly trained in our ISMS and their roles within this, we complete major incident response exercises twice per year to ensure that everyone knows what to do should we find ourselves in this situation.

We maintain appropriate levels of certification across the team to have confidence in their capabilities and keep training up to date including weekly ongoing security training.

Platform Operations & Support

All services are delivered from quality New Zealand data centres that meet our security standards and certifications. All platform operations are completed via secure connections with no direct access to platform from corporate offices.

Platform has security baked into our designs with physical separation between management planes and customer tenancies along with security focussed network segmentation. We maintain backup "out of band" access to all core components ensuing continuity of service and ensure that we actively deprecate unsupported or known security risk protocols.

We ensure that all components are maintained at supported versions and actively monitor CVE lists to identify at risk components and make sure that we have up to date protections and patching in place.

Base security practices such as MFA are mandatory for our platform including for customer access to their own environments. We apply the principles of least privilege and have protocols in place around the use of elevated privileges.

We do not allow customers to host unprotected workloads on our platform.

We maintain detailed records and logs of system activity and analyse these to identify potential issues or threats.

BESTPRACTICE CERTIFICATION
ISO27001
INFORMATION SECURITY
MANAGEMENT SYSTEM

JAS-ANZ

BESTPRACTICE