

Why ISO 27001 Accreditation is Crucial When Selecting a Managed Service Provider - blueAPACHE

Canonical: <https://www.blueapache.com/blog/why-iso-27001-is-crucial>

Details:

2021

Cybersecurity breaches have become common place headlining our news; even the highest profile of brand names is not immune, most recently witnessed with the massive data breach involving 500 million Facebook users' personal information¹. The reality is your information security posture is only as strong as your weakest link. With remote working arrangements becoming the standard, hackers continue to find new and sophisticated ways in accessing vulnerabilities and causing major business disruption. The complex nature surrounding secure delivery of data and applications can be a minefield, and over the past 12 months many organisations have discovered the benefits of partnering with a Managed Services Provider (MSP). Selecting the right provider who follows a robust security program can be a critical commercial decision, after all, your MSP will have access to highly sensitive company data from intellectual property, to financials and employee information. It's imperative in today's landscape that your provider follows strict Information Security Management System (ISMS) governance to minimise your risk and ensure business continuity by pro-actively limiting the impact of a security breach. ISO 27001, formally known as ISO/IEC 27001:2013 ISMS is a gold standard for cybersecurity frameworks. It is vendor-neutral, technology agnostic, nonaligned with a specific industry sector, and therefore, provides an excellent framework for establishing, implementing, maintaining and continually improving information security program for any organisation. Why select an ISO 27001 accredited MSP? Partnership with ISO 27001 accredited MSP ensures that your information is stored and processed in a risk-managed environment using the best practices. When you choose an ISO 27001 accredited IT services provider as your MSP, you eliminate uncertainty about how your data is being stored and managed. ISO 27001 accreditation requires organisations to go through a rigorous external third-party audit of the entire security program followed by two yearly surveillance audits. To stay compliant, organisations must recertify every three years. When you partner with an MSP with the accreditation, you get a slew of advantages:

Confidentiality through protection from unauthorised access and disclosure.

Integrity by ensuring data has not been altered without approval.

Availability and prevention of disastrous events that can put your organisation data at risk.

Cybersecurity threats and online crimes are constantly evolving. The major benefit of working with an ISO 27001 certified MSP is that you are assured of an independently third party audited accreditation. At blueAPACHE, we are committed to information security; continually improving our security program to challenge the current and upcoming threats. Our security program goes beyond our ISO 27001 security certifications; we invest in security so that our clients have secure and efficient access to their systems wherever they are, all the time. This enables our clients to achieve success, be agile and dynamic and support their client communities. Continue reading: How cybercriminals are exploiting the COVID-19 crisis – what you need to know to strengthen your human firewall! We are a proud supporter of this week's Privacy Awareness Week (PAW), an annual online event run by the Office of the Australian Information Commissioner (OAIC) highlighting the importance of securing personal information. ¹Paul Haskell-Dowland, The Conversation, 2021 – Available at: <https://theconversation.com/facebook-data-breach-what-happened-and-why-its-hard-to-know-if-your-data-was-leaked-158417>

What is ISO 27001 and why is it considered a gold standard for cybersecurity?

ISO 27001, formally known as ISO/IEC 27001:2013 ISMS, is described on our blog as a gold standard for cybersecurity frameworks. It is vendor-neutral, technology agnostic, and not aligned with a specific industry sector, making it an excellent framework for establishing, implementing, maintaining, and continually improving an information security program for any organisation.

Why is selecting an ISO 27001 accredited Managed Service Provider important?

Selecting an ISO 27001 accredited MSP is important because your provider will have access to highly sensitive company data, from intellectual property to financials and employee information. Following strict Information Security Management System (ISMS) governance minimises risk and ensures business continuity by proactively limiting the impact of a security breach.

What advantages does partnering with an ISO 27001 accredited MSP provide?

Partnering with an ISO 27001 accredited MSP provides confidentiality (protection from unauthorised access and disclosure), integrity (ensuring data has not been altered without approval), and availability (prevention of disastrous events that can put organisation data at risk).

What does ISO 27001 accreditation require of an organisation to obtain and maintain it?

ISO 27001 accreditation requires organisations to go through a rigorous external third-party audit of the entire security program, followed by two yearly surveillance audits. To stay compliant, organisations must recertify every three years.

What real-world example does the blueAPACHE article give to illustrate cybersecurity risks?

The article cites the massive data breach involving 500 million Facebook users' personal information as an example that even the highest-profile brand names are not immune to cybersecurity breaches, referencing Paul Haskell-Dowland's 2021 article in The Conversation.

How has remote working affected the cybersecurity landscape ?

with remote working arrangements becoming the standard, hackers continue to find new and sophisticated ways of accessing vulnerabilities and causing major business disruption, making the secure delivery of data and applications a complex challenge.

What is your commitment to information security beyond ISO 27001 certification?

We state it is committed to information security by continually improving its security program to challenge current and upcoming threats. The company says its security program goes beyond its ISO 27001 security certifications, investing in security so clients have secure and efficient access to their systems wherever they are, at all times, enabling clients to achieve success and be agile and dynamic.