Chapter 1 : Microsoft obtains new cloud-centric ISO certification | Blog | Microsoft Azure

Cloud service customer. Cloud service provider. The cloud service customer should agree with the cloud service provider on an appropriate allocation of information security roles and responsibilities, and confirm that it can fulfil its allocated roles and responsibilities.

Self-assessments are performed annually or when significant changes to the control environment occur. Who is the primary audience? Customers and relevant third parties with a business need. Annually or when significant changes to the privacy policies and practices occur. In order to bridge differences in approach and provide a streamlined means for U. This requires annual self-certification under the program. EU Model Contract Clauses are also offered to all customers who want to have that in place as well. Privacy Shield Framework established a program to provide companies on both sides of the Atlantic with a mechanism to comply with EU and Swiss data protection requirements when transferring personal data from the European Union or Switzerland, respectively, to the United States in support of transatlantic commerce. Registrants agree to certain requirements meant to safeguard this data. An independent third party annually assesses our Privacy Notice and Privacy Program to verify alignment with the framework requirements. A self-certification is also submitted to the program for evaluation of our alignment with the requirements as well. Privacy Shield Program Who is the primary audience? Customers controlling European or Swiss citizen data outside of the European Economic Area or Switzerland, respectively, and other interested regulatory third parties. We are also providing resources and documentation to support our customers in their roles as data controllers. At OneLogin, ensuring that all customer data is handled securely and responsibly is our number one priority. Here is an overview of what to expect from GDPR, how we are complying with this new regulation, and how we are empowering customers to comply. What is the purpose of GDPR? GDPR is a comprehensive data protection law that serves two purposes: GDPR gives control over personal data back to the EU residents and prohibits organizations from exploiting that data. GDPR makes data protection law identical throughout the single market. It provides businesses with simpler legal guidelines, which can be more easily enforced by government bodies. Who does GDPR apply to? GDPR applies to any organization operating within the EU, as well as organizations that offer goods or services to customers or businesses in the EU. This broadens the scope of protection of EU residents for improved privacy control. How will GDPR affect me? If you are a resident of the EU, congratulations! The European Union is taking steps to ensure that your data is used safely and appropriately. This will impact the way that you store, process, and utilize user data in a number of ways. Right to access and portability: Users can request confirmation as to whether their personal data is being processed, where and for what purpose. Further, the data controller is required to provide a copy of the personal data, free of charge, in an electronic format. Companies must take into account data privacy during design stages of all projects along with the lifecycle of the relevant data process. Companies must also take into account data privacy during design stages of all projects along with the lifecycle of the relevant data process. Right to be forgotten: Companies must allow users to erase their personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. This is not an exhaustive list. OneLogin is a global organization that both processes and controls data from around the world, including the EU. Our existing certifications and long-standing commitment to privacy frameworks prepare us for GDPR in many ways. To meet GDPR requirements, organizations are required to articulate data flows, and demonstrate how privacy is controlled and maintained. Organizations are also required to update their contractual language to reflect the additional accountability required by GDPR. To this end, OneLogin leverages data breach notification language, uses subcontractors, and communicates responsibilities to our own data processing vendors. How is OneLogin helping customers to be compliant? Right to access and portability IT administrators can easily find a user in the system and print out their information as stored in any of the user directories. Right to be forgotten OneLogin allows for the automated deprovisioning of users from other systems and external applications. Admins can delete users immediately to meet both privacy and enterprise security requirements. Admins can also manually audit provisioned apps. OneLogin is a trusted partner Privacy by design is a particularly challenging requirement, but as a vendor we are well-prepared for it. The OneLogin service has always handled information that must be protected; whether due to privacy regulations, credit card industry regulation, its designation as shared secrets, or several other data protection requirements. OneLogin incorporates privacy impact assessments that are performed periodically and as part of the design process for new features. Many of the compliance challenges are the result of older architectures that allow for limited control over how data is stored, managed, and processed. For example, it used to be very common for legacy applications to access the corporate directory directly. This meant they typically had access to all user information with few restrictions on what they modify, cache or store. We have come a long way since. These modern protocols use secure tokens, security assertions and automated provisioning. The user never signs-in to an app directly. Any trusted app can receive a secure token that represents the user. When a user is granted access to an application, their relevant metadata is pushed to the app. Applications do not authenticate users directly, which means better security and privacy. You can learn more about how we are embracing GDPR by reviewing our privacy policy. If you have questions or need more information please email privacy onelogin. These clauses are part of our Data Processing Addendum and offer an alternative means of fulfilling adequacy requirements, and therefore are an alternative to the US Privacy Shield Framework or Binding Corporate Rules. Provide a mechanism for customers in the EEA, who are considered the data controllers, to work with OneLogin, the data processor, and mutually agreeing to the transfer personal data outside of the EEA only under the proper safeguards and in compliance with EU data protection law. EU model contract clauses are executed like any other contract and are agreed to by both OneLogin and a given customer. Penetration Tests Application penetration tests are performed by independent third parties on a quarterly basis and by OneLogin on a weekly basis. Testers are granted access to their own OneLogin account and the underlying source code and we alternate the vendors that we use. We perform ad hoc pen tests, as needed, when rolling out significant features or functionality that might not be covered by the periodic tests. The core app is covered during every assessment and additional services including mobile apps and browser extensions are focus areas on a rotational basis. Third party penetration tests are performed on a quarterly basis and internal penetration tests are performed weekly. These scans are performed internally and externally as part of PCI requirements. Monitoring tools are also used to verify whether OneLogin systems are susceptible to emerging vulnerabilities by scanning the software packages installed on each system. Network vulnerability scans help OneLogin identify vulnerabilities and misconfigurations of websites, applications, and information technology infrastructures. Internal and external scans of the network environment. Network scans are performed on a quarterly basis and monitoring tools report ad hoc on emerging vulnerabilities. OneLogin - internal use only Bug Bounty Program Bug bounty programs provide another vehicle for organizations to discover vulnerabilities in their systems by tapping into a large network of global security researchers that are incentivized to responsibly disclose security bugs via a reward system. Operationally, the end results are very similar to a vendor-performed penetration test, but the number of researchers searching for bugs is much higher and not timeboxed, unlike a typical penetration test exercise. Researchers can apply to join our program via Bugcrowd or submit discovered bugs via our responsible disclosure form. All OneLogin properties, including the core SaaS service, browser extensions, and www sites.

Chapter 2 : ISO/IEC cloud privacy

ISO/IEC Preview Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC for cloud services ISO/IEC gives guidelines for information security controls applicable to the provision and use of cloud services by providing.

Dec 2, ISO Truth be told, ISO crept up on me. ISO is itself a fairly easy standard to understand. It outlines the controls a public cloud provider should take to properly secure their systems. The expectation would be that all cloud providers beyond Amazon Web Services such as Microsoft Azure, Google Cloud, Rackspace, etc would certify to the same standards. Before we can untangle the web, here is a quick primer on the basic ISO standards that related to Information Security: ISO is the code of practice for information security controls describing good practice information security control objectives and controls. ISO covers information security management measurement. ISO covers information security risk management. ISO is a guide to the certification or registration process for accredited ISMS certification or registration bodies. ISO provides guidance on information security management for inter-sector and inter-organisational communications. ISO is the information security management guideline for telecommunications organizations. ISO offers guidance on the governance of information security. ISO provides information security management guidelines for financial services. ISO covers the economics of information security management. ISO covers information security controls for cloud computing. They actually keep going up to but I stopped here for this exercise. Most people are familiar with ISO and but in the last few years, there are been a lot of additions to the ISO standards. ISO provides the controls needed for a well functioning ISMS â€” or they are the implementation guidelines for building out the program. When someone says they are or are getting ISO certified, most of the guidance and requirements to get certified are contained in ISO ISO and build on ISO in providing specific guidance on implementing under specific conditions. The standard is specifically for the Amazons and Googles but you should understand the controls they are expected to implement. While Amazon was first out of the gate with the ISO certification, I would expect the other major players to certify at least some parts of their environment in the near future. Finally, I would look at all of the standards. There is a wealth of information in each standard that may help you both in your career and at your current job. The standards are specifically generic â€” they have to work universally for almost anyone â€” so your millage may vary.

Chapter 3 : ISO/IEC Compliance - Amazon Web Services (AWS)

ISO generally focuses on the protection of the information in the cloud services, while ISO focuses on protecting the personal data, as I described in my article ISO vs. ISO - Standard for protecting privacy in the cloud.

Chapter 4 : ISO vs. ISO â€“ Security controls for cloud services

iso Controlling cloud-based information security. The International Organization for Standardization (ISO) is an independent, non-governmental international organization with a membership of national standards bodies.

Chapter 5 : ISO vs. ISO - What's the difference?

ISO/IEC Extending ISO/IEC into the Cloud. A Whitepaper. 3 Cloud customers are concerned about securityâ€"it remains a key reason why.

Chapter 6 : Using ISO to Conform to ISO and ISO

ISO/IEC is a unique technology standard in that it provides requirements for the customer as well as the cloud service provider. IT Managers and other technical staff responsible for moving organizations to the cloud or expanding a cloud *service engagement can reduce risks to their business by ensuring they understand their.*

Chapter 7 : Microsoft Trust Center | ISO/IEC Code of Practice for Information Security Controls

Information technology? Security techniques? Code of practice for information security controls based on ISO/IEC for cloud services.

Chapter 8 : Strengthening the Cloud: ISO and ISO - A-LIGN

ISO-IEC Overview. The ISO/IEC code of practice is designed for organizations to use as a reference for selecting cloud services information security controls when implementing a cloud computing information security management system based on ISO/IEC

Chapter 9 : ISO/IEC cloud security

We are happy to announce Microsoft Azure obtained the ISO/IEC certification, an international standard that aligns with and complements the ISO/IEC with an emphasis on cloud-specific threats and risks.