FERPA Implementation Guide

Microsoft Azure

Disclaimer

Published August 2016

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. Customers reading this document bear the risk of using it.

The information contained in this document must not be construed as legal advice. Customers should seek their own legal counsel for advice on compliance with regulatory requirements impacting their organization.

This document does not provide customers with any legal rights to any intellectual property in any Microsoft product. Customers may copy and use this document for their internal, reference purposes.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

NOTE: Certain recommendations in this paper may result in increased data, network, or compute resource usage, and may increase a customer's license or subscription costs.

Acknowledgements

Authors

Frank Simorjay
Jim Andersen (Cadence Preferred)

Contributors and Reviewers

Jeff Gallucci
Dan Ryan
Tom Shinder

Executive Summary

Educational organizations are continually under pressure to use scarce resources as efficiently as possible. They must provide innovation in instruction, tailor curriculums to diverse learner communities, respond to constituent demands and cooperate with law enforcement as the need arises. Advances in IT have enabled educational institutions to respond with more agility, while maintaining compliance with privacy and security regulations such as the Family Educational Rights and Privacy Act, (FERPA). As a leading cloud provider, Microsoft is vitally invested in helping ensure that educational organizations understand the shared responsibilities that exist between its educational customers and the Microsoft Cloud.

Deploying Microsoft Azure solutions can give educational organizations a method of focusing on their core business—education—while maintaining cost-effective IT services in a more secure FERPA-compliant environment. However, it is important for educational organizations to understand their unique threat environment so that they can see what they need to deploy onsite and how it meshes with what Microsoft Azure provides in the cloud. Using the shared responsibility strategy, Microsoft can help assure the protection of student data and FERPA compliance.

This paper will be most helpful to those in educational organizations who need guidance and best practices in designing secure solutions on Azure.

This whitepaper is intended for:

- School officials with legitimate educational interest
- School officials designated to assist with the onboarding of student transfers
- School officials responsible for FERPA audits or evaluations
- Appropriate parties in connection with financial aid to a student
- Organizations conducting certain studies on behalf of a school
- Accrediting organizations
- Appropriate emergency health and safety officials
- School officials responsible for complying with judicial orders or lawfully issued subpoenas
- State and local law enforcement officials within a juvenile justice system pursuant to specific state law

For additional information and security guidance, please refer to:

- Security, privacy, and compliance resources on the Microsoft Trust Center
- Microsoft cloud services and network security article for information on Network Security
- Azure documentation center for service documentation
- Azure security information hub for Azure security technical information

Contents

Introduction

Educational organizations considering a move to Azure are looking for guidance in designing and operating solutions that incorporate security controls to help them meet their compliance challenges.

Azure provides services that can help meet the security, privacy, and compliance needs of Microsoft customers. In addition, Microsoft works with customers to help them understand their responsibilities to protect their data and environment infrastructure after their service has been provisioned.

This document helps customers understand how they can improve the security of their solution service simply and effectively. In addition, each customer should have their own compliance mechanisms, policies, and procedures in place to ensure they do not use Azure in a way that violates any regulatory requirements. Users of Azure should independently verify with their own legal counsel that their implementation meets all local compliance regulatory requirements.

This paper provides insight into how Microsoft meets its compliance obligations on the platform and presents best practices and security principles that are aligned to the Family Educational Rights and Privacy Act, International Organization for Standardization (ISO) 27001, Microsoft's Security Development Lifecycle (SDL), and operational security for online security.

The content is divided into two major sections:

1. **Considerations and guidance** for using cloud technology including risk management, shared responsibility, establishing an information security management system, and establishing standard operating procedures.

   Primary Audience: Chief Information Security Officers (CISO), educational risk managers, school officials with legitimate educational interest, school officials responsible for FERPA compliance, and accrediting organizations

   Secondary Audience: Appropriate financial aid parties, appropriate emergency health and safety officials, officials whose role it is to comply with judicial orders or subpoenas, state and local juvenile justice officials, solution architects and developers.

2. **Key security principles** that are both aligned to a standard information security management standard, such as FERPA or ISO 27001, and standard development processes, such as Microsoft's Security Development Lifecycle.

   Primary Audience: School officials with legitimate educational interest, school officials responsible for FERPA compliance, accrediting organizations, solution architects, developers, and operations personnel

   Secondary Audience: Appropriate financial aid parties, appropriate emergency health and safety officials, officials whose role it is to comply with judicial orders or subpoenas, state and local juvenile justice officials, CISOs, and educational risk managers.

Compliance and security methodology

This guidance is rooted in well-established standards such as those from ISO, the National Institute of Standards and Technology (NIST), and FERPA as a foundation for establishing an information security management system (ISMS). After such a system is set up and the key ISMS best practices are established, ISMS development should focus on three key areas:

- Education industry compliance considerations
- Adopting secure development processes
- Establishing secure operations principles

The intention is to help ensure that standard security development and operations best practices are incorporated from the beginning of a cloud project, and key activities are communicated more effectively with all stakeholders in the context appropriate for their roles. These roles include compliance officers, legal advisors, risk managers, solution architects, developers, and operations personnel.

Best practices and recommendations will be presented in the subsequent sections. The following list specifies the sections and their alignment to the standards ISO, NIST, and FERPA:

Foundation

- Establishing an ISMS | Aligned to ISO 27001
- Establishing standard operating procedures that align to the ISMS | Aligned to ISO 27001

Compliance considerations

- Compliance regulations such as FERPA with clearly defined physical, technical, and administrative safeguards | Aligned to ISO 27001

Tools for solution design

- Adopt data governance practices | Aligned to ISO 27001 or FERPA
- Security Development Lifecycle | Aligned to ISO 27001
- Operational security for operational security | Aligned to ISO 27001 and NIST
- 13 key security principles for designing and securing solutions for Azure | Aligned to ISO 27001

Aligning using ISO

Initially, organizations should consider adopting an information security management system. One example is ISO 27001, an auditable, international, information security management standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that formally defines requirements for a complete ISMS to help protect and secure an organization's data. ISO 27001 details a set of best practices and is intended to be applicable to all organizations, regardless of their type or size.

For organizations that deal with sensitive information, the ratified ISO 27018, an extension of the ISO 27001 standard, governs the processing of personally identifiable information (PII) by cloud service

providers acting as Personally Identifiable Information (PII) processors. ISO 27018 details controls that address protecting PII in public cloud services. Azure was the first global cloud service to adopt ISO 27018, which provides an additional set of controls for an organization to consider when adopting an ISMS.

ISO 27002 is a complementary collection of 114 controls and best practice guidelines designed to meet the requirements detailed within ISO 27001. The controls are organized into 14 groups, and when properly implemented can help an organization achieve and maintain information security compliance by addressing specific issues that are identified during formal, periodic risk assessments. The 14 groups are listed here:

- Information security policies
- Operations security
- Organization of information security
- Communications security
- Human resource security
- System acquisition
- Asset management
- Development and maintenance
- Access control
- Supplier relationships
- Cryptography
- Information security incident management
- Physical and environmental security
- Information security aspects of business continuity management

Establishing an ISMS is a very deep and broad topic with complex challenges, and many resources are available to assist organizations in this endeavor. Educational organizations should consider conducting a risk assessment and aligning risk management and mitigation to that assessment. A second area of focus that should be considered is establishing standard operating procedures for each of the 14 ISO groups in order to establish core principles for the entire organization to follow.

Risk management

One of the best practices defined in ISO 27001 covers risk assessment and risk management. Organizations, especially those in regulated industries, are advised to undertake an assessment and establish a risk management program.

There are no shortages of risk management approaches, and organizations can adopt one that is appropriate for their needs. One approach could involve ISO 31000, which focuses specifically on risk management. In the Education industry, the FERPA statute requires a risk assessment and recommends the NIST Special Publication 800-30. Another approach could involve a portion of the NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. Within it, a risk management framework is presented with specific activities. For a specific industry and locale, there may be a standard approach that is well-suited to assess and mitigate risks. Understanding risks is key to helping organizations choose the right controls.

Standard operating procedures (SOP)

Organizations should consider establishing SOPs around critical areas of their ISMS. One way is to establish SOPs that align to each ISO group, and identifying an accountable owner who will maintain and operate within the organization. The following examples are presented with some guidelines:

Privacy

Independent software vendors (ISV), especially those developing and deploying Software as a Service (SaaS) solutions for their customers, will have to consider the implication of handling data on behalf of their customers. ISVs should consider providing a formal privacy statement that aligns with their internal processes and practices. Details about Azure privacy commitments can be found in the Microsoft Online Services Privacy Statement.

Incident response management

An important standard operating procedure that all organizations should implement is an organizational incident response plan. When creating an incident response plan, customers should consider the following five areas:

- **Detect**. Assemble a core team of experts who will respond to incidents. This team must undergo response training in order to act quickly and effectively when a security incident occurs.
- **Assess**. An initial assessment, communication containment methods, and notification policies must be included in the plan. This information must be kept current, and the core team must be trained on the plan in its latest iteration so that policies and procedures are followed quickly, accurately and efficiently**.**
- **Diagnose**. The response plan should incorporate standard procedures used to diagnose the cause of the incident to the extent that it allows the incident response team to understand root cause and initiate actions to remediate the issue in the affected parts of the system**.**
- **Stabilize and recover.** After initial root cause is remediated, and trouble-shooting procedures allow system stability, the plan should include standard operating procedures for bringing the system into a working state, if not full recovery. This step often includes recommendations for additional monitoring and penetration testing to validate mitigation efficacy.
- **Close and post mortem**. After resolution of the security incident, the response team should evaluate the event and record lessons learned during the incident response process. Policies should be updated as appropriate. The response plan should include post mortem standard operating procedures to ascertain the root cause of the incident and document the most effective trouble-shooting steps taken to mitigate the issue.

For more detailed information about an incident response plan, see Microsoft Azure Security Response in the Cloud.

When establishing a standard ISMS within an organization, the need to align to and adopt well-known and refined standard practices cannot be overemphasized.

ISO27001, 27002, and 27018 are standard practices to help protect IT environments from threats. These standards can help to design a robust secure environment and move it toward a state of compliance for demonstration to regulators. Meeting these obligations will help achieve a high quality bar for the education industry. This process is well defined and provides a set of basic guidelines that can be followed for successful adoption of Azure-based solutions.

Incorporating regulation considerations in Education

Education regulations differ between countries and regions, and sometimes even between states. An understanding of these regulations requires careful legal analysis to determine and establish which controls are necessary to demonstrate compliance with local laws.

From a platform perspective, Azure meets a broad set of international and industry-specific compliance standards and regulations applicable to cloud service providers, such as ISO 27001, FERPA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards including Australia IRAP, UK G-Cloud, and Singapore MTCS. Details of all compliance programs can be found on the Microsoft Trust Center.

The ISO 27001 audit scope includes controls that address FERPA security practices as recommended by the US Department of Education and the EU Data Protection Directive. This is a key reason why ISO 27001 is the basis for the guidance in this paper.

A few more details about these two regulations are provided in the following paragraphs:

FERPA

The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student educational records. The law applies to all schools that receive funds under an applicable program of the US Department of Education.

FERPA gives parents certain rights with respect to their children's educational records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are termed eligible students.

Parents or eligible students have the right to inspect and review the student's educational records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records locally.

Parents or eligible students have the right to request that a school correct records they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's educational record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

- School officials with legitimate educational interest
- Other schools to which a student is transferring
- Specified officials for audit or evaluation purposes
- Appropriate parties in connection with financial aid to a student
- Organizations conducting certain studies for or on behalf of the school
- Accrediting organizations
- To comply with a judicial order or lawfully issued subpoena
- Appropriate officials in cases of health and safety emergencies

- State and local authorities, within a juvenile justice system, pursuant to specific state law.

Schools may disclose, without consent, directory information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual method of notification (e.g., special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

European Union (EU) Data Protection Directive

FERPA is primarily a United States standard for education; its protections have broad applicability as well. Although the EU Data Protection Directive 95/46/EC is not education-specific, it is a comprehensive privacy standard for processing personal data from member states in the EU. Article 8 of the EU Data Protection Directive 95/46/EC makes provisions for "the processing of special categories of data" including personal data concerning education. Each member state may choose to add additional controls based on this provision for sensitive education data. Some member states have not added any controls specific to education, thus making cloud adoption with EU Model Clauses possible without additional regulatory barriers in those member countries.

The EU Model Clauses are standardized contractual clauses used in agreements between service providers (such as Microsoft when it offers Azure services under the EU Model Clauses) and their customers to ensure, in a standardized way, that the appropriate safeguards are in place to protect personal data that leaves the European Economic Area (EEA).

Compliance with EU data protection laws also means that on a practical level customers need fewer approvals from individual data protection authorities to transfer personal data outside of the EU. The reason for this is because most EU member states do not require an additional prior authorization from the local data protection authority if the transfer is based on an agreement that complies with the EU Model Clauses.

Due to its strong contractual commitments to comply with EU data protection laws regarding the international transfer of data, Microsoft was the first company to receive a letter of endorsement and joint approval from the EU's Article 29 Working Party, which includes data protection authorities from each of the EU member states. Azure agreements include the EU Model Clauses that provide customers additional guarantees around transfers of personal data for the Azure services that are in scope. This inclusion ensures that customers can use Microsoft cloud services to move data freely through the Microsoft cloud from Europe to the rest of the world.

When considering cloud services, it is noteworthy to mention that services are not automatically covered by the contractual agreements upon general availability. New services must achieve the ISO 27001 certification first, and may then be added to an in-scope service list. These services are independently

audited once a year for ISO 27001/27002 and 27018 compliance by Microsoft's ISO accredited auditor. The current compliance certificate may be found on the Microsoft Trust Center.

On Azure, both of these contractual agreements are incorporated in the Online Services Terms (OST); execution of the volume licensing agreement includes execution of EU Model Clauses and, for applicable customers, the Business Associate Agreement (BAA), unless the customer opts out.

Considerations and tools for success

After an ISMS foundation is set and best practices are adopted, additional areas need to be evaluated and understood to determine an organization's risk posture and keys for mitigating its' risks.

The first area is understanding the principles of shared responsibilities for meeting compliance, where customers and the cloud provider have distinct responsibilities in meeting compliance end-to-end. Educational organizations need to understand what service models are being used in the design and then determine what controls need to be in place to meet their compliance needs. Educational organizations also need to understand which areas the cloud provider is responsible for with regard to meeting compliance obligations, and which areas are the responsibility of the user or educational organization.

Another consideration is establishing governance practices that include classifying data and protecting it based on different levels of data sensitivities. Not all data should be made available to all users within a customer cloud account. Data governance practices and policies should be created to ensure that only those users with appropriate access permission can view data specific to their level of permission.

Incorporating both these considerations in a solution design will help present a clear picture of how to mitigate for risks and design with compliance in mind.

Shared responsibilities

The widely understood cloud service models as defined in the NIST Definition of Cloud Computing, Special Publication 800-145 are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The service model a customer chooses also dictates the responsibilities of managing their cloud environment. A critical distinction between what NIST defines and what Microsoft Azure, Office 365 and Dynamics CRM Online offer is illustrated in the shared responsibility matrix below.

The following diagram shows the split in service responsibilities by key areas and is critical for all customers to understand, but especially those in regulated industries as they assess and mitigate risks.

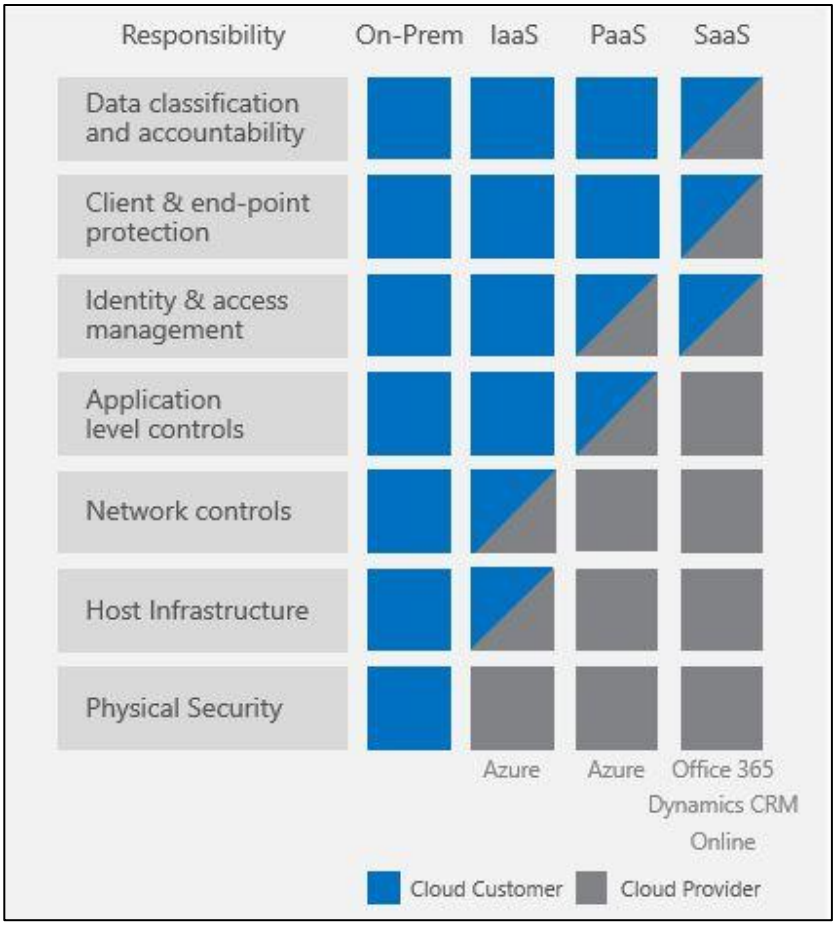

Figure 1 – Shared Responsibility Matrix

- The customer is completely responsible for all aspects of operations when solutions are deployed on-premises.
- With Infrastructure as a Service (IaaS), the lower levels of the stack, physical hosts or servers, and host security are managed by the platform vendor. The customer is still responsible for securing and managing the operating system, network configuration, applications, identity, clients, and data. For the developer, an obvious benefit with IaaS is that it reduces the developer requirement in configuring physical computers.
- With Platform as a Service (PaaS), everything from network connectivity through the runtime or identity service may be provided and managed by the platform vendor. PaaS offerings further reduce the developer burden by additionally supporting the platform runtime and related application services. With PaaS, the developer can almost immediately begin creating the business logic for an application.
- With Software as a Service (SaaS), a vendor provides the application and abstracts customers from all of the underlying components. Nonetheless, the customer continues to be responsible to ensure that data is classified correctly, that security-related controls provided to the customer are configured correctly, and that user devices are secured and protected when connected to the service.

Applying data governance practices

An educational organization acting as the service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.

Regardless of any technical controls deployed by the cloud supplier, controls will be fundamentally undermined if operating outside an effective risk management and governance program. When purchasing a cloud service, ensure that the supplier has a suitable security governance framework in place that will permit the service provider to direct their overall approach to the management of the service and information within it. A governance framework will ensure that procedure, personnel, physical, and technical controls remain effective through the lifetime of the service, in response to changes in the service, and changes in threat and technology developments.

The Azure FERPA Compliance Framework workbook (Azure FERPA Compliance Framework Mapping.xlsx) found on the Service Trust Portal, includes a standard methodology for defining compliance domains, determining which objectives apply to a given team or asset, and capturing how domain control objectives are addressed in sufficient detail as they apply to a given set of industry standards, regulations or business requirements.

The workbook helps align controls to FERPA, and provides alignment to other control frameworks to better understand the role of the FERPA controls. This helps educators to design and build services using a common set of industry accepted controls, streamlining compliance across a range of regulation issues faced by education institutions.

Service Trust Portal

Customers with either an existing subscription or a trial subscription to Microsoft Azure products can use the resources available at the Microsoft Service Trust Portal (STP). The STP offers access to a deep set of security, privacy, and compliance resources, such as independent audit reports of Microsoft cloud services, risk assessments, security best practices, and other similar materials.

Each educational organization with a cloud subscription has a tenant for Azure, Office 365 and/or Dynamics CRM Online. The tenant Global Administrator provides user access to compliance personnel.

Customers with an active subscription to the Microsoft Azure, Office 365, and Dynamics CRM Online or have an Azure Active Directory account can access the STP directly. Customers will be asked to provide their credentials. Access credentials are managed through the cloud Global Administrator.

Visit the Service Trust Portal for specific details on accessing the Portal.

New customers or customers wanting to create a trial evaluation account, click either:

- Sign up for Office 365
- Sign up for Dynamics CRM Online

Or,

- Sign up for, purchase, upgrade or activate Azure

Complete the form and follow the additional steps to confirm the registration. More information can be found on the Get Started with the Service Trust Portal support page.

Microsoft compliance processes also make it easier for customers to achieve compliance across multiple services and meet their changing needs efficiently. Together, security-enhanced technology and effective compliance processes enable Microsoft to maintain and expand a rich set of third-party certifications. These help customers demonstrate compliance readiness to their customers, auditors, and regulators. As part of its commitment to transparency, Microsoft shares third-party verification results with its customers who have successfully completed the process to obtain these NDA resources on the Service Trust Portal.

Comprehensive, independently-verified compliance. Azure is designed with a compliance strategy that helps customers address business objectives and industry standards and regulations. The security compliance framework includes test and audit phases, security analytics, risk management best practices, and security benchmark analysis to achieve certificates and attestations. Microsoft Azure offers the following certifications for all in-scope services.

- **International Organization for Standardization (ISO) 27001 and 27018** audit reports and scope statements.
- **Federal Risk and Authorization Management Program (FedRAMP) System Security Plan.**
- **CSA CCM**. The Cloud Security Alliance (CSA) is a non-profit, member-driven organization with a mission to promote the use of best practices for providing security assurance within the cloud. The CSA Cloud Controls Matrix (CCM) provides detailed information about how Azure fulfils the security, privacy, compliance, and risk management requirements defined in the CCM version 3.01, and is published in the CSA's Security Trust and Assurance Registry (STAR).
- **EU Model Clauses**. Microsoft offers customers EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU. Microsoft is the first company to receive joint approval from the EU's Article 29 Working Party that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. This ensures that Azure customers can use Microsoft services to move data freely through our cloud from Europe to the rest of the world.
- **ISO/IEC 27018**. Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.
- **ISO/IEC 27001/27002:2013**. Azure complies with this standard, which defines the security controls required of an information security management system.
- **PCI DSS**. Azure is Level 1 compliant with Payment Card Industry (PCI) Data Security Standards (DSS) version 3.0, the global certification standard for organizations that accept most payments cards, as well store, process, or transmit cardholder data.
- **SOC 1 and SOC 2**. Azure has been audited against the Service Organization Control (SOC) reporting framework for both SOC 1 Type 2 and SOC 2 Type 2. Both reports are available to customers to meet a wide range of US and international auditing requirements. The SOC 1 Type 2 audit report attests to the design and operating effectiveness of Azure controls. The SOC 2 Type 2

audit included a further examination of Azure controls related to security, availability, and confidentiality. Azure is audited annually to ensure that security controls are maintained.

Audit Information

Microsoft Cloud Trust Center

The FERPA page in the Compliance section of the Microsoft Trust Center is the starting point for understanding the roles that Microsoft and educational organizations play in ensuring the use of Microsoft Azure products is compliant with FERPA. Customers are encouraged to read the information on the FERPA page in the Microsoft Trust Center and visit the associated links to get a better understanding of Microsoft's commitment to FERPA compliance and their role in auditing their own cloud solution.

Key principles and recommendations for secure development and operations

These controls are arranged to indicate the order of their importance to educational customers. More detail and specific recommendations can be found in The Microsoft whitepaper: 13 Effective Security Controls for ISO 27001 Compliance.

As outlined in shared responsibilities, some services elements, and recommendations only apply to a service model. To help simplify the discussion, services will be explored from the highest order service, or PaaS, moving down to IaaS service elements.

Platform service recommendations (PaaS)

Customers who purchase Azure as their cloud platform (PaaS) to host their data should consider the following controls:

1. **Encrypt all customer data**

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the message or information is encrypted using an encryption algorithm, which generates cipher text that can only be read if decrypted. An encryption scheme usually uses an encryption key generated by an algorithm. BitLocker encryption can be used to protect data at rest, and Transport Layer Security (TLS) can be used to protect data in transit.

Azure offers rich security functionality, including deep support for standardized encryption protocols. Developers can use the cryptographic service providers (CSPs) built into the Microsoft .NET Framework to access Advanced Encryption Standard (AES) algorithms, along with Secure Hash Algorithm (SHA-2) functionality to handle such tasks as validating digital signatures. Moreover, the Azure platform builds on the straightforward key management methods incorporated into the .NET security model, so developers can retain custom encryption keys within the Azure storage services.

2. **Enable identity, authentication solutions and access control**

Identity and authentication are essential to implement SDL effectively and securely. The implementation of these capabilities is important for identifying unique users of a service because they help ensure that only the right person accesses the service. The correct implementation will help ensure that the user who is logging in is actually the user that was assigned access rights. Identity and authentication are the first line of security defense at the organizational level and have the potential to be the weakest link in the security chain because they are the primary control that opens the 'door' to access management on which many aspects of security rely.

Identity management remains a priority, even as business networks change. Identity management is as much about preventing unauthorized access to data as it is about controlling the authorized use of data. Identity management helps systems control the amount and type of data that users can access. A well-implemented solution helps ensure that users who are performing necessary functions are doing so at the appropriate privilege level. Identity management is also critical for maintaining separation of roles and duties, which may be required by specific regulatory and compliance standards. Knowing who a user is lets an application determine how it should interact with that user. Managing identity is just as important in the public cloud as it is in on-premises environments.

Azure provides services to help track identity and manage your users. Azure Active Directory (Azure AD) is a comprehensive identity and access management service for the cloud that helps secure access to data in on-premises and cloud applications; it also simplifies the management of users and groups. It combines core directory services, advanced identity governance, security, and application access management.

As with identity, authentication is essential for managing user identities. Authentication is the process of proving identity, typically through credentials, such as a user name and password. More and more, teachers, staff, other educational officials, appropriate law enforcement and vendors require access from outside. Greater numbers of schools allow their teachers, administrators and staff to use their own devices, (BYOD), that access is no longer limited to school-owned and managed laptops.

Users often connect from personal and mobile devices across unsecured networks. Organizational data and applications are accessed through these networks. With escalating IT security threats and a growing number of users, applications, and devices, multi-factor authentication has become the new standard for securing access.

3. Use appropriate access controls

Access control is a mechanism for providing a user who has a valid identity, and who has authorized rights and/or privileges, to access and perform functions using information systems, applications, programs, or files. Comprehensive access control strategies need to be in place, especially when considering the fact that corporate employees expect to work from any location, on devices of their choice, and to seamlessly connect and access business applications.

Azure Active Directory single sign-on provides is a cloud-based service that provides authenticate and authorization for users to gain access to web applications and services, while allowing authentication and authorization to be factored out of custom built solutions. Instead of implementing an authentication system with user accounts that are specific to an application, it is possible to let Azure Active Directory to orchestrate the authentication and much of the authorization of users.

Role-based access control (RBAC) features can be used to restrict access and permissions for specific cloud resources. To help detect suspicious access, Azure Active Directory offers reports that provide alerts about anomalous activity, such as a user logging in from an unknown device. In addition, operational logging and alerting capabilities can notify customers if someone stops a website, or if a virtual machine is deleted.

4. Log security events, implement monitoring and visualization capabilities

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries. Each entry contains information related to a specific event that has occurred within a system or network. A forensic analysis uses a security and audit solution to seek out evidence that potentially malicious users leave behind. Regardless of what users do in their IT environment, many of the activities they participate in generate security artifacts. Evidence about their use is stored in event logs.

Azure Operational Insights collects these artifacts as soon as they occur, before anyone can tamper with them, and allows different types of analysis by correlating data across multiple computers. Azure enables customers to perform security event generation and collection from Azure IaaS and PaaS roles to central storage in their subscriptions. These collected events can be exported to on-premises security information and event management (SIEM) systems for ongoing monitoring. After the data is transferred to storage, there are many options to view the diagnostic data.

5. **Keep service and server inventory current and up-to-date**

Service and server inventory is about knowing what subscriptions, domains, services, networks, and hosts are owned and managed. Keeping track of the services and mitigating the risks that come with those services is key for secure operations. Using tools and scripts to inventory a subscription, and export to excel can help provide insight into an organizations Azure assets. Additionally, having an understanding and priority of the data that is being protected by implementing data classification, as described in the Data classification for cloud readiness white paper is recommended.

6. **Train all staff in cyber security**

If a development team does not understand the basics of secure design and development or the risks of running web-based solutions and services, security training is imperative and should be completed before any Azure-based application is designed, built, tested, or deployed. All members of the operations and development teams should be informed about security basics and recent trends in security and privacy, and they should attend at least one relevant security training class every year at a minimum.

Staff, teachers, administrators and vendors should be encouraged to seek opportunities for additional security and privacy education when possible. Teachers and administrators who are well-versed and up-to-date on security issues are better able to design, develop, and operate software with security in mind first.

Infrastructure as a service recommendations (IaaS)

While no less important, customers who purchase Azure as their cloud infrastructure (IaaS) to manage their data should implement the following controls:

1. **Patch all systems and ensure security updates are deployed**

Software systems need to be updated with necessary security updates regularly. Organizations need to watch out for security threats and maintain stability of software environments. Minimizing security threats requires properly configured systems that use the latest software and have the recommended software updates/patches installed. Microsoft Security Center can help you get a central view of the security state of all of your Azure resources. At a glance, verify that the appropriate security controls are in place and configured correctly.

2. **Use industry-recommended, enterprise-wide antimalware solution**

Malware, also known as malicious code and malicious software, refers to programs that are inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system to annoy or disrupt the victim. Malware such as viruses, Trojans, and worms are usually designed to perform nefarious functions in such a way that users are unaware of them, at least initially. Customers should install and configure reputable anti-malware and anti-virus software on their systems to prevent breaches of security and other security incidences. Microsoft Security Center can be used to help monitor the state of an organizations Azure deployment, reducing the risk of Azure hosts, that are not protected against malware.

3. **Effective certificate acquisition and management**

A certificate is a form of identification for websites and web applications that is used to verify authenticity. Websites rely on TLS and Secure Socket Layer (SSL) to encrypt data communications. To securely configure solutions that require certificates it is recommended to use TLS over SSL as a more robust, and secure solution. Self-signed certificates can be acceptable in some restricted use cases (dev and test). However, a signed and authorized certificate that is issued by a certification authority (CA) or a trusted third-party who issues certificates for this purpose is recommended.

4. **Penetration testing**

Designers and school IT departments need to think like attackers when planning and designing an organization's network and services. Penetration testing is not about verifying functionality, but about verifying the absence of insecure functionality. Effective penetration testing is about finding properties in software and its environment that can be varied, varying them, and seeing how the software responds. The goal is to ensure that software performs reliably and securely under reasonable and even unreasonable production scenarios. Many software weaknesses can be identified by implementing SDL for new services

5. **Maintain clear server configuration with security in mind**

Server misconfiguration is one of the most common causes for unauthorized users accessing and compromising the host. Because of the potentially complex security configuration requirements, it is essential to use a master server image that has security measures in place. Azure provides customers a marketplace with a gallery of servers that have been configured with security in mind. However, the use of

the servers in the marketplace requires attention when educational organizations require custom security modifications and to prevent security configuration drift. Azure Security Center can provide insight into configuration issues and help remediate virtual hosts that require attention.

6. **Determine the root cause of incidents**

Root cause analysis (RCA) is a structured and facilitated team process used to identify root causes of an event that resulted in an undesired outcome. The end result of this exercise is to develop corrective actions that can be driven back into policy. The RCA process provides a way to identify breakdowns in processes and systems that contributed to the event and how to prevent future events. The purpose of an RCA is to find out what happened, why it happened, and determine what changes need to be made.

Closing

The Microsoft Cloud is built upon trust. To that end, we focus a significant amount of our efforts on security, privacy, compliance, and transparency. This document is meant to provide customers with a level of transparency about how the Microsoft Azure can be used and who can use it. Microsoft's goal is to provide cloud solutions that help customers comply with FERPA requirements. It also illustrates our commitment to protecting our customers and our Azure Cloud environment with both logical and network solutions, physical protection, and a validation criterion. As we continue to invest in Azure , we look forward to the opportunity to innovate with the Education Sector environment, and provide Microsoft solutions that help customers meet their FERPA and other regulatory requirements.