Axcient

Mapping CIS Controls to Axcient x360

Reasonable Cybersecurity for MSPs

MSP Guide to Compliance and Reasonable Cybersecurity Through Critical Security Controls

Many MSPs are looking to the CIS Critical Security Controls® framework to implement thorough (or reasonable) cybersecurity for their clients. This guide will demonstrate how Axcient's x360Recover, x360Cloud, and x360Sync are essential components in an MSP's toolkit when pulling together a solid security playbook.

Many U.S. States require governmental agencies and other entities that work with them to implement cybersecurity best practices. Several of them specifically cite CIS Controls as a framework well suited to demonstrate a "reasonable" commitment to security. It has become increasingly complex to confidently define what is reasonable for an MSP. This guide will illustrate how our products map to CIS Controls and provide insight into how to implement Reasonable Cybersecurity in the face of breaches and cyber-attacks.

CIS Controls

The Center for Internet Security is a non-profit globally recognized for sound best practices for securing IT systems and data. Commonly known as "CIS," it describes its CIS Controls as: "a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture. Today, thousands of cybersecurity practitioners from around the world use the CIS Controls and/or contribute to their development via a community consensus process." Security-focused MSPs follow its prioritized set of actions to protect themselves and their client data from cyber-attack vectors.

Axcient's Map to CIS Controls

Implementing each of the 18 Controls and the corresponding 153 CIS Critical Security Controls safeguards is no small task. Our team created this map to help our partners with the Axcient Governance, Risk, and Compliance Team has mapped out how our x360 solutions map to 3 of the CIS Controls:

- **Control 3: Data Protection -** Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.
- **Control 11: Data Recovery -** Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.
- **Control 17: Incident Response Management -** Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Axcient is a 100% MSP-only solution provider committed to redefining data protection, so we cannot satisfy every control, but we map to 12 Control safeguards that are our wheelhouse. Let's look at how Axcient's x360 solutions satisfy safeguards in Controls 3, 11, and 17.

How Axcient Satisfies CIS Controls

Control 3: Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

3.4 Enforce Data Retention

Objective: Retain data according to the enterprise's documented data management process.
Data retention must include both minimum and maximum timelines.

x360Sync

- **Features and Functionalities:** Automated retention policies for data are user configurable.
- **How It Satisfies the Control:** By setting specific retention periods for different organizations, x360Sync ensures compliance with enterprise data retention requirements, allowing for both minimum and maximum retention periods.

x360Recover

- **Features and Functionalities:** Managed backup data retention policies and tiered retention.
- **How It Satisfies the Control:** Ensures backups are retained according to organizational policies, supporting compliance with data retention standards.

x360Cloud

- **Features and Functionalities:** Long-term data retention for cloud backups.
- **How It Satisfies the Control:** Long-term retention that ensures cloud-stored data adheres to the enterprise's data retention policies, facilitating regulatory compliance.

3.5 Securely Dispose of Data

Objective: Securely dispose of data as outlined in the enterprise's documented data management process.
Ensure the disposal process and method are commensurate with the data sensitivity.

x360Sync

- **Features and Functionalities:** Secure deletion features to permanently remove data.
- **How It Satisfies the Control:** Provides mechanisms to securely and automatically delete sensitive data, ensuring compliance with organizational data disposal policies.

x360Recover

- **Features and Functionalities:** Options for secure data destruction of backup data.
- **How It Satisfies the Control:** Ensures data no longer needed is securely disposed of, preventing unauthorized access post-deletion.

x360Cloud

- **Features and Functionalities:** Secure deletion tools for cloud-based data.
- **How It Satisfies the Control:** Allows for secure and permanent removal of cloud-stored data, adhering to security and compliance requirements.

3.10 Encrypt Sensitive Data in Transit

Objective: Encrypt sensitive data in transit to protect it from unauthorized access during transfer.

x360Sync

- **Features and Functionalities:** TLS/SSL encryption for data transfer.
- **How It Satisfies the Control:** Ensures that all data transferred between endpoints and the server is encrypted, protecting it from interception and unauthorized access during transit.

x360Recover

- **Features and Functionalities:** Encrypted data transfer protocols using TLS/SSL and SSH.
- **How It Satisfies the Control:** Protects backup data during transfer, ensuring its confidentiality and integrity.

x360Cloud

- **Features and Functionalities:** End-to-end encryption for cloud data transfers via TLS/SSL.
- **How It Satisfies the Control:** Protects sensitive data during upload and download processes, ensuring it remains secure during transit.

3.11 Encrypt Sensitive Data at Rest

Objective: Encrypt sensitive data at rest on servers, applications, and databases to protect it from unauthorized access.

x360Sync

- **Features and Functionalities:** AES-256 encryption for data stored on servers.
- **How It Satisfies the Control:** Ensures that all stored data is encrypted, providing robust protection against unauthorized access and breaches.

x360Recover

- **Features and Functionalities:** Encrypted backups stored using industry-standard encryption method of AES-256.
- **How It Satisfies the Control:** Protects backup data at rest, ensuring its confidentiality and integrity even if physical security is compromised.

x360Cloud

- **Features and Functionalities:** Cloud storage encryption using strong encryption algorithms.
- **How It Satisfies the Control:** Secures sensitive data stored in the cloud, protecting it from unauthorized access and breaches.

3.12 Segment Data Processing and Storage Based on Sensitivity

Objective: Segment data processing and storage based on the sensitivity of the data to prevent unauthorized access.

x360Sync

- **Features and Functionalities:** Role-based access control and data segmentation.
- **How It Satisfies the Control:** Allows for the separation of data based on sensitivity levels, ensuring that only authorized users can access sensitive information.

x360Recover

- **Features and Functionalities:** Logical segmentation of backup data.
- **How It Satisfies the Control:** Allows for sensitive backup data to be stored separately from less sensitive data, reducing the risk of unauthorized access.

x360Cloud

- **Features and Functionalities:** Logical segmentation of backup data.
- **How It Satisfies the Control:** Ensures that sensitive data is stored and processed in isolated environments, protecting it from unauthorized access and breaches.

3.14 Log Sensitive Data Access

Objective: Log sensitive data access, including modification and disposal, to maintain an audit trail.

x360Sync

- **Features and Functionalities:** Detailed logging of all access and modifications to data.
- **How It Satisfies the Control:** Provides comprehensive audit trails that capture all access, changes, and deletions of sensitive data, ensuring accountability and traceability.

x360Recover

- **Features and Functionalities:** Logging and monitoring of backup access and modifications.
- **How It Satisfies the Control:** Ensures that all interactions with backup data are recorded, providing an audit trail for security and compliance purposes.

x360Cloud

- **Features and Functionalities:** Cloud-based logging of access and modifications and logging and monitoring of backup access and modifications.
- **How It Satisfies the Control:** Captures and stores logs of all access and changes to cloud-stored data, providing an audit trail for compliance and security.

Control 11: Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

11.1 Establish and Maintain a Data Recovery Process

Objective: Establish and maintain a documented data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually or when significant enterprise changes occur that could impact this Safeguard.

x360Sync

- **Features and Functionalities:** Provides file synchronization and sharing with version history and the ability to revert to previous versions of files. Ensures that users can recover deleted or previous file versions.
- **How It Satisfies the Control:** Maintains a process for file-level data recovery through synchronization and version control, supporting quick recovery from data loss incidents.

x360Recover

- **Features and Functionalities:** Provides a comprehensive disaster recovery process including full system recovery, virtualization, and individual file restore. The Recovery Center guides users through various recovery scenarios and offers detailed documentation on recovery procedures. Airgap feature that ensures backups can always be recovered.
- **How It Satisfies the Control:** Ensures a documented and maintained data recovery process for handling full system failures, individual file losses, and virtualized recovery scenarios.

x360Cloud

- **Features and Functionalities:** Offers detailed recovery options for Microsoft 365 and Google Workspace, including item-level recovery for emails, documents, and other data. Supports tracking and managing recovery operations through the user dashboard.
- **How It Satisfies the Control:** Establishes a documented recovery process tailored to cloud applications, ensuring detailed and manageable recovery steps for various data types.

11.2 Perform Automated Backups

Objective: Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.

x360Sync

- **Features and Functionalities:** Continuously synchronizes files across devices, ensuring real-time backups of the latest file versions.
- **How It Satisfies the Control:** Provides automated, continuous backup of files as changes occur, supporting real-time data protection and recovery.

x360Recover

- **Features and Functionalities:** Supports automated backups for servers and workstations with configurable schedules, offers image-based backups.
- **How It Satisfies the Control:** Ensures that automated backups are regularly performed without user intervention, meeting requirements for consistent data protection.

x360Cloud

- **Features and Functionalities:** Automates backups for cloud applications like Microsoft 365 and Google Workspace, capturing data at least once a day
- **How It Satisfies the Control:** Guarantees regular, automated backups of cloud data, ensuring continuous protection and compliance with backup policies.

11.3 Protect Recovery Data

Objective: Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

x360Sync

- **Features and Functionalities:** Employs TLS/SSL for data in transit and 256-bit AES for data at rest.
- **How It Satisfies the Control:** Provides secure protection of synchronized and backed-up files through encryption, supporting secure data recovery.

x360Recover

- **Features and Functionalities:** Employs TLS/SSL for data in transit and 256-bit AES for data at rest.
- **How It Satisfies the Control:** Protects recovery data with encryption standards equivalent to those used for the original data, meeting requirements for secure data protection.

x360Cloud

- **Features and Functionalities:** Employs TLS/SSL for data in transit and 256-bit AES for data at rest.
- **How It Satisfies the Control:** Ensures that recovery data is protected with strong encryption, maintaining the same security level as the original data.

11.4 Establish and Maintain an Isolated Instance of Recovery Data

Objective: Establish and maintain an isolated instance of recovery data. Example implementations include version-controlling backup destinations through offline, cloud, or offsite systems or services.

x360Sync

- **Features and Functionalities:** Provides version history and file recovery, allowing recovery from isolated versions of files.
- **How It Satisfies the Control:** Maintains isolated instances of file versions, supporting secure recovery operations.

x360Recover

- **Features and Functionalities:** Provides a separate instance of storage for backup data to customers.
- **How It Satisfies the Control:** Ensures isolated storage of recovery data, preventing contamination and maintaining data integrity during recovery.

x360Cloud

- **Features and Functionalities:** Allows for recovery of data to different user accounts, maintaining separation of restored data through defined recovery procedures.
- **How It Satisfies the Control:** Provides isolated recovery instances for cloud application data, ensuring data integrity and compliance with isolation requirements.

11.5 Test Data Recovery

Objective: Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

x360Sync

- **Features and Functionalities:** Provides version history and restore options that can be used to test data recovery processes regularly.
- **How It Satisfies the Control:** Ensures the reliability of file recovery through regular testing and validation of restore capabilities.

x360Recover

- **Features and Functionalities:** Features a Recovery Center that allows for the testing of data recovery through virtualization and file restoration processes. AutoVerify feature ensures that the virtual machine image boots.
- **How It Satisfies the Control:** Supports regular testing of data recovery capabilities, ensuring that recovery processes are effective and meet organizational requirements.

x360Cloud

- **Features and Functionalities:** Enables administrators to perform restore tests by recovering data to different user accounts and tracking the restoration process.
- **How It Satisfies the Control:** Ensures the reliability of cloud data recovery through regular testing and validation of backup integrity.

Control 17: Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

17.7 Conduct Routine Incident Response Exercises

Objective: Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision-making, and workflows. Conduct testing on an annual basis, at a minimum.

x360Sync

- **Features and Functionalities:** Real-time synchronization and sharing of files. Logs user activities and file changes.
- **How It Satisfies the Control:** Utilizes activity logs for incident response scenarios, assessing decision-making and identifying areas for improvement.

x360Recover

- **Features and Functionalities:** Regular testing of recovery plans through appliance-free and virtualized recovery. Reports on backup statuses and health checks.
- **How It Satisfies the Control:** Enables simulation of disaster recovery scenarios, assessing communication channels and workflows during exercises.

x360Cloud

- **Features and Functionalities:** Efficient cloud data backup and recovery. Logs all backup and recovery activities.
- **How It Satisfies the Control:** Facilitates testing of data recovery processes during incident response exercises, providing a thorough analysis

The CIS Reasonable Cybersecurity Guide

Navigating the ever-evolving cybersecurity landscape can feel like walking a tightrope for managed service providers (MSPs). You're responsible for safeguarding the digital assets of your diverse client base, so a clear understanding of "reasonable cybersecurity" is crucial.

The ambiguity surrounding this term has long been a source of frustration. What constitutes reasonable security for one company might be woefully inadequate for another. This ambiguity can lead to confusion and even litigation following a data breach.

The Center for Internet Security (CIS) has stepped in to provide much-needed clarity with its "Reasonable Cybersecurity: A Framework for Organizations" guide. This comprehensive resource offers a standardized approach to building a robust cybersecurity program, regardless of industry or size.

The Legal Landscape: Why Reasonable Cybersecurity Matters

Data breaches are a constant threat in today's digital world, and the repercussions can be far-reaching. Beyond the immediate financial losses and reputational damage, organizations can face significant legal consequences following a breach.

The legal landscape surrounding data security is complex and constantly evolving. However, several key federal laws and regulations can impose hefty fines and penalties on organizations that fail to adequately protect sensitive data. These include:

- **The Federal Trade Commission (FTC) Act:** The FTC has broad authority to enforce unfair and deceptive trade practices, which can encompass inadequate data security measures. In the wake of a breach, the FTC may investigate and pursue civil penalties if it determines the organization's security practices were unreasonable.
- **Gramm-Leach-Bliley Act (GLBA):** This law applies to financial institutions and requires them to implement a comprehensive information security program to protect customer data. Failure to comply with GLBA can result in significant fines and enforcement actions.
- **Health Insurance Portability and Accountability Act (HIPAA):** HIPAA sets strict security standards for healthcare providers and health plans that handle protected health information (PHI). Violations of HIPAA's security rules can lead to civil and even criminal penalties.
- **Family Educational Rights and Privacy Act (FERPA):** A Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable U.S. Department of Education program. The law gives parents certain rights regarding their children's education records and students once they are 18.
- **General Data Protection Regulation (GDPR):** Rules on ways to use, process, and store personally identifiable data.). It applies to all organizations within the EU and any organizations that supply goods or services to the EU or monitor EU citizens.
- **Payment Card Industry (PCI):** Compliance requirements to ensure the security of credit card information that is stored, transmitted, or processed.

Beyond Federal Laws: It's important to note that these are just a few examples, and several other federal regulations and state laws can impose data security obligations on organizations depending on their industry and the type of data they collect.

The Importance of Reasonableness

The concept of "reasonable cybersecurity" plays a critical role in legal proceedings following a data breach. While there's no single definition of "reasonable," the CIS Reasonable Cybersecurity Guide provides a valuable framework for organizations to demonstrate they have taken appropriate steps to protect sensitive data. By implementing the guide's recommendations, organizations can significantly strengthen their legal defense in the event of a breach.

In essence, a robust cybersecurity program isn't just about mitigating technical risks but also legal risks. The CIS Reasonable Cybersecurity Guide provides a roadmap for achieving a security posture that meets a reasonable standard, helping organizations protect themselves from a data breach's financial and legal repercussions.

The Five Essential Elements of Reasonable Cybersecurity

The CIS guide outlines five fundamental elements that every effective cybersecurity program and MSP's security playbook needs to encompass:

1. **Identify:** This involves understanding your organization's critical assets and the potential threats they face. This includes data, systems, applications, and even physical security measures.
2. **Protect:** Once you've identified your vulnerabilities, it's time to implement safeguards. This includes firewalls, intrusion detection systems (IDS), data encryption, and access controls.
3. **Detect:** Early detection is critical for minimizing damage from a cyberattack. Security information and event management (SIEM) solutions can help you monitor your network for suspicious activity.
4. **Respond:** Having a well-defined incident response plan allows you to react swiftly and efficiently in the event of a breach. This plan should outline roles, responsibilities, and communication protocols.
5. **Recover:** Recovering from a cyberattack involves restoring compromised systems and data. Regular backups and disaster recovery plans are essential for minimizing downtime and ensuring business continuity.

Implementing Reasonable Cybersecurity

The CIS guide goes beyond theory, offering practical guidance on implementing its recommendations. This includes:

- **Prioritization:** The guide acknowledges that resources may be limited. It recommends prioritizing controls based on risk and potential impact.
- **Customization:** The framework is designed to be adaptable to different organizational needs. You can tailor the controls to your specific industry and threat landscape.
- **Metrics and Measurement:** The guide emphasizes the importance of measuring the effectiveness of your cybersecurity controls. This allows you to identify areas for improvement and demonstrate the value of your program to stakeholders.

Benefits for MSPs

The CIS Reasonable Cybersecurity Guide is a valuable tool for MSPs in several ways:

- **Client Education:** You can leverage the guide to educate your clients during QBRs on the importance of a robust cybersecurity program and the benefits of implementing the CIS framework.
- **Standardized Approach:** The guide provides a consistent and standardized approach to help inform your Reference Architecture that can be applied across a diverse client base. This simplifies the process of assessing and securing client environments.
- **Enhanced Service Offerings:** By incorporating the CIS framework into your service offerings, you can bundle security into your offering to differentiate yourself from competitors and demonstrate your commitment to client security.

A Roadmap to CIS Controls and Reasonable Cybersecurity

CIS Controls are an excellent framework for exceeding the "reasonable" benchmarks for MSP security. The CIS Reasonable Cybersecurity Guide is a great reminder and resource for MSPs and their clients to establish a strong foundation for cybersecurity. Defining your MSP's "reasonable cybersecurity" can guide establishing your network and reference architecture, regular risk assessments, and corresponding disaster recovery plans and testing cadence. By adopting the framework's principles and leveraging the available resources, you can significantly reduce your risk profile and build a more secure digital future for your clients.

Taking Action

- Download the CIS Reasonable Cybersecurity Guide and the current CIS Controls.
- Get the Reference Architecture Guide for MSPs.
- Develop your Security Playbook.
- Revisit your DR planning with the Disaster Recovery Planning and Testing Best Practices Guide for MSPs.
- Start incorporating the CIS framework into your client assessments and Quarterly Business reviews with help from the QBR Handbook for MSPs.

About Axcient

Axcient is an award-winning leader in business continuity and disaster recovery for Managed Service Providers (MSPs). Axcient x360 provides one platform for MSPs to Protect Everything ™, and includes BCDR, Microsoft 365 and Google Workspace backup, and secure sync and share. Trusted by more than 5,400 MSP partners worldwide, Axcient protects business data and continuity in the event of security breaches, human error, and natural disasters.

Axcient

Axcient, 707 17th Street, Suite 3900, Denver, CO, 80202
Tel: 720-204-4500 | axcient.com