keepit®

SEC guidelines

What you should do now to be compliant

Throughout 2023, the SEC has introduced new cybersecurity guidelines, aiming to set a new standard for cybersecurity risk management measures and reporting obligations. Now publicly-traded organizations — and those that do business with them — are incentivized more than ever to take measures to minimize cyber risks and ensure business continuity to ensure compliance with these guidelines.

What to do now:

Get your business ready with best practices

What you should do now is run a risk analysis and map out critical processes your business relies on, as well as the technology supporting these processes. Once you have established which of your systems and data is business-critical to back up, create a strong disaster recovery plan and test to know if it works. You can use the following Map-Prioritize-Test framework to help guide you through the process:

1. Map critical systems

Assess and analyze critical infrastructure across on-premises, native cloud, and public cloud environments. Identify and prioritize crucial data, ensuring business continuity. Don't overlook SaaS applications like Entra ID; safeguarding identities and credentials is vital. Neglecting identity and access data can impact business continuity even if other data is fully restored. Microsoft recognizes identity systems as more critical than human life support systems: read more about this.

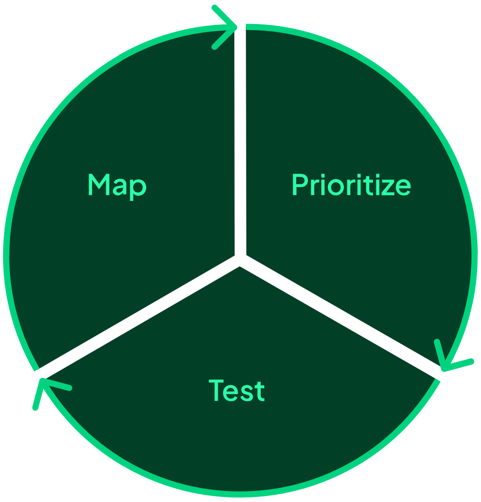
2. Prioritize: What is critical to maintain access to?

What kind of data do you have? How do you protect it? What is the most critical data to regain access to in the event of an attack? Are your CEO's emails critical to your business continuity? Or maybe your logistics data, customer data, intelligence dashboards, or code? Find out what you need to recover first.

3. Test that your backup works

Business continuity testing is a key element of any cybersecurity posture and a necessary part of the framework provided by the SEC. Ensure that your data recovery works:

- Validate restoration capability promptly.
- Determine acceptable downtime.
- Regularly test backups for confidence in your dynamic disaster recovery plan and supporting software.



Choosing a backup and disaster recovery partner

After implementing the above framework, your next task is to explore solutions tailored to your requirements. When selecting a vendor, adhere to industry best practices for data protection. Consider the following:

Security and privacy:

Choose a vendor you can trust to keep your data safe. Implement access controls to safeguard against unauthorized access and process data in compliance with privacy laws. Choose a vendor with leading security controls that is proven to meet demanding regulatory requirements through security certifications so you know your data is always safe.

Recovery time:

Recognize the impossibility of recovering petabytes of data within seconds. Prioritize solutions that enable the swift recovery of identified critical data. Business continuity depends on both uninterrupted data availability and minimizing downtime through rapid recovery. Opt for a solution supporting granular, instant, and prioritized recovery of essential data.

Encryption and immutability:

As natural targets for cybercriminals, backups need robust data protection measures, both at rest and during transfer. Vitally important is ensuring data encryption and immutability to keep hackers from altering or deleting your data — even if they were to gain access.

Vendor independence:

Choose a cloud backup provider that ensures separation from your SaaS vendor's public cloud. Employ air-gapping measures and secure data on distinct logical and physical infrastructures. This safeguards against data loss during public cloud unavailability and prevents ransomware attacks from compromising your backups.

Who do you trust to keep your data safe? Here at Keepit, we:

Offer next-level data protection for your business-critical SaaS applications data

Own and operate our own infrastructure and data center regions across the globe so we can always ensure data accessibility

Deploy leading security measures, such as air gapping, immutability, and encryption both in transfer and at rest

Guarantee full compliance with all applicable regulations and laws keepit®

SEC guidelines at a glance

What is the purpose of the new SEC guidelines?

The recommendations of the SEC on cybersecurity aim to strengthen cybersecurity resilience and increase the security posture of organizations in the United States. Next to cyber-incident reporting requirements, organizations are required to describe their cybersecurity risk management program and disclose governance information in relation to cybersecurity. The main goal is that organizations can maintain a high level of readiness to execute critical functions during a disruption (e.g., a cyberattack) or an emergency.

The SEC guidelines require backup and disaster recovery

Organizations need to establish and maintain business continuity plans to address events that may pose a significant risk of disrupting their operations. As such, this includes a requirement to protect business SaaS data when it supports critical operations.

Who do the guidelines apply to?

The SEC's guidelines apply to all U.S.-listed companies. However, most public companies rely on smaller and private companies throughout their supply chain and the SEC clearly states that cyber procedures need to be extended to all third-party vendors. Therefore, whether public or not, organizations should familiarize themselves with the new regulations and monitor their preparedness. The ultimate objective should be creating an effective cyber risk management program and a solid business continuity plan, beyond just completing compliance checklists.

Start a conversation today

If you'd like to receive advice on your compliance journey and discuss which steps your business needs to take now to comply with the SEC guidelines, let's have a conversation.

Book a meeting

www.keepit.com