



Eliminate Audit Risks and Surprises With ITaaS

Leverage ITaaS for virtualized, fully managed infrastructure configured from the start with your compliance needs in mind

Business is uncertain enough without the added disruption of a costly IT audit that uncovers gaps in compliance that take time, money, and resources to mitigate — and no business is immune.

Google was fined \$57 billion for GDPR violations by CNIL, a French data protection agency.¹ The average cost of failing to comply with data protection regulations is \$14.82 million, and it's estimated that the cost of failure is 2.7 times higher than the cost of complying with regulations.²

IT audits include a comprehensive review of how well a company is complying with regulatory guidelines. This includes a thorough review of the company's compliance preparations, security policies, user access controls, data security, and risk management procedures. Once an IT auditor approaches the business with a request, the company must respond with documentation and artifacts to demonstrate compliance with security and regulatory requirements.

Preparing for IT Audit Impact

If an IT audit detects compliance failures, the company can face hefty fines. An IT audit can happen at any time. In fact, some business contracts and third-party agreements include a "right to audit" clause to allow partners to conduct or demand security assessments.

Part of the challenge for many companies isn't the IT audit itself, but a lack of preparedness for the audit. Yet many companies only think about compliance after an IT auditor approaches them. This puts the business in a reactionary mode that can be costly and disruptive.

Common Causes of IT Audit Failure

1. **Leadership.** A lack of dedication to making compliance a priority at the top of the organization proliferates throughout the organization.
2. **Documentation.** The inability to provide evidence or records that support system compliance or performance leaves auditors to rely on inquiry, which is a weak form of audit evidence.
3. **Human Error.** Human error caused by manual systems or faults of omission can leave data exposed and vulnerable.
4. **Infrastructure.** IT infrastructure misaligned with compliance mandates can be an IT audit vulnerability. For example, sensitive data and information stored on mobile devices and public clouds must be secured.
5. **Preparedness.** Risk assessments and internal audits are often put off because there's a lack of time or expertise to perform them.

Easing Audits With ITaaS

Since data risk resides within infrastructure, IT as a Service (ITaaS) can help companies comply with regulatory requirements and respond to IT audits with less cost and business impact. ITaaS delivers infrastructure as a service that is managed by a provider who can align IT processes with compliance requirements. The ITaaS provider can also ensure that security policies are updated as regulations change, eliminating the risk and cost of being caught operating outside of stated guidelines. And now, with many businesses relying on cloud-based applications more than ever because of COVID-19, ITaaS provides secure access to cloud-based data and applications to satisfy many data security regulatory requirements.

ITaaS from Adar for Strong Audit Protection and Remediation

Adar offers ITaaS that delivers a comprehensive, seamlessly integrated IT environment that combines infrastructure, cloud technologies, and managed services made highly affordable with a fixed cost per user. The ITaaS from Adar platform includes robust security and compliance features, such as a dedicated firewall, a 100% network uptime guarantee, automatic security patching, and 24/7/365 monitoring — keeping your business connected, protected, and compliant.

Adar customizes its ITaaS, building it with the customer's compliance needs in mind from the start. As regulations change or evolve, Adar's team works to maintain safety, security, and compliance. If an IT auditor comes knocking, Adar experts and engineers can help customers quickly and accurately respond to IT audit requests and remediate issues so they can:

- Eliminate the human capital costs associated with audit preparation and response
- Prevent business disruptions caused by compliance fines or remediation efforts
- Gain audit and security expertise to augment existing IT resources

How Does Adar Simplify IT Audits?

- Discovery during onboarding to identify compliance mandates
- Virtual infrastructure aligned with compliance needs
- Ongoing security and compliance updates as requirements change
- Proactive remediation of compliance gaps
- Technical responses to IT audit requests, complete with audit trails, artifacts, and remediation

What Types of Audits Can Adar Assist With?

- FINRA
- HIPAA
- NY DFS
- SEC
- HITRUST
- GDPR

Adar: All Virtual, All Done

Adar takes the guesswork out of deployment, management, optimization, and pricing of all your IT needs. With solutions for local, national, and international organizations, Adar pairs cutting-edge virtualized environments with enterprise-level security, support, and award-winning customer service — all monitored and maintained for you 24/7/365.

Contact us today to learn more about our ITaaS solutions.

Adar | 877.860.0700 | sayhello@adarit.com | adarit.com

¹Tech Crunch, "French Data Protection Watchdog Fines Google \$57 Million Under the GDPR," Jan. 2019.

²Security Intelligence, "Failure to Comply With Data Protection Regulations Can Cost Firms Nearly \$15 Million," May 2018.