



EBOOK

Staying Compliant with Key Data Security Regulations

Essential Salesforce DevSecOps Considerations & Tools

INTRODUCTION

Data security is an increasingly difficult effort for major companies and organizations. Breaches, hacks, and leaks are more costly and prevalent than ever. What was once thought to be a problem only for those who couldn't afford adequate data security measures has become a problem for massive operations—including everyone from Fortune 500 companies to departments of government.

The exact data security regulations that apply to a singular company will depend on the location of operations, who that company does business with, and which types of data are held within their system. This means that every regulation doesn't apply to every business. However, it can also mean that more than one regulation can apply to a singular business.

The vast network of compliance standards has overlapping qualities that make it easier to abide by many regulations with a singular data security strategy. Anybody that operates with sensitive information—such as the healthcare, banking, insurance, and pharmaceutical industries—needs to be aware of these qualities.

Intentional processes and the utilization of proper tools make it much easier for those in regulated industries to adhere to essential standards. We'll focus on three of the most widespread regulations: the Sarbanes-Oxley Act (SOX), General Data Protection Regulation (GDPR), and Health Insurance Portability and Accountability Act (HIPAA).

These 5 considerations will provide the necessary infrastructure you need to maintain compliance with these data security regulations:

1. Find Sensitive Data	004
2. Ensure Accurate Reporting	006
3. Document Stored Data	008
4. Institute Tools and Procedures for Data Protection	010
5. Establish Protocol in the Event of a Breach	012

01

Find Sensitive Data



FIND SENSITIVE DATA

Every data security regulation specifies particular data sets that need to be protected. A company's first step to adhering to this regulation is to locate and identify the specified data. Anything that remains unfound is liable to contribute to falling out of compliance with applicable regulations.

SOX

Financial records need to be accounted for and accurate in order to properly comply with Sox regulations. Companies need to locate financial statements, ensure they are up to date, and compile them with no gaps of unaccounted periods of time. Any changes in financial records needs to be explained.

HIPAA

Healthcare providers are responsible for protecting the sensitive information of patients. This includes personally identifiable information (PII) as well as protected health information (PHI). These types of sensitive data need to be vigorously protected. They also need to be made available to patients should they be requested.

GDPR

Companies that collect data on citizens of EU countries need to abide by strict handling protocols. This includes making sure the data is accurate, available, and transparent. However, this is impossible if a company is unable to locate and identify which information needs to be protected.

AutoRABIT Assistance

Manually scanning your system for sensitive data and metadata will take an extremely long time. And because this is an ongoing effort, it's unrealistic to accomplish this without the help of automation. AutoRABIT Vault enables teams to compare live environments with backup repositories to spot discrepancies. AutoRABIT ARM tracks who made changes, where, and when. And CodeScan can provide a current overview of your system's data.

"CodeScan really has saved us a lot of time in doing code reviews. We had the opportunity to let our developers install it in the VS Code IDE and CodeScan did everything else."

- SHESHANT K.

02

Ensure Accurate Reporting



ENSURE ACCURATE REPORTING

A major aspect of regulatory compliance is being able to prove you are abiding by the stipulated requirements. Ample and accurate reporting is a necessity to accomplish this. Auditors will ask for a specific set of data—depending on which regulations apply to your organization—and you will be expected to quickly provide this data in a coherent format.

SOX

Financial data must be provided to portray a realistic viewpoint of the company's gains, losses, and expenditures. Any mistakes this reporting are likely to lead to fines and penalties as they put the company's actions closer to fraud. Shareholders and auditors expect transparency.

HIPAA

The protection of sensitive patient information requires strong access controls and other measures to ensure data security. HIPAA requires these measures to be quantifiable through ample reports—especially in the case of a breach. A failure to keep proper track of security considerations can be a violation.

GDPR

A data breach must also be reported to remain compliant with the GDPR. This includes the nature of the breach, what happened as a result of the breach, and the measures the organization took to address the breach. Accurate and up-to-date data must be provided to remain in compliance.

AutoRABIT Assistance

AutoRABIT ARM, Vault, and CodeScan all offer reporting capabilities to keep you compliant with data security regulations. These reports offer a comprehensive snapshot of the health of your environment and can be used to create reports to provide the alerts you need after a breach occurs.

03

Document Stored Data



DOCUMENT STORED DATA

Finding sensitive data within your system is only the first step to properly handling protected information. It is also required by many regulations that a company keeps updated documentation of this data so it can be easily found and provided if an auditor requests it. This includes the data stored directly on your system along with any data backup repositories.

SOX

Transparency of financial data is the focus of the Sarbanes-Oxley Act. It is essential for companies in regulated industries to find, flag, and document any information that relates to financial records that will need to be provided to auditors and shareholders to convey an accurate representation of the company's finances.

HIPAA

PII and PHI are incredibly valuable. This is why cybercriminals frequently target healthcare companies and why HIPAA has strict guidelines for how this information is handled. Documentation is required to highlight this information so auditors have a clear view of what needs to be protected and what you're doing to guard it.

GDPR

Document the data within your system will make it much easier to abide by the 7 principals of the GDPR. Ensuring the data you have is accurate, not holding it for longer than you need it, and proper documentation are just a few of the considerations that must be addressed.

AutoRABIT Assistance

Source control systems offer time stamps and personal identifiers, so you always know who touched what parts of the system and when. Scan your system with ARM and CodeScan to locate data and metadata so you can organize and document sensitive pieces of information.

03

Institute Tools and Procedures for Data Protection



INSTITUTE TOOLS AND PROCEDURES FOR DATA PROTECTION

Reasonable data security measures are expected and required by various regulations. Companies that have accepted the responsibility of gathering sensitive information must then provide proper coverage so it is not compromised. Utilizing adequate tools and procedures to protect this information is non-negotiable.

SOX

Compromised financial data can lead to inadequate—or incorrect—reporting. Safeguarding performance, ensuring functionality of your systems, guarding against data tampering, and enabling role-based permissions are just a few of the considerations that need to be taken to adhere to SOX guidelines.

HIPAA

As defined by the HHS: “The HIPAA Security Rule establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.”

GDPR

The GDPR’s principals require companies that gather sensitive data to properly protect it. Every type of potentially sensitive data in the company’s possession must be protected with adequate safety measures to prevent an unnecessary leak, hack, or exposure of user data. This includes measures such as encryption, access controls, and more.

AutoRABIT Assistance

A comprehensive data security strategy requires multiple automated tools working in tandem. The AutoRABIT platform offers static code analysis to scan your system for potential threats, CI/CD pipelines to ensure stronger applications and updates, and a data backup and recovery tool that ensures you can quickly return to operations after an outage. AutoRABIT also offers flexible hosting options including on-premises hosting for the ultimate level of control.

03

Establish Protocol in the Event of a Breach



ESTABLISH PROTOCOL IN THE EVENT OF A BREACH

Even the strongest data security strategies need to prepare for worst case scenarios. This includes maintaining a current data backup and recovery plan, but for compliance reasons, it also means having a protocol for reporting an incident. SOX, HIPAA, and the GDPR all require disclosures when a data security breach occurs.

SOX

Security breaches—as well as any breakdowns of file or network integrity—need to be reported to auditors as soon as possible. SOX compliance necessitates complete transparency with all aspects of handling financial data. This extends to incidents of possible exposure.

HIPAA

The Department of Health and Human Services (HHS) and the Office for Civil Rights (OCR) must be notified if there is a breach to your system. Patient information might be compromised as a result of this breach which will necessitate a series of actions on the company's behalf. Securing the system and notifying the proper authorities needs to be at the front of that list.

GDPR

Companies have a 72-hour window in which to report a data security breach to the proper supervisory authority. This will include the scope and nature of the breach, potential consequences, how the threat will be addressed, and contact information for the appointed data protection officer.

AutoRABIT Assistance

Various dashboards and reports are available on the AutoRABIT platform to provide a high-level analysis of your system's health. These reports can be leveraged to spot unauthorized access to your system, enabling you to recognize the issue so it can be quickly rectified and reported. Audit and eDiscovery support is available for detailed reporting of who made changes to your system, where, and when.

CONCLUSION

Data security regulations are in place to ensure companies maintain good practices when handling sensitive information. This can come in the form of personally identifiable information, financial information, health information, or anything else that has the potential to negatively impact a person's life should it be exposed.

There are a series of overlapping qualities of these regulations that all companies—whether they operate in a regulated industry or not—should work towards. Above all else, it's essential for companies to enact a data security strategy that provides a series of fortifications to lessen the likelihood of experiencing a breach.

However, nobody is immune to a data breach. There must also be systems in place to restore lost information and report the incident to relevant authorities—data backup and recovery.

AutoRABIT provides a series of tools that address the various aspects of compliance with data security regulations. AutoRABIT offers proper oversight, strong code, a reliable backup and recovery plan, and self-hosting for a well-rounded approach to proper data security and regulatory compliance.


“AutoRABIT has helped us add a lot of automation to our software development lifecycle. I highly recommend it!”

- FORREST COOK

ABOUT AUTORABIT

AutoRABIT is a Continuous Delivery suite for SaaS platforms. We automate and accelerate the entire application development and release process. This enables continuous integration and delivery by providing fast, simple, and secure end-to-end automation across all Salesforce implementations. We help enterprises achieve higher release velocity and faster time-to-market.

AutoRABIT provides static code analysis, automated metadata deployment, version controlling, advanced data loading, orgs and sandbox management, test automation, and reporting. Our services complement and extend Salesforce DX. AutoRABIT Vault—our backup and recovery solution—streamlines Salesforce data, simplifies data backup challenges, offers disaster recovery, and endpoint data protection on the Cloud. CodeScan provides full visibility into code health from the first line written through final deployment into production. Record Migrator provides automatic bundling of all feature dependencies for Salesforce managed packages and deployment of templates ensures fast, efficient, and seamless releases.

Visit us at www.aurorabit.com to learn more. 

“AutoRABIT is a well-blended suite of solutions that complemented our Salesforce Release Management efforts.”

- JAKEER H.

CERTIFIED
+ COMPLIANT



CALIFORNIA
CONSUMER PRIVACY ACT

