Security Benchmark for Salesforce: A comprehensive security standard for Salesforce environments

Independent, prescriptive and auditable security controls for evaluating the security posture of Salesforce organizations.

What SBS Is

Salesforce has evolved far beyond its CRM origins to become a mission-critical business platform for many of the world's largest enterprises and government agencies. It is widely recognized as one of the most secure enterprise SaaS platforms in operation, with strong default controls, mature identity primitives, and extensive compliance certifications. However, incident reporting from 2024 and 2025, including analysis published by Google Threat Intelligence, have shown that Salesforce environments are increasingly being compromised through inconsistent implementation and operation of Salesforce security controls at scale. These campaigns have demonstrated repeated abuse of overprivileged users, ungoverned administrator access, and OAuth-based integrations, where legitimate Salesforce features were leveraged to enable data exfiltration, lateral access, and delayed detection when governance and operational discipline broke down.

The Security Benchmark for Salesforce (SBS) addresses a critical gap between what Salesforce makes possible and what is consistently implemented, measured, and defended in real-world enterprise environments. While Salesforce provides extensive security mechanisms, there is no widely accepted, practitioner-defined baseline for what constitutes an adequate Salesforce security posture at enterprise scale. Without such a benchmark, organizations lack an objective way to assess preparedness, compare posture, or understand how their Salesforce environments will withstand, contain, and be investigated during a security incident. SBS defines a set of verifiable conditions that systematically raise security posture over time, under the assumption that security incidents will occur. Its purpose is to reduce breach impact by limiting blast radius, preserving forensic visibility, and enabling effective incident response.

Purpose and Scope

SBS defines the conditions that must be true for a Salesforce environment to be considered securely operated in the context of modern threat activity. It is intended for chief information security officers, security architecture teams, auditors, system integrators, and security tooling as a common reference for evaluating Salesforce security posture in a consistent, auditable, and repeatable manner.

The benchmark applies to Salesforce environments that function as critical business platforms and data systems. It addresses security across organizational, technical, and operational domains, including identity and privilege management, integration governance, data access visibility, development practices, and change management. SBS is designed to support prevention, detection, and recovery by enabling organizations to understand how specific Salesforce security controls reduce breach likelihood, limit impact, and accelerate post-incident assessment.

Control Structure

Each SBS control is expressed as a normative requirement and includes clearly defined audit procedures and remediation guidance. Controls are written to support objective verification and are designed to be evaluated independently or as part of a broader security assessment.

SBS focuses on platform-relevant security outcomes and avoids prescribing specific vendors, tools, or implementation approaches. Where controls depend on optional Salesforce capabilities or external security functions, those dependencies are documented explicitly.

Relationship to Other Frameworks

SBS is complementary to established security frameworks such as NIST and ISO. While those frameworks define program-level security principles, SBS provides Salesforce-specific security requirements that translate those principles into concrete, auditable expectations for Salesforce environments.

SBS is not a certification program and does not replace regulatory or compliance obligations. It is intended to serve as a platform-specific benchmark that organizations may map to broader governance and risk management frameworks.

Governance and Independence

SBS is maintained by an editorial board and contributors drawn from the Salesforce and security practitioner communities. It is an independent initiative and is not official, endorsed, or supported by Salesforce.

Core Attributes

Binary and Auditable

Each control results in a clear compliant/noncompliant determination.

Platform-Specific

Written exclusively for Salesforce's architecture, features, and security model.

Prescriptive

Clearly states what must be done, not optional guidance.

Vendor-Neutral

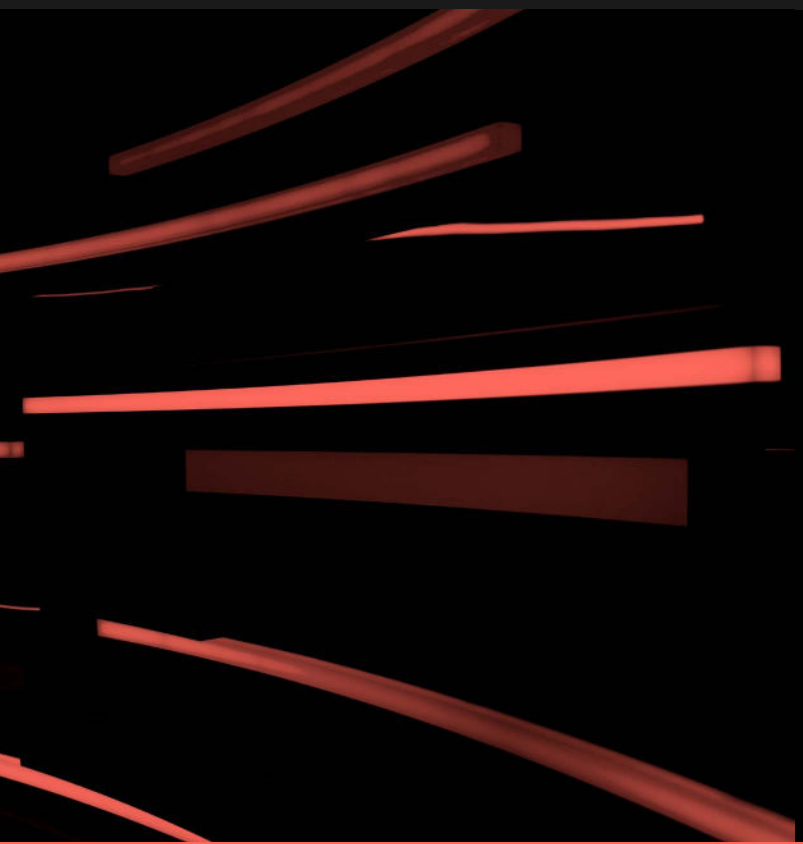
Usable with any tooling, assessment method, or internal security program.

Practitioner-Informed

Incorporates real-world experience from practitioners securing Salesforce environments.

Code-Ready Format

Available in structured XML for vendors to build automated scanners, compliance dashboards, and reporting tools.



Versioning and Governance

Semantic Versioning

SBS follows semantic versioning to ensure stability and predictability for security programs.

Transparent Updates

As Salesforce evolves, controls are reviewed and updated with clear revision notes.

Public Documentation

All changes are documented transparently through the public specification repository.

Community Input

Governance processes prioritize consistency, backward compatibility, and community feedback.

Authors

The Security Benchmark for Salesforce is developed by the following authors. Editorial direction is centralized under a Chief Editor to ensure consistency, coherence, and long-term integrity of the benchmark.

Participation as an author is in an individual, professional capacity. The Security Benchmark for Salesforce is an independent initiative and is not owned, controlled, sponsored, or endorsed by the employers of its authors. The views expressed reflect the professional judgment of the individual authors and not those of their respective organizations.

Pablo Gonzalez
Director of Product, AutoRABIT
Chief Editor. Product management and security architecture experience in DevSecOps and Salesforce platform security.

Jannis Schreiber
Technical Architect, The Mobility House
IT management and software engineering experience with focus on enterprise Salesforce implementations and sustainable technology solutions.

Jakub Stefaniak
Salesforce CTA & CTO, Aquiva Labs
Technical architecture and executive leadership experience with expertise in AppExchange product development and platform security.

Anderson Anthony
Salesforce Security Consultant
Salesforce security administration experience specializing in governance, risk management, and compliance for regulated environments.

Justin Hazard
CISO, AutoRABIT
15+ years of information security experience from SOC operations to executive security leadership, with focus on building security teams and developing security professionals.

John Crimmings
Senior Principle, Slalom
Seasoned Salesforce architect with deep expertise in enterprise security design, data protection strategies, and building secure, scalable platform solutions.

Scott Covert
Founder, Tython
14+ years of Salesforce platform development experience, specializing in cloud computing solutions, application development, and product leadership on the Force.com platform.

Lawrence Newcombe
Salesforce CTA, GiveClarity
Technical and solution architecture experience specializing in nonprofit sector transformation programs, AppExchange product development, and complex security implementations including identity and integration.

Salah Mansour Akridiss
Salesforce Architect,
Banque Internationale à Luxembourg
Salesforce technical architecture experience with focus on platform security, enterprise implementations, and secure solution design for regulated financial services.

Doug Merrett
Founder, Platinum7
13 years of experience at Salesforce with deep expertise in platform security, compliance, and resilience across enterprise environments.

Mika Ståhlberg
Co-founder & CTO, Valo
20+ years of cyber security and software engineering leadership, with expertise spanning AI-driven cloud solutions, low-level forensics, security governance, and Salesforce integration architecture.