

# Qualifying ServiceNow as a Vendor

The ServiceNow Trust Journey

## Introduction

## Why certification matters

### GDPR

## Overview of certifications and attestations

### ISO/IEC 27001:2013

### ISO/IEC 27017:2015

### ISO/IEC 27018:2014

### SSAE 18 SOC 1 and SOC 2 reports

### FedRAMP JAB High authorization

### DoD Impact Level 4 authorization

### Privacy Shield compliance

### Multi-Tier Cloud Security Standard for Singapore (MTCS) Level 3

### ASD IRAP Certified Cloud Service

## Summary

# Introduction

Earning and maintaining trust is essential to building successful partnerships. ServiceNow believes that it is important for customers to have complete confidence in our ability to prevent and mitigate security threats, protect the confidentiality, integrity, and availability of their data, and to help them comply with a growing number of global standards. We have made significant investments in technology, processes, and expertise to ensure that our cloud services meet the most stringent global standards for performance, scalability, security, privacy, and compliance.

The most effective way of demonstrating this to our customers is through the process of independent certification and accreditation. This document gives an overview of the different standards around the world that ServiceNow complies with, followed by a brief description of their value and context.

## Why certification matters

Every year ServiceNow is rigorously audited by independent third-party companies and government bodies to prove that we comply with various global and regional standards governing information security. Each audit represents not just a 'tick in the box', but a significant commitment and ongoing effort; each one involves thousands of point-in-time and ongoing assessments covering every aspect of our information security program and efforts.

Our accreditors are experts in their respective fields with a deep understanding of the different global and regional laws and standards that must be complied with. They thoroughly assess ServiceNow's processes and controls against these standards, verifying that they are met or exceeded at all times. We give them unfettered access and encourage them to fault us so that we may improve. When the audit reports are complete, we make them available to customers.

All of this means that customers can be confident that ServiceNow consistently demonstrates excellent security controls and practices. It reduces the need for customers to generate and assess large quantities of detailed questions on these topics, as multiple well-qualified, independent assessors regularly do this on their behalf.

### GDPR

The General Data Protection Regulation (GDPR) is not listed below because GDPR is not a standard—it is a regulation, i.e. a law, and ServiceNow complies with the law in all jurisdictions in which it operates. ServiceNow has found transition to GDPR compliance a relatively pain-free process. It is not yet possible to achieve certification against GDPR, but ServiceNow will consider that in future should it become possible.

## Overview of certifications and attestations

Introduction

Why certification matters

GDPR

Overview of certifications  
and attestations

ISO/IEC 27001:2013

ISO/IEC 27017:2015

ISO/IEC 27018:2014

SSAE 18 SOC 1 and  
SOC 2 reports

FedRAMP JAB High  
authorization

DoD Impact Level 4  
authorization

Privacy Shield  
compliance

Multi-Tier Cloud Security  
Standard for Singapore  
(MTCS) Level 3

ASD IRAP Certified Cloud  
Service

Summary

Certification	Description	Industry	Geography
ISO/IEC 27001:2013	Specifies information security management best practices and controls	All industries	International
ISO/IEC 27017:2015	Implementation of cloud-specific information security controls	All industries	International
ISO/IEC 27018:2014	Securing personally identifiable information (PII) in the cloud	All industries	International
SSAE 18 SOC 1 Type 2 Report	Protecting the confidentiality and privacy of information in the cloud that affects the financial reports of customers	All industries	International
SOC 2 Type 2 Report	Focuses on controls that are relevant to security, availability, processing integrity, confidentiality, or privacy	All industries	International
FedRAMP JAB High p-ATO	US government-wide program that provides a standardized approach for assessing, monitoring, and authorizing cloud computing products and services	US Federal Government	United States Federal
DoD Impact Level 4 Authorization	US government baseline for security requirements for cloud service providers that host DoD/IC information	US Department of Defense/ Intelligence Community	United States Federal
Privacy Shield Frameworks	Sets out standards regarding the safe transfer of data between the EU/Switzerland and the US	All industries	International
Multi-Tier Cloud Security Standard for Singapore (MTCS) Level 3	Certifies the adoption of sound risk management and security practices for cloud companies	All industries	Singapore
ASD IRAP Certified Cloud Service	Helps Australian government agencies effectively engage and consume cloud-based solutions.	Australian Federal Government	Australia

## Introduction

## Why certification matters

### GDPR

## Overview of certifications and attestations

### ISO/IEC 27001:2013

### ISO/IEC 27017:2015

### ISO/IEC 27018:2014

### SSAE 18 SOC 1 and SOC 2 reports

### FedRAMP JAB High authorization

### DoD Impact Level 4 authorization

### Privacy Shield compliance

### Multi-Tier Cloud Security Standard for Singapore (MTCS) Level 3

### ASD IRAP Certified Cloud Service

## Summary

## ISO/IEC 27001:2013

The ISO/IEC 27001:2013 certification specifies security management best practices and controls based on the ISO/IEC 27002 best practice guide. It ensures that our information security management system (ISMS) is fine-tuned to keep pace with changes to security threats, essential in the fast-paced world of IT security.

Re-certification is obtained by audit every three years, inclusive of an annual surveillance audit order to prove that ServiceNow:

1. Has designed and implemented a comprehensive ISMS.
2. Has adopted a continuous risk management process to ensure that the appropriate information security controls are in place to meet an evolving threat landscape and risks.
3. Systematically evaluates information security risks appropriately, taking into account several factors, including the impact of company threats and vulnerabilities.

ServiceNow has been an ISO/IEC 27001 certified organization since 2012 and the certificate is available [here](#).

## ISO/IEC 27017:2015

The ISO/IEC 27017:2015 standard is concerned with the implementation of the cloud-specific information security controls specified in ISO/IEC 27002.

The certification is gained by an annual independent audit and ServiceNow has been an ISO/IEC 27017:2015 certified organization since 2018.

## ISO/IEC 27018:2014

The ISO/IEC 27018:2014 is a code of practice based on ISO/IEC 27002 and is concerned with the protection of personally identifiable information (PII) in public clouds in accordance with the privacy principles in ISO/IEC 29100.

The certification is gained by annual independent audit and ServiceNow has been an ISO/IEC 27018:2014 certified organization since 2016.

## SSAE 18 SOC 1 and SOC 2 reports

The Service Organizational Control (SOC) framework is an attestation that ServiceNow meets the required standard regarding having controls in place to protect the confidentiality, integrity and availability of our customers' data in the cloud.

- SOC 1 focuses on the effectiveness of internal controls that affect the financial reports of customers
- SOC 2 evaluates controls that are relevant to availability, integrity, security, confidentiality, or privacy.

ServiceNow is audited annually by a third party and has maintained its SSAE 18 SOC 1 Type 2 attestation since 2011 (SSAE 18 superseded SSAE 16 in 2017). SSAE 18 is aligned with international standard ISAE3402 and replaced the now-deprecated SAS70.

ServiceNow has also undertaken an annual SOC 2 Type 2 attestation since 2013, relevant to security and availability controls listed in the AICPA Trust Services Criteria (TSC).

A SOC 1 Type 2 bridge letter is provided between audit periods so that the company is covered for the entire year. This bridge letter is available via [ServiceNow CORE](#) to ServiceNow customers at the end of every January.

## FedRAMP JAB High authorization (for US government entities)

ServiceNow is honored to have achieved the U.S. Federal Risk and Authorization Management Program Joint Authorization Board p-ATO (FedRAMP JAB) at the High level. This enables us to accelerate the adoption of our secure cloud solutions by US federal agencies and provides a standardized approach for assessing, monitoring, and authorizing cloud computing products and services under the Federal Information Security Management Act (FISMA).

ServiceNow received its JAB High Provisional Authority to Operate (p-ATO) in 2019. The FedRAMP JAB High p-ATO also meets the requirements for DoD Impact Level 4.

Introduction

Why certification matters

GDPR

Overview of certifications  
and attestations

ISO/IEC 27001:2013

ISO/IEC 27017:2015

ISO/IEC 27018:2014

SSAE 18 SOC 1 and  
SOC 2 reports

FedRAMP JAB High  
authorization

DoD Impact Level 4  
authorization

Privacy Shield  
compliance

Multi-Tier Cloud Security  
Standard for Singapore  
(MTCS) Level 3

ASD IRAP Certified Cloud  
Service

Summary

## DoD Impact Level 4 authorization (for US DoD/IC entities)

DoD Impact Level 4 authorization facilitates the procurement of ServiceNow products by the US Department of Defense (DoD) and Intelligence Community (IC). It sets out a baseline standard defined by the Defense Information System Agency (DISA) in the Security Requirements Guide (SRG) for cloud computing.

In 2019, ServiceNow obtained its DoD Impact Level 4 (IL-4) authorization. The IL-4 standard is based on FedRAMP High controls, as well as addition controls defined by DISA.

## Privacy Shield compliance

ServiceNow complies with the EU U.S. Privacy Shield Framework and the Swiss – U.S. Privacy Shield Framework set forth by the United States Department of Commerce with respect to the collection, use, and retention of personal data transferred from the European Union and the United Kingdom, and Switzerland to the United States, respectively. To learn more about the Privacy Shield Framework, please visit the Department of Commerce's dedicated Privacy Shield website, located [here](#).

## Multi-Tier Cloud Security Standard for Singapore (MTCS) Level 3

MTCS Level 3 is a certification that ensures that ServiceNow meets standards regarding the confidentiality and integrity of our customers' data in the cloud for Singapore. It builds upon ISO/IEC 27001 and covers the sovereignty, retention, and availability of data, along with business continuity planning and disaster recovery.

ServiceNow is proud to have achieved MTCS Level 3, the highest level of certification available.

## ASD IRAP Certified Cloud Service

Being an ASD IRAP Certified Cloud Service enables ServiceNow to effectively engage with Australian government agencies in order for them to use the Now Platform®. This certification standard is set by the Australian Signals Directorate (ASD) which is an intelligence agency in the Australian government's Department of Defense.

ServiceNow is proud to have gained ASD Certification in 2017 and has been issued with an ASD Certification Letter and Certification Report accordingly.

## Summary

ServiceNow holds itself to extremely high security standards and we aim to be transparent about our efforts and our achievements. The best way to achieve this transparency is by inviting continuous assessment against multiple robust international and regional standards, to ensure that our customers' data is in safe hands.