ServiceNow security for financial services

Understanding the security, resilience, and compliance of the Now Platform®
Table of contents

Introduction .................................................................................................................................................. 3
Business requirements ................................................................................................................................. 3
Concerns and risks .................................................................................................................................. 3
  Operational resilience .............................................................................................................................. 3
  Security challenges ................................................................................................................................. 4
How does ServiceNow help? ..................................................................................................................... 4
  Qualification ........................................................................................................................................ 5
  PCI DSS ................................................................................................................................................ 6
The General Data Protection Regulation (GDPR) ..................................................................................... 7
  Security controls and features ................................................................................................................ 7
Mobile apps ............................................................................................................................................. 8
Conclusion ............................................................................................................................................... 9
Resources ............................................................................................................................................... 9
Introduction

The financial services industry operates in a unique business environment with very particular requirements. The need to handle large volumes of sensitive and valuable data in line with the high levels of regulation makes service provision critical but also very challenging. Software as a Service (SaaS) solutions can be attractive to financial services organizations which prioritize efficiency, flexibility, and scalability. However, this is often tempered by the need to ensure security and compliance: there are many strict criteria varying from location to location which must be continually fulfilled.

ServiceNow offers an ideal solution for financial services organizations because security is a foundation of the Now Platform, along with scalability and resilience. It has a strong track record with financial services customers, backed up by excellent regulatory compliance, as demonstrated by the attestations and certifications we have achieved.

Together with the ServiceNow Assurance Pack (SNAP), this document helps you to understand how ServiceNow operates a reliable and secure service, the standards we uphold, and the processes and mechanisms we use to ensure that the Now Platform and your data are kept safe.

Business requirements

The business environment in this sector is constantly changing and the advent of FinTech startups and challenger banks means that efficiency and agility are increasingly important. It is essential that organizations reduce costs and complexity to enhance their competitiveness. Minimizing management overheads for systems and infrastructure is key, along with rapid, simplified service development and implementation.

Innovation in services and user experience is vital for attracting and retaining customers. The shift to online and mobile banking is a good example of how this can be achieved, delivering convenience and novel features in tandem with business efficiency. The next step in this process is to provide open services and integration with new platforms and applications, even those from third parties.

Replacing out-of-date systems and infrastructure for performance and reliability is a significant and continual undertaking. Ideally this should be performed with an eye to streamlining business processes and improving service efficiency. But these benefits come with the challenges of delivering services at potentially global scale with the highest levels of reliability and security.

Concerns and risks

Financial services organizations are understandably concerned about the risks associated with information security and the potential for compromise of the confidentiality, integrity, and availability of financial information.

A breach could have far-reaching consequences, including reputational impact, compliance failures, and theft (of data or capital). Any of these consequences could in turn have a negative effect on an organization’s perception of trustworthiness. Failure to comply with data protection laws and regulations such as GDPR, CCPA, GLBA, PSD2 could result in severe financial penalties or even the loss of rights to operate. Theft and fraudulent activity could lead to misappropriation of funds – and perhaps more importantly, loss of customer data. All of these could adversely affect customer retention and business relationships.

Operational resilience
The US Federal Reserve defines operational resilience as “the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies” such as acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters.

Operational resilience and service availability are critical for any financial services organization. As many recent high-profile cases in the UK and the US have demonstrated, the longer any service disruption continues, the greater the resulting financial impact and loss of trust. This topic has become so important that many financial services regulators have or are planning regulations requiring ongoing review of supplier arrangements for security, risk, and operational resilience.

- In the UK in late 2019, the Bank of England, the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA), proposed a stronger regulatory framework promoting operational resilience of regulated firms.
- A 2019 consultation paper from The Australian Securities & Investments Commission (ASIC) outlined new operational resilience requirements for securities and futures market operators and participants.
- The German Federal Financial Supervisory Authority (BaFin) published supervisory guidance for financial institutions and insurance companies regarding ensuring appropriate resilient architectures for critical systems during the latter part of 2018.
- The US Federal Reserve also offers guidance to US-based financial services organizations across a number of technology areas, including operational resilience.

Security challenges

Systems and data are the foundations of financial services and must be protected against inappropriate access, but this is not straightforward to achieve, due to both internal and external factors.

Security and risk management is challenging, particularly for large organizations with complex structures. It can be difficult to maintain state-of-the-art defense, controls, and oversight of data security, particularly with layers of complex technology, information overload, and resourcing challenges. Legacy systems add to the challenge, as in some cases they cannot be adequately secured—either because they can no longer be updated to the latest security standards, or because of the risks associated with making changes to functioning, critical systems. Even if the technology is under control, promoting a culture of security among users and customers is essential, as they can present a high level of risk in themselves.

Added to this are the many complex issues around regulatory compliance, particularly when operating across multiple geographical regions. Requirements in Germany may be very different from those in Japan, for example; regulations vary even within the United States.

There is also variance across industries. Services operating in or related to finance have specific, more stringent requirements than other sectors, such as those mandated by PCI-DSS.

How does ServiceNow help?

ServiceNow can help with all of these challenges. The Now Platform provides a highly flexible, scalable, and reliable offering which can be used to deliver services to large numbers of users across regions and operating platforms, including mobile. Security and reliability are foundational elements of the system. Our security organization comprises around 150 personnel globally and implements a comprehensive security program under the oversight of the chief information security officer (CISO). We go to great lengths to ensure the security of the service we provide, and an array of certifications and attestations demonstrate that we meet stringent
regulations across the world. Our robust service-level agreements (SLAs) give customers confidence in our ability to meet their needs.

**Qualification**

ServiceNow is committed to a best practice approach to information security which benefits all of our customers and all of their data. To this end, ServiceNow has implemented a cybersecurity program and policies based on the ISO/IEC 27002:2013 code of practice and has been assessed by a qualified third-party body as an ISO/IEC 27001:2013 certified organization. The certification also applies to the services we provide to our customers.

We hold a range of security and privacy certifications and attestations. These require demonstrably high standards and regular verification via third-party audit of our practices and processes. These provide evidence of ServiceNow’s commitment to risk reduction and security for our customers. Further detail can be found in the [Qualifying ServiceNow as a Vendor eBook](#).

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

The Payment Card Industry Data Security Standard (PCI-DSS), is a propriety information security standard for organizations that process, store, or transmit cardholder data (CHD). This includes those defined by the standard as payment brands, merchants, and service providers. At a high level, PCI-DSS is concerned with appropriate controls and best practice in specific relation to protecting payment card information.

ServiceNow is not a processor, merchant, or service provider in PCI terms and does not itself store or process any cardholder information.

Nevertheless, our overall security stance means we address many of the concerns. Here is a summary of the 12 requirements from PCI-DSS version 3.2.1 and the controls and measures ServiceNow has in place to address them. These apply well beyond this specific standard and should be expected in any high-security environment.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>How ServiceNow meets it</th>
</tr>
</thead>
</table>
| 1. Install and maintain a firewall configuration to protect cardholder data | - Network firewalls at public ingress points filter network traffic based on protocol and destination  
- Host-based firewalls on systems hosting customer data |
| 2. Do not use vendor-supplied defaults for system passwords and other security parameters | - Own configurations and credentials applied to infrastructure systems  
- Vendor defaults not retained  
- ServiceNow instance default credentials are customer-configurable |
| 3. Protect stored cardholder data | - Field-level data encryption facilities  
- Customer-defined retention periods for data records  
- The ServiceNow Assurance Pack (SNAP) provides more information on data security |
| 4. Encrypt transmission of cardholder data across open, public networks | - All data sent over public networks encrypted with TLS  
- Opportunistic TLS available for email sent to or from ServiceNow instances  
- Encryption options available to customers when transmitting CHD from instances to external systems |
| 5. Protect all systems against malware and regularly update anti-virus software or programs | - Anti-malware software on all service-supporting systems  
- Frequent malware signature updates  
- Instances can scan uploaded documents for malware |
| 6. Develop and maintain secure systems and applications | - Platform developed with security best practice from e.g. OWASP (incl. Top 10) and NIST in Secure Software Development Lifecycle (SSDLC)  
- Infrastructure implemented with principle of least privilege |
More information on ServiceNow’s approach to data security, including personally identifiable information (PII) and sensitive personal information (SPI), is discussed further in the Safeguarding Your Data eBook.

The General Data Protection Regulation (GDPR)

The GDPR is designed to protect and enable the privacy rights of EU citizens. The GDPR establishes global privacy requirements governing how personal data is managed and respected while respecting individual choice, regardless of where data is sent, processed, or stored.

ServiceNow believes the GDPR is an important step forward for clarifying and enabling individual privacy rights. We understand that GDPR compliance is a shared responsibility. This is why ServiceNow is committed to be GDPR compliant across our enterprise cloud services.

More information on this topic is available in the whitepaper Preparing for the GDPR.

Security controls and features
The Now Platform provides a range of facilities to allow you to implement your organization’s information security policies and meet the requirements for any applicable legislation. Examples can be seen in the table below.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Summary</th>
<th>Key Features</th>
<th>More details</th>
</tr>
</thead>
</table>
| Availability           | Ensuring that services and data are available for use at all times      | • Advanced High Availability (AHA) architecture  
                             • Regional, paired DCs  
                             • Multi-instance architecture                                       | Delivering Performance, Scalability, and Availability                           |
| Encryption             | Protecting data while in use, in storage and during transmission        | At Rest  
                             • Full Disk  
                             • Column  
                             • Data Base (DBE)  
                             • Edge                                                     | Data Encryption with ServiceNow                                                 |
|                        |                                                                         | In Transit  
                             • HTTPS (TLS 1.2)                                               |                                                                                |
| Compliance             | Following high security and privacy standards in technology and processes | • Regular third-party auditing and attestation                                                 | Qualifying ServiceNow as a Vendor                                              |
| Vulnerability Management| Reducing security risk from software flaws                           | • ServiceNow Patching program  
                             • Annual customer penetration tests |                                                                                |
| Authentication         | Confirming user identity before allowing access to service and data    | • Local accounts  
                             • LDAP integration  
                             • SAML integration  
                             • Multi-factor auth (MFA)                                      | Securing the Now Platform                                                      |
| Authorization          | Controlling levels of access to services and data                      | • Access control lists (ACL)  
                             • Role-based access controls (RBAC)                           |                                                                                |
| Data lifecycle         | Managing treatment of data from creation, use and destruction          | • Data classification, retention and disposal policies                                           |                                                                                |
| Logging                | Activity recording and analysis                                        | • System and database logs  
                             • Table auditing  
                             • Syslog output  
                             • SIEM integration                                              | Safeguarding Your Data                                                         |
| ServiceNow Access to Data | Preventing unauthorized data access by ServiceNow                   | • ServiceNow Controlled Access (SNCA)  
                             • ServiceNow Access Control Plugin (SNAC)  
                             • High Security Plugin (HSP)                                     | Data Access Controls                                                          |

Mobile apps

© 2020 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, Now Platform, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries. Other company and product names may be trademarks of the respective companies with which they are associated.
ServiceNow provides native mobile apps for iOS and Android. These apps allow the Now Platform’s powerful functionality to be easily accessed from smartphones and tablets. The mobile apps employ OAuth 2.0 and the authentication mechanisms (including MFA) that customers already use with ServiceNow, plus AppAuth. Mobile users are subject to the same access controls as other users. All data in transit is protected with TLS, and no customer data is stored on the mobile device by default.

**Conclusion**

Financial services organizations have particular requirements for IT services and data protection, driven by risk and compliance factors. This can lead to a reluctance to use cloud services because of stringent regulatory requirements and concern for the security of customer data and funds.

The Now Platform is designed and operated with security and resilience as the highest priority, with appropriate policies, controls and processes in place. We maintain a range of certifications and attestations which qualify us to operate in this industry, and the loyalty of our existing financial services customers demonstrates that we meet their needs and can be trusted to protect financial services data.

**Resources**

- [How to contact ServiceNow](#)
- [ServiceNow Assurance Pack (SNAP)](#)
- [ServiceNow Governance Risk & Compliance in Financial Services](#) (Webinar)
- [Trust and Compliance Center](#)
- [Compliance Operations Readiness Evidence Portal](#)
- [Security Resource Center](#)
- [www.servicenow.com](#)