ServiceNow: A Secure Platform to Transform Financial Services

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

Introduction 3
Business context 3
Concerns and risks 3
  Overview 4
  Operational resilience 4
  Material outsourcing and concentration risk 5
  Regulatory oversight of outsourcing in Europe 5
  Security challenges 6
ServiceNow: A Trusted Platform for Financial Services 7
  A resilient and scalable architecture 7
  Compliance with global standards 8
  The General Data Protection Regulation (GDPR) 9
  PCI-DSS 10
  Security controls and features 10
Financial Services Workflows 11
  Workflows with embedded compliance 11
  Securing client and financially sensitive data on ServiceNow 12
How we use our own products 14
Conclusion 15
Resources 15
Appendix A: Contractual Addendum for Financial Services 16
Appendix B: Financial Services Regulations in Europe 17
  EIOPA Guidelines 17
  FCA Guidelines 17
  PRA Guidelines 17
Introduction

The Financial Services industry operates in a unique business environment with very particular requirements. Providing critical services that handle large volumes of sensitive and valuable data while meeting strict regulations for security and privacy can present significant challenges.

Software as a Service (SaaS) solutions can be attractive to Financial Services organizations who prioritize efficiency, flexibility, and scalability. However, any benefits must be considered from a security and compliance perspective: there are many criteria to be met, and these can vary across borders.

ServiceNow’s offerings present an ideal solution for Financial Services organizations because security, along with scalability and resilience form the foundations of the Now Platform. We have a strong track record of serving a number of Financial Services customers, and this is backed up by excellent regulatory compliance – as demonstrated by the attestations and certifications we have achieved.

This document is designed to be consumed alongside the ServiceNow Assurance Pack (SNAP), and will first examine the challenges faced by Financial Services organizations, then explore how ServiceNow can help to address them to ensure that your data is safe within the Now Platform.

Business context

This sector is one of the most heavily regulated in the world, and the business environment changes constantly. The advent of FinTech startups and challenger banks means that efficiency and agility are increasingly important—but these must be balanced with regulatory compliance.

Organizations must reduce costs and complexity to enhance their competitiveness. Minimizing management overheads for systems and infrastructure is key—along with rapid, simplified, development and implementation of new services.

Innovation in services and user experience is vital for attracting and retaining customers. The shift to personalized digital banking is a good example of this—giving customers new features and convenience, while at the same time improving business efficiency. There is further opportunity in providing open services—allowing integration with new platforms and applications—including those from third parties. Organizations that embrace transformation will thrive on the speed, extensibility and adaptability to future change that it brings—allowing them to distinguish themselves from their peers.

Improving performance and reliability is a significant ongoing challenge, and often means replacing out-of-date systems and infrastructure. This process can also be an opportunity to streamline business processes and improve service efficiency, but any benefits must be balanced with the need to deliver services at a global scale with the highest levels of reliability and security.

Concerns and risks

This section describes some of the regulatory, compliance and security challenges that arise in the areas of resilience, outsourcing, oversight and data security. We will then address how ServiceNow can help with these issues in: ‘ServiceNow: A Trusted Platform for Financial Services’.
Overview

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 system breach could have far-reaching consequences, including reputational impact, compliance and regulatory impact, and theft (of data or capital). Any of these could in turn have a negative effect on an organization’s perceived trustworthiness. Failure to comply with data protection laws and regulations such as the GDPR, CCPA, GLBA, PSD2 could result in severe financial penalties or even the loss of rights to operate. Fraudulent activity could lead to misappropriation of funds—and perhaps more importantly, loss of customer data. All of these can 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” e.g. acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters. These concerns apply equally to more mundane, everyday events like power outages, equipment failures, software issues and problems caused by human error.

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 means that service providers must demonstrate comprehensive and effective Business Continuity Planning and Disaster Recovery capabilities.

This topic has become so important that many financial services regulators have introduced—or are planning—regulations that require the 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.
- Towards the end of 2018, the German Federal Financial Supervisory Authority (BaFin) published supervisory guidance for financial institutions and insurance companies to ensure appropriately resilient critical systems architectures are used.
- The US Federal Reserve also offers guidance to US-based financial services organizations across a number of technology areas, including operational resilience.

ServiceNow’s proven high levels of service reliability should alleviate these concerns for Financial Services customers. The Now Platform provides customers with the processes and controls necessary to implement their operational resilience programs.

ServiceNow is uniquely able to offer multiple solutions on a single integrated platform, built around a high-quality business and technology service data model. These include: SecOps, Integrated Risk Management (IRM), IT Service Management (ITSM), CloudOps, Business Continuity Management/Business Continuity Planning (BCM/BCP), Vendor Risk Management (VRM) and Customer Service Management (CSM). In particular, IRM on the Now Platform allows customers to tightly couple risk to controls to resiliency planning. More information is available in our Operational Resilience Solution Brief.
Material outsourcing and concentration risk

Another important consideration is Material Outsourcing. The FCA defines Material Outsourcing as “…outsourcing services of such importance that weakness, or failure, of the services would cast serious doubt upon the firm’s continuing satisfaction of the threshold conditions or compliance with the Principles.”

This obligates Financial Services organizations to understand the implications of using 3rd parties (who may themselves outsource certain functions), to help deliver key parts of their service, and to notify the authorities of such dependencies.

Similarly, in its ‘Guidance for firms outsourcing to the ‘cloud’ and other third-party IT services’, the FCA highlights Concentration Risk (the vulnerability of an organization to the failure of any 3rd party that it may depend on for delivery of significant proportions of its services).

“In our guidance, this term refers to our expectation that firms should monitor any reliance they themselves have on a single provider, consider the action they would take if this provider failed, and whether any concentration risk is within their risk tolerance.”

This could include providers like ServiceNow and means that Financial Services Organizations require a high degree of confidence in a provider’s viability—both in the financial strength of the business and in the technical resilience of its services. This confidence relies on service providers being transparent about service availability (including related processes and mechanisms) and regulatory compliance. A strong track record of providing reliable services for similar organizations is also beneficial.

ServiceNow’s in-house service delivery does not rely on subcontractors. Our customers’ confidence in our proven resilience and availability allows them to entrust their most critical operations to our platform and services.

The Now Platform provides a single source of truth for operational and technical data. An integrated data model combined with a secure, reliable platform significantly reduces the typical risks associated with the legacy, fragmented technology systems. It also provides increased efficiency through process streamlining.

We have recently released an integrated Business Continuity Management (BCM) suite, to assist customers in the event of major disruption.

Regulatory Oversight of Outsourcing in Europe

Recently, financial regulators including the European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) and UK’s FCA and PRA have issued new guidance regarding outsourcing arrangements, with relevance to cloud services.

ServiceNow is not a financial institution so does not fall under the scope of these guidelines.

However, ServiceNow recognizes that companies in all industries are challenged to address a growing number of evolving regulatory requirements and is committed to helping its customers navigate the ever-changing regulatory landscape. ServiceNow devotes significant time and resources to delivering assurance to our customers.

European Banking Authority (EBA) Guidelines

The EBA has published new guidelines on outsourcing. These came into effect on 30 September 2019 and impose various requirements applying to outsourcing arrangements entered into, reviewed or amended from that date.
The Guidelines also prescribe risk-mitigating measures and actions in various areas that institutions must take when outsourcing, to ensure that:

- There is effective day-to-day management by senior management or the management body.
- There is effective oversight by the management body.
- Both outsourcing policy and outsourcing processes are sound.
- Institutions and payment institutions have an effective and efficient internal control framework, which also encompasses outsourced functions.
- All risks associated with the outsourcing of critical or important functions are identified, assessed, monitored, managed, reported and, as appropriate, mitigated.
- There are appropriate plans for the exit from outsourcing arrangements of critical or important functions, e.g. by migrating to another service provider or by reintegrating the critical or important outsourced functions.
- Competent authorities remain able to effectively supervise institutions and payment institutions, including the functions that have been outsourced.

Due to their importance, ServiceNow has created an analysis of the EBA guidelines to support our regulated customers by illustrating how ServiceNow’s application, processes and internal controls relate to the EBA’s recommendations. This can help customers obtain or maintain compliance. We are also introducing a Financial Services Addendum to our standard agreements for clarity (see Appendix A for details).

Our Security Office continually reviews other publications targeted at European and UK Financial Services Organizations that have relevance to our customers. However, there is currently no requirement to publish individual responses since we have already addressed the overarching EBA Guidelines (see Appendix B for details).

We can of course help customers that wish to consider any of these guidelines in more detail.

Security challenges

Systems and data are foundational to Financial Services and must be protected against any type of inappropriate access. However, security and risk management are 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 well-managed, fostering a culture of security among users and customers is essential, to reduce the level of risk they may otherwise present.

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.

ServiceNow treats security with the utmost priority, and it is fundamental to our offering. The platform is secure by design and default—and has extensive controls and features so customers can safeguard their data.
ServiceNow: A Trusted Platform for Financial Services

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. Security and reliability are foundational elements of the system. Our security organization comprises almost 200 personnel globally and implements a comprehensive security program under the oversight of the Chief Information Security Officer (CISO). It also includes a Financial Services division to align our risk, security and compliance strategy with that of the industry.

We go to great lengths to ensure our service operates with the high levels of security our customers demand. The Security and Legal teams work together to ensure we comply with the appropriate certifications and attestations to meet stringent regulations across the world. Our robust service-level agreements (SLAs) give customers confidence in our ability to meet their needs.

ServiceNow has a strong track record of serving our Financial Services customers, who benefit from the power and flexibility of the platform and the confidence of working with a very reliable and scalable service. They also appreciate the ability to unify services on a common platform, reduce the complexity from diverse systems, and work with a trusted partner on a shared responsibility model for security. All of this can actually help to increase operational resilience and reduce concentration risk.

Customers procure access to ServiceNow with an annual subscription model, meaning they are not tied-in to the service. We provide transparency about compliance and security through our compliance portal—CORE.

Our 97% customer retention rate indicates high levels of customer satisfaction.

A resilient and scalable architecture

ServiceNow offers world-class performance and reliability. We have built our platform to be superbly reliable and with capacity to support many millions of users across the globe. We own and run all cloud infrastructure other than physical datacenters which host our equipment, and meet the highest operational standards as proven by our various certifications and attestations. We provide full transparency on this to customers through our compliance portal (CORE) and documentation (e.g. SNAP). Almost all development and operational work is handled in-house, which allows us the utmost confidence in the quality of the services we offer.

Some of the key features and capabilities include:

- **Advanced High Availability** – ServiceNow’s Cloud operates from a network of data center locations, globally distributed to accommodate major centers of demand. It is architected for very high reliability and scalability, with no single points of failure. Each datacenter is paired with another in the same region, with each one able to fully accommodate the workload of both if necessary. This, together with our multi-instance-architecture has proven to deliver industry-leading availability over recent years.

- **Multi-instance Architecture** – ServiceNow’s Multi Instance Architecture means that services operate from shared physical infrastructure like routers and servers, but with logically isolated software ‘instances’ comprising an application node and database server. Each customer’s instances are allocated for their exclusive use. To achieve high availability, instances operate in redundant pairs, with each node in a separate DC. Instance pairs operate in an active/standby mode, with data continuously replicated between them. Either node can be made active, seamlessly when required, e.g. for maintenance and upgrades, or in the case of a failure. No downtime occurs because the switching process is fast and fully automated.
• **Business Continuity Planning** – Our Business Continuity and Disaster Recovery planning covers both the internal corporate environment and the separate, isolated customer cloud service. A failure of the corporate network would not impact service provision of Customer instances from the cloud DCs. Plans are fully documented and tested annually as required for compliance, and reports are available to customers.

• **Transparency in Performance and Reliability** – We are confident in the quality and reliability of services we provide, so we can give customers clear service availability metrics, and offer industry-leading Service Level Agreements. These go together with a commitment to Customer Success and outstanding Customer Support—ServiceNow takes any technical issues customers may experience seriously and works to resolve them as quickly and efficiently as possible.

• **Universal Access** – People need the ability to work from anywhere—not just from a desk in an office. The Now platform comes with native mobile apps for iOS and Android, enabling users to access services securely from almost any device. This helps eliminate delays and bottlenecks, and is especially useful for stakeholders who may need to monitor service operation, oversee issues and submit approvals.

  ServiceNow’s mobile apps employ robust authentication (including MFA), and 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.

• **Customer Flexibility** – Customers retain ownership of any data they may store on the Now Platform and can retrieve it at any time for archival or warehousing in secondary storage as required. Service Contracts are renewed annually, giving customers complete flexibility in their decision to use ServiceNow. Our customer retention rates are unmatched in the industry.

Comprehensive information on these topics and more is available on the Trust Site, and in the SNAP documents, in particular the **Advanced High Availability eBook** and **Securing the Now Platform**.

**Compliance with global standards**

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 Compliance section of our Trust Site.
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.

<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 16 SOC 1 Type 2 Report</td>
<td>Protecting the confidentiality and privacy of information in the cloud that affects the financial reports of customers</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>US 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>US 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>
<tr>
<td>ASD IRAP Certified Cloud Service</td>
<td>Helps Australian government agencies effectively engage and consume cloud-based solutions</td>
<td>Australian Federal Government</td>
<td>Australia</td>
</tr>
<tr>
<td>Cloud Computing Compliance Controls Catalog (C3)</td>
<td>Cloud-specific compliance controls catalog developed by the German Federal Office for Information Security (BSI)</td>
<td>All industries</td>
<td>Germany</td>
</tr>
<tr>
<td>Government of Canada Protected-B Cloud Provider</td>
<td>The Canadian Centre for Cyber Security (CCCS) defined data classification level that is approved to be stored within the cloud</td>
<td>Canadian Federal Government</td>
<td>Canada</td>
</tr>
</tbody>
</table>

ServiceNow is committed to high standards of security.
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 as it applies 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.*

Though our service does not come under the scope of PCI-DSS, our existing security program already addresses many of its concerns. We are currently assessing the benefits of obtaining compliance to simplify the issue for our customers. You can find more information on ServiceNow’s approach to data security, including personally identifiable information (PII) and sensitive personal information (SPI) in the [Safeguarding Your Data eBook](#).

**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>
<tbody>
<tr>
<td>Availability</td>
<td>Ensuring that services and data are available for use at all times</td>
<td>• Advanced High Availability architecture</td>
<td><a href="#">Delivering Performance, Scalability, and Availability</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Regional, paired DCs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Multi-instance architecture</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Protecting data while in use, in storage and during transmission</td>
<td><strong>At Rest</strong>&lt;br&gt;• Full Disk Encryption&lt;br&gt;• Column-Level Encryption&lt;br&gt;• Data Base Encryption&lt;br&gt;• Edge Encryption</td>
<td><a href="#">Data Encryption with ServiceNow</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>In Transit</strong>&lt;br&gt;• HTTPS (TLS 1.2)&lt;br&gt;</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td>Following high security and privacy standards in technology and processes</td>
<td>• Regular third-party auditing and attestation</td>
<td><a href="#">ServiceNow Trust Site</a></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Reducing security risk from software flaws</td>
<td>• ServiceNow Patching program&lt;br&gt;• Annual customer penetration tests</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Confirming user identity before allowing access to service and data</td>
<td>• Local accounts&lt;br&gt;• LDAP integration&lt;br&gt;• SAML integration&lt;br&gt;• Multi-Factor Authentication (MFA)&lt;br&gt;• IP address controls</td>
<td><a href="#">Securing the Now Platform</a></td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Financial Services Workflows

Our commitment to the Financial Services industry extends to the unique products and solutions we provide customers on a single enterprise platform. Built on our well-established Customer Service platform, our new Financial Services Operations product enables customers to efficiently route work across their enterprise—to boost visibility, enable compliance, and deliver great service. Financial Services Operations removes the legacy system fragmentation that creates the friction in customer experiences, reducing the complexity and cost of delivering quality differentiated services.

Workflows with embedded compliance

Many processes within Financial institutions are subject to global regulatory control and regular audit—such as complaints, disputes, trade failures and payments. Organizations go to extreme lengths to ensure the compliance of their operations, through the three lines of defense approach, which requires high volumes of data processing and dedicated resources.

ServiceNow has applied first-principles thinking to how organizations can maintain compliance, embed automation into each process and deliver exceptional frictionless customer outcomes in a highly regulated market.

The platform provides five key control capabilities that can ensure the timely, compliant and auditable processing of any customer workflow:

- **Data Control** – The platform Data Policy Management ensures that the completeness and quality of the data captured adheres to strict requirements, which is also mandated through system-to-system integration.

- **Service Level (SLA) Control** – ServiceNow utilizes a powerful service level engine on the platform to intelligently monitor the health and timely delivery of customer cases, and where necessary take corrective action to ensure that regulatory obligations for resolution times are met.
• **Workflow Control** – ServiceNow workflows are data-driven and ‘tuned in’ to the context of the record in real-time. Steps within the workflow may be subject to regulatory control, such as credit risk assessment. The workflow ensures that these steps are completed in the correct sequence and timeframe, and to the required standard to progress. The workflow provides the compliance guiderails for the process.

• **Governance, Risk and Compliance Control** – Uniquely, ServiceNow has an Integrated Risk Management suite on the same platform that drives the processes, and this enables true continuous controls monitoring. On the Now Platform, an organization’s policies and controls for risk-mitigation and compliance inform performance targets for customer workflows. These can detect and correct issues in real time, avoiding reliance on other lines of defense.

• **Auditing and Monitoring Controls** – every action and update in ServiceNow is recorded through immutable logs with alerting for anomalies. Administrators can walk through the history of any customer journey.

A workflow can incorporate and combine different types of controls:

- **Data and security control**: Validates data capture, field transformations, mandatory data requirements, data type enforcement
- **Service-level control**: Monitors service levels for response and resolution—alerts and actions if targets will not be hit
- **Regulatory and policy control**: Monitors the platform data against automated control checks—enacts remediation workflow
- **Workflow control**: Codifies the process into a data-driven workflow—monitors the progress of each activity

These controls help to ensure that any middle or back office workflow process on the platform adheres to regulatory obligations, and a customer’s unique policies and risk strategies.

### Securing client and financially sensitive data on ServiceNow

Trust is the ultimate currency with clients, and so customers must protect their client’s data with every safeguard possible. ServiceNow provides configurable security options for each workflow use case. We maintain a [Security Best Practice Guide](#) to help customers implement an optimal security configuration.

Each ServiceNow account team works closely with their customers to determine how sensitive data point should be secured. We consider the data flows, integrations, reporting, user experience, Business logic, and data classification requirements to recommend the best combination of security controls for the data and use case. Our multi-instance architecture gives customers greater flexibility over the way security controls are implemented to best meet their individual needs.
These methods include:

- **Field Transformation**: ServiceNow can detect a particular type/classification of data and transform its value before it is stored. This could for example truncate a credit card number to the last 4 digits, or mask a transaction ID. This can prevent sensitive data being stored in inappropriate fields.

- **Encrypt-at-rest**: ServiceNow offers 3 types of complementary (layered approach) encryption-at-rest solutions. This includes Database encryption which protects the entire database, Column-Level encryption which protects specific fields and Edge encryption which protects sensitive data before it leaves the customer’s own network and hits the database. Our [Data Encryption e-book](#) provides further details on these and more.

- **Remote Tables**: The Now Platform can connect to third-party sources, or to another instance, to retrieve external data and optionally cache it in memory. You can view external data in lists or forms and process it. You can also group, sort, aggregate, and filter the data just like you would for standard internal tables / data stored in the ServiceNow database.

- **Just-in-time access**: The ServiceNow platform contains an array of industry-grade integration options to exchange data with remote sources. These can be called on-demand without the need to store the data which can then be displayed in form or Service Portal widgets.

An individual data point can be secured with multiple capabilities:

- Value modified using rule set—such as truncation or obfuscation
- Encrypted before it hits the database
- No persistence of data
- Only lives temporarily in memory
- No persistence of data
- Present through user interface on demand
- Secure REST API services
- Field Transformation
- Encrypt at Rest Database, Column, Proxy (Edge)
- Store in memory Remote tables
- Just-in-time access

Data Point: Account
Further still, the platform offers global security options such as IP whitelisting, granular access controls and industry-grade authentication—all configured and monitored from the Instance Security Center. The flexibility and range of options on offer enables customers to tailor and harden the environment to their own unique requirements and monitor their security posture using metrics through the Instance Security Center.
How we use our own products

Running any large international organization is complex and requires efficient, easy-to-use systems and processes with a degree of automation providing smooth, streamlined workflows. ServiceNow is no exception, and we have a wide range of requirements across the business, ranging from HR to IT, Operations Management to Information Security. Processes like on-boarding new employees or introducing new IT Services require input and data from different departments and diverse systems. These must all come together seamlessly to deliver good business outcomes, e.g. so that a new starter can begin their first day at work with everything in place, whether from HR, Payroll, IT or Facilities.

We believe that the best tools to help with these challenges come from our own stable—the Now Platform, and the products built on it - many of which were developed in response to our own needs for digital transformation. These solutions are tried and tested because we treat ourselves as customer zero. Our Security Operations product was developed to help with our internal data security needs. The DevOps product helps with our platform’s Secure Software Development Lifecycle (SDLC). We even manage our entire customer cloud—comprising over a hundred thousand instances – with our own IT product suite.

Making these capabilities readily accessible to users, including from mobile devices, means that employees can be more self-sufficient and get things done more quickly, making for a better experience and increased efficiency.

Our Business Continuity Management product allows you to identify potential Operational Resilience issues and develop and test your BC plans while integrating existing IT workflows.

More details of how we use our own products are available on the ServiceNow website.

Conclusion

In today’s connected digital online environment, Financial Services organizations are under ever greater pressure from regulators and customers to provide secure, available and scalable services. This must all be achieved cost-effectively to maintain a competitive edge and has led to rapid growth in cloud adoption to help deliver core services.

Customers deserve the highest levels of trustworthiness and transparency from their critical service providers. This has never been more important and is now also becoming a regulatory expectation.

The Now Platform is designed and operated with security and resilience as the highest priority, with appropriate policies, controls and processes in place. ServiceNow maintains a range of certifications and attestations which qualify us to serve the Financial Services industry, and the Now Platform provides ample controls and facilities to fulfill customer security requirements. The loyalty of our existing Financial Services customers demonstrates that we are a trusted partner for enabling services and protecting data.

Resources

How to contact ServiceNow
ServiceNow Assurance Pack (SNAP)
Trust and Compliance Center
Compliance Operations Readiness Evidence Portal
Security Resource Center
Appendix A: Contractual Addendum for Financial Services

ServiceNow wants to make this change to its standard agreements as we know how important it is for our affected customers to comply with these guidelines. The addendum allows financial institutions to clearly see all contractual provisions related to their obligations under the guidelines. Statement from the addendum below for reference:

“This financial services addendum ("FS Addendum") supplements the Agreement and is subject to and incorporated therein by this reference. In the event of any conflict between the terms of this FS Addendum and the terms of the Agreement with respect to the subject matter herein, this FS Addendum shall prevail. Capitalized terms used and not defined in this FS Addendum shall have the same meaning given to them in the Agreement.”

Both the mapping and the addendum drafts are currently under review with likely publish dates of Q3 or Q4 2020.

Appendix B: Financial Services Regulations in Europe

EIOPA Guidelines

The EIOPA published its Final Report on public consultation No. 19/270 in:

“Guidelines on outsourcing to cloud service providers”
Published 31/01/2020.

These Guidelines apply from January 2021 to all cloud outsourcing arrangements entered into or amended on or after this date.

Although only applicable to insurance and re-insurance companies, EIOPA also acknowledge the following in relation to the EBA guidelines:

“The use of cloud outsourcing is a practice common to all financial undertakings and not only to insurance and reinsurance undertakings. Moreover, the main risks associated to this practice are similar across sectors. Acknowledging this, and recognising the potential risks of regulatory fragmentation in this area, EIOPA has considered the most recent guidance published by the European Banking Authority (EBA) on this field: the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) which have incorporated the EBA Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03).”

FCA Guidelines

The FCA have published a number of documents relating to Outsourcing and particularly outsourcing to the cloud. These only apply to UK institutions.

The most relevant of these documents is:

“Finalised guidance - FG 16/5 Guidance for firms outsourcing to the ‘cloud’ and other third-party IT services”
Published 01/07/2016 (Updated Dec 2019) Deadline 1 October 2020.

This clarifies the requirements on firms when outsourcing to the ‘cloud’ and other third-party IT services. The guidance is intended to help all firms to effectively oversee all aspects of the life-cycle of their outsourcing arrangements; from making the decision to outsource, selecting an outsource provider, and monitoring outsourced activities on an ongoing basis, through to exit.
Paragraph 1.8 is notable:

“This guidance is not binding and is intended to illustrate ways in which firms can comply with the relevant rules. We expect firms to take note of the guidance and, where appropriate, use it to inform their systems and controls on outsourcing.”

This guidance does not apply to credit institutions and investment firms subject to the EU Capital Requirement Regulations (EU 575/2013) i.e. Banks, Building Societies and IFPRU investment firms as defined in the FCA Handbook; and payment and electronic money institutions to whom the EBA Guidelines on outsourcing arrangements are addressed.

PRA Guidelines

The PRA has launched a number of consultations on the topics of outsourcing and risk. This is the most applicable to institutions using ServiceNow:

“Consultation Paper | CP30/19 Outsourcing and third party risk management”

The deadline for responses will, in line with the FCA, be extended to 1 October 2020.

This CP is relevant to all UK banks, building societies and PRA-designated investment firms, insurance and reinsurance firms and groups in scope of Solvency II, including the Society of Lloyd’s and managing agents, and branches of overseas banks and insurers.

In this consultation paper (CP), the PRA sets out and invites comments on its proposals for modernising the regulatory framework on outsourcing and third party risk management. The guidance pursues the following objectives:

• Complement the policy proposals on operational resilience in CP29/19 ‘Operational resilience: impact tolerances for important business services’, published simultaneously with this CP.1
• Facilitate greater resilience and adoption of the cloud and other new technologies as set out in the Bank of England (the Bank)’s response to the ‘Future of Finance’ report.
• Implement the European Banking Authority (EBA) ‘Guidelines on Outsourcing Arrangements’ [EBA Outsourcing Guidelines]. The draft Supervisory Statement (SS) clarifies how the PRA expects banks to approach the EBA Outsourcing Guidelines in the context of its requirements and expectations. In addition, certain chapters in the draft SS elaborate on the expectations in the EBA Outsourcing Guidelines.

The PRA will publish its final policy on the proposals in this CP in the second half of 2020 with implementation shortly after.

Certain proposals in this CP, which derive from the EBA Outsourcing Guidelines or, (if adopted in the current form), the draft EIOPA Cloud Guidelines would be subject to longer implementation periods. In particular, those relating to:

• The register of outsourcing arrangements (‘Outsourcing Register’); and
• The revision by:
  • Banks of Outsourcing arrangements entered into before 30 September 2019; and
  • Insurers of Cloud Outsourcing arrangements entered into before 1 July 2020 (‘Legacy Outsourcing Arrangements’) to bring them into compliance with the EBA Outsourcing Guidelines and EIOPA Cloud Guidelines, respectively.