servicenow

ServiceNow Security for the UK Public Sector

How ServiceNow supports the UK Government 'Cloud First Policy' and the NCSC 'Cloud Security Principles'

servicenow

Table of contents

Introduction 3
The UK public sector approach to adopting cloud solutions 3
UK public sector regulatory requirements 4
Historical context: Government Protective Marking Scheme (GPMS) 4
2013 Review of the GPMS and the reclassification of Impact Levels 4
The fundamental changes: Government Security Classifications Policy (GSCP) 5
Overview of the GSCP OFFICIAL classification 6
Baseline security requirements 6
Marking OFFICIAL information 6
The OFFICIAL-SENSITIVE classification 6
Common misconceptions 7
Misconception #1 - UK data must remain within the UK and be accessed only from the UK 7
Misconception #2 - Handling government data requires security cleared (SC) personnel 7
Misconception #3 - Aggregation increases classification level 7
Successful public sector commercial cloud adoption 8
How ServiceNow supports the UK public sector 9
Conclusion 10
Additional resources 10
Appendix A – ServiceNow's response to the UK Government's NCSC Cloud Security Principles 11
Definitions 11
Principle 1 – Data in transit protection 12
Principle 2 – Asset protection and resilience 12
Principle 3 – Separation between users 13
Principle 4 – Governance framework 14
Principle 5 – Operational security 15
Principle 6 – Personnel security 16
Principle 7 – Secure development 16
Principle 8 – Supply chain security 17
Principle 9 – Secure user management 18
Principle 10 – Identity and authentication 19
Principle 11 – External interface protection 19
Principle 12 – Secure service administration 21
Principle 13 – Audit information for users 22
Principle 14 – Secure use of the service 22

servicenow

Introduction

Cloud services present a leap forward in capability and value. They can also present a leap forward in security, but for many organizations, using traditional assurance practices and methodologies intended for on-premise or commercial off-the-shelf software (COTS) solutions that are infrastructure-centric may hinder proper assessment of cloud services.

Effectively evaluating cloud services requires a data-centric approach, rather than one focused on the infrastructure. In this context, responsibilities for infrastructure fall on the cloud service provider – a customer has limited ability to impose their organization's standards, especially in relation to infrastructure.

The UK Government introduced their 'Cloud First Policy' in 2013, and ever since departments have been looking to the cloud to provide effective and scalable solutions to support their business requirements. Several of ServiceNow's customers have asked for our advice in this area and ServiceNow is happy to support customers throughout this process. This document provides an overview of the challenges typically faced by UK public sector and how ServiceNow can be successfully adopted to support the Government's Cloud First Policy.

This document also includes a detailed point-by-point response to the UK Government *National Cyber Security Centre (NCSC)'s 'Cloud Security Principles'* (see 'Appendix A – ServiceNow's response to the UK Government's NCSC Cloud Security Principles').

The UK public sector approach to adopting cloud solutions

The Cloud First Policy states that customers should follow the NCSC Cloud Security Guidance. This guidance discusses Data Separation, the Cloud Security Principles, and Security Responsibilities.

> *"When procuring new or existing services,* public sector organisations should consider and fully evaluate potential cloud solutions first before considering any other option. *This approach is mandatory for central government and strongly recommended to the wider public sector."*[1]

Furthermore, the UK Government also advises:

> *"Your service team must consider cloud purchases before any other options because of the Government's Cloud First Policy"*[2]
>
> *"On balance we think well-engineered SaaS is better for security than the alternatives."*[3]

However, many public-sector bodies have found the adoption of the new policy to be challenging, and there is often some confusion regarding the changes to the UK Government security classification scheme.

Mature cloud assurance guidelines are now available from the NCSC. ServiceNow recommends potential public-sector cloud customers reference all of these documents. They set valuable context for cloud consumers and allow them to ask cloud service providers the right questions, get answers consistent with the guidance, and to show their working to their accreditor:

- NCSC Guidance: Cloud security guidance
- NCSC Blog Post: Debunking cloud security myths

[1] UK Government Cloud First Policy
[2] UK Government Service Manual: Securing Your Cloud Environment
[3] National Cyber Security Centre - Debunking Cloud Security Myths

- NCSC Guidance: Implementing the Cloud Security Principles[4]
- NCSC Guidance: Separation and cloud security

UK public sector regulatory requirements

Historical context: Government Protective Marking Scheme (GPMS)

It is useful to understand how the industry interpreted guidance in the past, in order to fully understand the spirit of what the Government has changed, and why.

The sequence of interpretations made under the previous regime was:

- the automatic linking of Business Impact Levels (BILs) with classifications
- the automatic and inseparable linking of classifications with the infrastructure
- the industry undertaking wholesale infrastructure accreditations to an Impact Level (IL)

The net result was that the industry overcomplicated the interpretation of the new guidance by attempting to accredit infrastructures to Impact Levels. This was never their intended purpose; Impact Levels only ever described the impact of the realization of a risk to an information asset, i.e. if disclosed, altered, or lost.

This led to a downplaying of appropriate information-centric risk assessments. The focus instead turned to the provision and procurement of accredited solutions or infrastructures: organizations accredited the box rather than assuring the individual items in the box.

The industry further complicated things by assuming that aggregated data sets increased the Business Impact Level, which raised the classification, which in turn increased the Impact Level requirement of the underlying infrastructure and the security clearances required to administrate it. This resulted in a lot of pressure to "round-up" classifications and corresponding expense: the more things in the box, the more secure the box needed to be.

2013 Review of the GPMS and the reclassification of Impact Levels

Towards the end of 2012 the UK Government announced that it intended to move to new information classification policy and carried out a review of the Government Protective Marking Scheme (GPMS).

The GPMS Review found a number of issues with the previous classifications, specifically around onerous technology requirements. These led to the use of niche products, which in turn increased pressure on the public purse. The previous classifications also gave rise to a tendency to over-classify data in case of doubt. Organisations were deferring to the mandatory requirements of the National Technical Authority rather than undertaking a self-determined, risk-driven approach.

In April 2014, as a result of these findings, the Cabinet Office reduced the existing six Business Impact Levels (BILs) to three (see table below). This latest guidance is described in the Government (GSCP), which replaces the GPMS.

Before (GPMS)	After (GSCP)
UNCLASSIFIED	-
Impact Level 2 – Protect	OFFICIAL

[4] See 'Appendix A – ServiceNow's response to the UK Government's NCSC Cloud Security Principles'

Before (GPMS)	After (GSCP)
Impact Level 3 – Restricted Impact Level 4 - Confidential	
SECRET	SECRET
TOP SECRET	TOP SECRET

However, it is worth noting that there is no automatic direct mapping between the old scheme's Impact Levels 2, 3, and 4 and the new OFFICIAL classification, and it is certainly not correct to assume that all existing data that was classified Impact Level 2, 3, and 4 is now classified as OFFICIAL.

The GSCP expects that the vast majority of government data will fall under the OFFICIAL classification and need not be marked as such. Where a case for a classification at SECRET or above is not clear, but there is a justifiable requirement for a local distinction, then organisations may use the caveated classification "OFFICIAL-SENSITIVE". Data under this classification must be conspicuously marked as such. However, it does not automatically attract any additional HMG requirement for special handling, logging, or ICT separation. Therefore, any decisions about special handling of that data, apply only within the organisation that made the classification.

Business Impact Levels (BILs) are still relevant, but only in reference to data, not to infrastructure.

The UK Cabinet Office Security Policy Framework (SPF) incorporates the GSCP and presents a substantial shift away from the Government's previous approach of central prescription. It now directs organisations toward assuming responsibility for information risk management themselves, and for the subsequent selection and implementation of appropriate technological controls.

The fundamental changes: Government Security Classifications Policy (GSCP)

The Cabinet Office's Security Policy Framework focuses less on infrastructure-centric risks and more on data-centric risks. This is clear from the key principles in the GSCP document:

1. *All* information that Her Majesty's Government (HMG) needs to collect, store, process, generate or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.
2. *Everyone* who works with government (including staff, contractors, and service providers) has a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.
3. Access to sensitive information must *only* be granted on the basis of a genuine 'need to know' and an appropriate personnel security control.
4. Assets received from or exchanged with external partners *must* be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

The supplier guidance states that:

> *"Departments are required to assess their legacy contracts on a case by case basis, adopting a measured and pragmatic approach to transition to minimize contract changes outside of business cycles."*

This suggests that relevant contracts should be modified *before* the natural termination date, if the opportunity arises and where it is pragmatic to do so. This could potentially save years of

lock-in to legacy compliance for both suppliers and customers. Any changes should be prepared well in advance of any renewal date or the end of a business cycle.

Overview of the GSCP OFFICIAL classification

Note: The Government Security Classification Policy (GSCP) operates according to a number of key principles. This document discusses only those which relate to the OFFICIAL (and OFFICIAL-SENSITIVE) classification within the context of the ServiceNow offering.

Each GSCP classification is an indication of the sensitivity of the information (in terms of the likely impact resulting from compromise, loss, or misuse), and entails a baseline set of personnel, physical, and information security controls that offer an appropriate level of protection against a typical threat profile. The typical threat profile for the OFFICIAL classification is broadly similar to that of a large UK private company with valuable information and services. It anticipates the need to defend UK Government data or services against compromise by attackers with bounded capabilities and resources.

The majority of information that is created or processed by the public sector will fit the OFFICIAL classification, and many departments and agencies will operate exclusively at this level. This includes:

- The day-to-day business of government, service delivery, and public finances
- Routine international relations and diplomatic activities
- Public safety, criminal justice, and enforcement activities
- Many aspects of defence, security, and resilience
- Commercial interests, including information provided in confidence and intellectual property.
- Personally Identifiable Information (PII) that is required to be protected under the Data Protection Act 2018, General Data Protection Regulation (GDPR - Regulation (EU) 2016/679) or other legislation (e.g. in relation to health records)

Some of this information could have negative consequences if lost, stolen, or published in the media, but may not be subject to a heightened threat profile.

Baseline security requirements

- All HMG information must be handled with care to prevent loss or inappropriate access, and to deter deliberate compromise or opportunist attack
- Staff must be trained to understand that they are *personally responsible* for securely handling any information that is entrusted to them, in line with local business processes
- Baseline security controls reflect commercial good practice

Marking OFFICIAL information

There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes.

The OFFICIAL-SENSITIVE classification

A limited subset of OFFICIAL information could have more damaging consequences for individuals, an organisation, or government if it were lost, stolen, or published in the media. This subset of information should still be managed within the OFFICIAL classification tier but may attract additional measures (generally procedural or personnel-related) to reinforce its "need to

know" nature. In such cases where there is a *clear and justifiable requirement* to reinforce the "need to know" sensitivity, assets should be conspicuously marked "OFFICIAL–SENSITIVE".

Common misconceptions

Misconception #1 - UK data must remain within the UK and be accessed only from the UK

Data Protection regulations such as the EU GDPR and UK Data Protection Act (the UK implementation of GDPR) include provisions for data transfers. In the case of the Data Protection Act, transfers can include those to "third countries" outside of the UK.

ServiceNow customer data is not routinely transmitted or stored outside of the customer's chosen data center region. For the UK region, customer data centers are located in Newport, Wales and London (Slough), England. Customer data remains hosted within these location in the UK at all times.

However, incidental data transfers in conjunction with support activities undertaken by ServiceNow personnel from outside the UK may occur occasionally under these circumstances. This possibility is stated in the contractual agreements ServiceNow signs with its customers.

ServiceNow is also able to contract that its provisions regarding data transfers are adequate through the use of Standard Contract Clauses (SCC), also known as EU Model Clauses.

Regional changes to the statutory and regulatory frameworks and legislation (e.g. those resulting from the UK exit from the European Union) are continuously monitored. Any changes to requirements identified as relevant will be addressed to ensure ServiceNow's offerings remain compliant in all relevant jurisdictions.

Misconception #2 - Handling government data requires security cleared (SC) personnel

OFFICIAL classification requires only Baseline Personnel Security Standard (BPSS)[5], or equivalent security clearance, not the more stringent 'SC' or 'SC Cleared'.

The Government found that Risk Assessors routinely determined infrastructure to have a higher level of classification than the data it contained, due to aggregation[6,7]. This resulted in an unnecessary increase in the level of Security Clearance required.

ServiceNow's staff are background cleared to a standard equivalent to or exceeding BPSS, e.g., requiring 5 years of full background checks as opposed to 3 years of employment checks only. It is on this basis that customers using ServiceNow for OFFICIAL classified data are able to proceed without the need for SC clearance.

Misconception #3 - Aggregation increases classification level

Historically, the aggregation of records did not automatically cause an increase in the overall classification level. In some circumstances, aggregation could increase the potential impact of any data loss, and so the Impact Level of the combined data might need to be raised.

Many information security managers mistakenly believed that a higher Impact Level automatically meant a higher classification. This was not the intent, and the Government's wholesale change to information security management aimed to address this.

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf
[6] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf
[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/286667/FAQ2_-_Managing_Information_Risk_at_OFFICIAL_v2_-_March_2014.pdf

The Impact Level of a total loss of an aggregated dataset may be higher than that of individual components, but this depends on the dataset. For example, the contents of a Configuration Management Database (CMDB) has limited value compared with an aggregation of PII records. The Government's view, however, is that the overall classification of an aggregated dataset should not necessarily be changed merely due to aggregation, or even the increased impact. They state:

> *"Aggregated datasets of OFFICIAL information should typically be managed within the same infrastructure and there is no threshold where increased volume will cause an uplift in the classification level e.g. a database containing 100,000 OFFICIAL records does not become a SECRET database."*

They go on to say:

> *"Access to aggregated datasets of OFFICIAL information should be carefully managed and this may include technical controls which physically limit the amount of data that can be accessed or presented to a user or device. Storage of aggregated data on mobile devices should always be minimised as far as business requirements will allow."*

ServiceNow provides a number of technical controls within the Now Platform to specifically counter the aggregation risk, including preventative and detective controls.

Successful public sector commercial cloud adoption

ServiceNow's cloud-hosted SaaS offering has been successfully deployed by UK Ministerial Departments, Public Sector bodies, and agencies handling OFFICIAL and OFFICIAL-SENSITIVE data. The joint approach taken by those customers and ServiceNow has echoed the spirit of the changes from GPMS to GSCP—a move away from accreditation of individual products and services by niche, government-focused specialists, towards a customer-driven, risk-management based evaluation of commercial suppliers.

This requires a complete understanding of the data that is held within the system, of who needs to access it and why, and of the controls in place for protection from risks to confidentiality, integrity, or availability.

In an effort to simplify the approach to using commercial products and services in the Public Sector, the Government has transferred responsibility for risk management onto the customer. This entails a new approach to information gathering and product assessment. Risks must be properly articulated, or they cannot be assessed and managed. Questions about a product, service, or one of its components should relate directly to the confidentiality, integrity, or availability of the named information assets that will be stored in the system. The questions need to focus on managing information risk, rather than on complying with detailed prescriptive technical controls.

Suppliers of services to the UK public sector are often subject to contracts containing outdated terms such as Security Aspects Letters and Risk Management and Accreditation Document Sets (RMADS). The contracts may also insist that data should only reside in, and be accessed from, the UK. These contract terms predate the changes that the UK government made in 2014. Since contracts can run for multi-year periods, or roll on annually without review, many providers are now forced to comply with obsolete contractual limitations. This places unnecessary constraints on providers, end users, and customers, and limits opportunities to lower costs and/or increase system function and performance.

Some organisations have already successfully adapted to the spirit of the UK Government's changes in this area. They have updated legacy contracts or policies by adding addendums

which deal specifically with the outdated, conflicting terms. The Government's aim is the wider use of competitively sourced commercial products, with all risks appropriately managed.

Public Sector organizations who have adopted the ServiceNow Cloud have been able to do so by entering fully into the spirit of the new classification scheme. This enables and supports Government departments in embracing commercially available products.

Those customers that are using ServiceNow's cloud to process OFFICIAL data have satisfied their own Risk Management process, the OFFICIAL handling principles and controls, followed the GOV UK and National Cyber Security Centre (NCSC) Cloud guidance, and successfully demonstrated to their accreditors that this is the case. They will have followed the decision-making process in the NCSC Cloud Security Guidance document and taken the following journey:

1. Embraced the opportunity to adopt a risk-based approach rather than follow deprecated legacy rules. This included updating their own procurement processes and security policies in line with new government direction. They identified their risks and requirements, used them to develop solutions with adequate, proportionate, and appropriate security, and showed their working.
2. Concluded that the data they store in the Now Platform is classified no higher than OFFICIAL (including caveated OFFICIAL-SENSITIVE), and that the controls within ServiceNow, its SaaS offering, and underlying platform, are sufficient to meet their risk management requirements. The controls also satisfy new government best practice for handling information at OFFICIAL, which is predominantly ISO 27002 based.
3. Accepted that regular uncontrolled access to data classified as OFFICIAL only requires Baseline Personnel Security Standard (BPSS) - the basic UK clearance - or equivalent, and not SC Clearance[8]. They have examined ServiceNow's personnel vetting procedure and are satisfied with its equivalency, and that ServiceNow is respecting "need to know" within its product and organization.
4. Confirmed that aggregation of records does not automatically increase the classification from OFFICIAL to SECRET[8,9] and so no additional controls or clearances are needed. The two references cited describe how aggregated data sets do not automatically increase in impact level, and that the data owner may elect to put additional controls in-place, such as enhanced logging.
5. Accepted that offshoring of OFFICIAL data is permitted by HMG[8], though data relating to individuals (PII) remains subject to applicable data privacy regulations. ServiceNow is able to demonstrate adequate controls and will enter into Standard Contract Clauses (SCC) or other relevant or recognized contractual mechanisms as required.
6. Verified that the controls governing ServiceNow's tenancy and support model are sufficient for them to accept the risks they have identified and that they have defined those risks around their data, not their infrastructure.

How ServiceNow supports the UK public sector

ServiceNow has used best practices from across the industry as a foundation for its security model, demonstrated through attainment of the relevant credentials. Please see Securing the

[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf
[9] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/286667/FAQ2_-_Managing_Information_Risk_at_OFFICIAL_v2_-_March_2014.pdf

Now Platform for information on our certifications and attestations, and what they mean for customers.

ServiceNow has supported the process by:

1. Providing evidence and transparent disclosures about its products, platform, infrastructure and organization
2. Referring to a number of commercial assurance baselines, as listed further in this section
3. Providing responses to specific HMG guidance where applicable
4. Standardizing information exchange using third party formats

Legal protections for the customer and their data are also important. ServiceNow can provide the following key documents for UK public sector assurance provision:

- Comprehensively scoped ISO 27001:2013, ISO 27017:2015 and ISO 27018:2014 certifications,
- Cyber Essentials Plus Certification
- SSAE18 SOC2 Type II audits
- Cloud Security Alliance (CSA) Consensus Assessment Initiative Questionnaire (CAIQ) and Cloud Controls Matrix (CCM)
- Shared Assessments Standardized Information Gathering (SIG) questionnaire
- Data Transfer Addendums/EU Model Clauses

Conclusion

ServiceNow's standard SaaS offering has proven suitable for handling OFFICIAL data and is already being used by many UK Public Sector organisations. This is the outcome that the Government intended by introducing its changes, and major Government Departments are currently reaping the benefits of those changes by using ServiceNow.

Additional resources

- Trust and Compliance Center
- Securing the Now Platform eBook
- ServiceNow Assurance Pack (SNAP) (requires CORE login)
- Product Documentation

Appendix A – ServiceNow's response to the UK Government's NCSC Cloud Security Principles

The UK government has made considerable efforts in recent years to enable adoption of cloud services[10]. A "Cloud First" policy was introduced in 2013 for UK public sector organizations and government departments when making technology decisions[11].

Supporting guidance in the form of the Cloud Security Principles[12] were first published in April 2014 by the Communications-Electronics Security Group (CESG), a UK government agency. The principles are currently available at the UK National Cyber Security Centre (NCSC).

The principles are intended to assist cloud service consumers with assessing and evaluating associated risks, and are aligned with ISO/IEC 27001, an internationally recognized information security management standard.

ServiceNow has implemented an ISO/IEC 27001 information security management system (ISMS) in accordance with reference to and guidance from the ISO/IEC 27002 code of practice. As such, ServiceNow has been accredited as an ISO/IEC 27001:2013 certified organization[13].

Definitions

Now Platform

The Now Platform is a powerful cloud application that enables customers to link real-time data with activities, tasks, and processes to achieve better work outcomes in a single system of action.

Instance

An instance is an entirely discrete entity of the Now Platform consisting of two or more application nodes and a single database. This stores all data, code, and configuration information for the instance.

ServiceNow Cloud

ServiceNow instances are provisioned within a highly available cloud infrastructure which offers production instance redundancy between two data center clusters in every geography. This is supported by global operations and support organizations, conforming to a common set of standards, policies, processes, and tools.

[10] https://www.gov.uk/guidance/public-sector-use-of-the-public-cloud
[11] https://www.gov.uk/guidance/government-cloud-first-policy
[12] https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles
[13] https://cert.schellmanco.com/?certthash=O6sysQQQ1ixb

Responses to the Cloud Security Principles

The goals of each principle are reproduced here in their currently published form, along with the corresponding ServiceNow response.

Principle 1 – Data in transit protection

"User data transiting networks should be adequately protected against tampering and eavesdropping."

Goals of the principle	How does ServiceNow address the goals?
• Data in transit is protected between end user device(s) and the service • Data in transit is protected internally within the service • Data in transit is protected between the service and other services (e.g. where APIs are exposed)	All end user and API (web services) access to an instance of the Now Platform is encrypted using HTTPS. TLS 1.2 cipher suites are provided by ServiceNow's internet-facing infrastructure. Other secure protocols for specific, customer-driven integrations are also available, such as LDAPS, SFTP, FTPS, and SCP. ServiceNow also provides United States FIPS 197 (Federal Information Processing Standards) compliant cryptographic suites for data in transit over HTTPS outside of its private cloud network. Specifically, the platform supports: • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 These are FIPS approved cipher suites (Per NIST 800-52 r1 DRAFT). Customers must use endpoints and browsers capable of using and preferring TLS v1.2 in order to leverage the FIPS 140-2 compliant cryptographic implementation. Access to the private cloud infrastructure in which the service is hosted is only permissible via a ServiceNow issued endpoint. The endpoint requires possession of a valid client certificate and use of a 2FA secure VPN to grant access to the underlying ServiceNow infrastructure. A secure administrative sandbox is further used by support and technical personnel on their individual endpoints. It is not possible using this approach to copy data from the infrastructure or a customer's ServiceNow instance to a ServiceNow endpoint. Communications within ServiceNow private networks between endpoints used for administering its infrastructure and components of that infrastructure are encrypted using well-established protocols such as SSH and SFTP.

Principle 2 – Asset protection and resilience

"User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure."

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should seek to understand: • In which countries their data will be stored, processed and managed. They should also consider how this affects compliance with relevant	ServiceNow operates its service globally, including a redundant data centre pair in the UK, with centers located in Newport, Wales and London (Slough), England. Public sector customers operating in the UK usually elect to use this pair. The data centre providers control physical access to their facilities up to the boundary represented by the ServiceNow colocation spaces. Access to the spaces themselves is controlled by ServiceNow, using both biometric and

Goals of the principle	How does ServiceNow address the goals?
legislation e.g. Data Protection Act (DPA), GDPR etc. • Whether the legal jurisdiction(s) within which the service provider operates are acceptable to them	access card readers combined with PIN entry. The ServiceNow data centre operations team maintains and manages the access control lists for its spaces. Limited access is provided for data centre provider personnel where required, either on a ServiceNow pre-approved basis or for health and safety purposes. No ServiceNow personnel other than those directly responsible for data centre fabric have physical access to ServiceNow data centre locations. The ServiceNow data centre colocation model aligns regional processing locations with common regulatory frameworks within specific geographies, such as GDPR. Processing of customer data occurs only within these data centre locations with no scheduled or regular transfers of data to any other geography. Incidental transfers, e.g. those that may occur during after-hours support engagements, are the only circumstance where customer data may be temporarily transmitted to another region. ServiceNow is also able to offer a data processing contract addendum to all customers which includes the EU standard model contract clauses in an unaltered form[14].

Principle 3 – Separation between users

"A malicious or compromised user of the service should not be able to affect the service or data of another."

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should seek to: • Understand the types of user they share the service or platform with • Have confidence that the service provides sufficient separation of their data and service from other users of the service • Have confidence that management of their service is kept separate from other users (covered separately as part of Principle 9)	All ServiceNow customers are hosted in private data centre colocation spaces and share a common physical server infrastructure. No host-based virtualization is used in provision of the service. Customers each access logically separate and individual instances of the Now Platform. These consist of a number of redundant application nodes and a dedicated database. Each instance is also connected to a single database software service. The database service and the tables it provides are used by and *only accessible to that specific single instance*. In the scenario of a customer being assigned multiple instances of the Now Platform, this means entirely separate database services and tables, one per instance. There is absolutely no sharing of customer databases, even for a single customer with several instances. ServiceNow does not operate a multi-tenant environment with multiple customers sharing a common database. ServiceNow has implemented additional logical separation mechanisms at the operating system layer, in order to further isolate each Now Platform instance. This includes per-instance daemon (system) user accounts, file system permissions, and system services which enforce mandatory access controls. Host-based firewalls are also deployed on host systems where customer data is present in order to further control egress and ingress to these systems.

[14] https://www.servicenow.com/company/trust/faq.html

Goals of the principle	How does ServiceNow address the goals?
	These controls significantly mitigate the opportunity for lateral movement between individual instances by any potential threat actor. Customers may optionally extend the "multi-instance" or logically single tenant model further by purchasing a dedicated hardware option, meaning they will not share server hardware with any other customers. This option includes servers at the application and database tiers only. Other related services and infrastructures remain shared across all customers.

Principle 4 – Governance framework

"The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined."

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should ensure that: • A clearly identified, and named, board representative (or a person with the direct delegated authority) is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer' • A documented framework exists for security governance, with policies governing key aspects of information security relevant to the service • Security and information security are part of the service provider's financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk • Processes to identify and ensure compliance with applicable legal and regulatory requirements have been established	ServiceNow has a dedicated security organization comprised of a number of different teams with distinct responsibilities towards securing the Now Platform. An entirely separate team handles information security within the ServiceNow corporate environment. The security organization is led by a chief information security officer (CISO), reporting to the chief information officer (CIO). For the benefit of all customers, ServiceNow has implemented industry-recognized information security and governance frameworks and standards. This includes accreditation to ISO/IEC 27018:2014, ISO/IEC 27017:2015, and ISO/IEC 27001:2013. ServiceNow undertakes regular ISO 27001 and 27018 surveillance audits, along with third-party audits and attestations. This includes the annual preparation and subsequent customer availability of SSAE18 SOC1 and SOC2 reports. These undertakings are intended to ensure the suitability and effectiveness of its policies, standards, controls, and processes. When combined with internal and third-party audits, these efforts represent a significant commitment to maintaining a vigorous and transparent security program. ServiceNow has in place processes and personnel to analyze, evaluate, score, prioritize, and manage risks as part of its information security risk management (ISRM) program. This program provides a structured and managed approach to identifying, recording, analyzing, and guiding the treatment and remediation of risks within ServiceNow. A global legal team ensures compliance with all relevant statutory legal and regulatory obligations within the various regions in which ServiceNow operates. Finally, transparency is a significant element of any security program. ServiceNow makes accreditation and attestation documentation available to customers via a self-service governance facility, called CORE (compliance operations readiness evidence). CORE also provides access to many internal ServiceNow documents, including policies, standards, and operating procedures. Executive summaries of major release application penetration testing reports and network penetration testing

Goals of the principle	How does ServiceNow address the goals?
	reports are also available to customers within CORE. For further information, please visit the ServiceNow CORE solutions brief here.

Principle 5 – Operational security

"The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes."

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should be confident that: • The status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime • Changes to the service are assessed for potential security impact. Then managed and tracked through to completion	ServiceNow manages its services and infrastructure using its own instances of the Now Platform. A central configuration management database (CMDB) is deployed and updated continuously with the latest ServiceNow hardware and software. Within its Cloud, ServiceNow has deployed a number of detective and preventative controls and processes. These include: • Network and host-based firewalls at the network perimeter and at various server infrastructure tiers in order prevent the ingress and egress of network traffic not intended for or relevant to instances of ServiceNow • Redundant intrusion detection system (IDS) monitoring network traffic as it transits into the Cloud network. This feeds the ServiceNow security information and event management (SIEM) systems • Traffic modeling and monitoring against operational baselines Alerts and notifications are generated by the SIEM systems in accordance with pre-defined triggers and metrics that are updated constantly. These are reviewed by a 24/7/365 security operations team with global coverage. Events, alerts, and relevant logs from servers, network devices, and ancillary systems are also forwarded to the SIEM. This allows ServiceNow to build and maintain a comprehensive manifest of the activities that are occurring in its environment on a day-to-day basis. ServiceNow tunes and adjusts monitoring to meet the specific characteristics of ServiceNow instances. External security alerts or events, multiple threat feed sources, and other relevant information are all stored and aggregated in an internal ServiceNow instance used for their ongoing assessment and management. The ServiceNow security operations team also completes daily checklists across a range of security domains, including privilege account usage, IDS alerts, file integrity monitoring (FIM), and database access. The daily checklists and captured events are managed through a ServiceNow instance. Any variances that are discovered are raised as incidents for tracking, notifications, and investigation. In operating its own environment, ServiceNow uses change management processes based on ITIL v3 principles. Changes pass through multiple levels of approvals and change advisory board (CAB) meetings are held at least three times per week to review upcoming changes. Emergency changes

Goals of the principle	How does ServiceNow address the goals?
	are also subject to additional "X" CAB reviews, as required. Employees are not able to submit and approve their own change requests. Automation is used extensively both in the execution of changes and in the management of configurations and revisions made to them to ensure they are authorized. Change management within a customer's instance(s) of ServiceNow and monitoring for appropriate use of that instance on a general basis remains a customer responsibility.

Principle 6 – Personnel security

"Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel."

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should be confident that: • The level of security screening conducted on service provider staff with access to the consumers information, or with ability to affect the service, is appropriate • The minimum number of people necessary have access to the consumers information or could affect the service	Prior to employment, ServiceNow screens all directly employed personnel, temporary workers, and contractors, and requires similar screening controls from its vendors. The exact nature of screening varies from region to region based on both the nature of their role and legal obligations or relevant restrictions that may be in place in specific geographies. In the UK, the background screening process is at least equivalent to the Government Baseline Personnel Security Standard (BPSS). Personnel are also contractually obliged to report any change in their personal circumstances which could be relevant to their employment, e.g. bankruptcy or criminal convictions. ServiceNow personnel undergo annual security awareness training and other relevant training as needed. The former includes the completion of a post-training assessment to measure their understanding and determine further training needs if required. Access to ServiceNow infrastructure or systems hosting customer data is provided based on employee role in accordance with the least privilege model. In addition, any required access is permitted only where an approved employee has also passed a number of gates. This includes first being assigned to an incident or problem for a specific customer which requires the employee to access a customer instance for the relevant purposes. Customers may also control access to their instances and require their own approval to be granted before access can be undertaken[15].

Principle 7 – Secure development

"Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity."

[15] https://docs.servicenow.com/bundle/london-platform-administration/page/administer/security/concept/c_SNCAccessControl.html

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should be confident that: • New and evolving threats are reviewed, and the service improved in line with them • Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment • Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment	ServiceNow follows recognized industry guidance and best practice from organizations including OWASP (Open Web Application Security Project), NIST (National Institute of Standards and Technology), CSA (Cloud Security Alliance) and CIS (Center for Internet Security). This includes guidance relevant to how ServiceNow develops its software products, implements its cloud infrastructure, and assesses its service in the context of new or existing threats. Software security teams within ServiceNow provide input throughout the development lifecycle from the initial release planning phase into the final release stages, including formal signoff. Signoff for the final release phases is also required from the ServiceNow CISO. The teams perform a number of functions, including but not limited to: • Managing the various internal and external testing programs • Performing assessments of internal ServiceNow services and infrastructure • Undertaking architectural reviews for features in new releases of the Now Platform • Curating educational security materials, including those for customers Test instances of currently supported ServiceNow versions are tested on an ongoing, continuous basis. This includes both manual testing and testing by a dynamic web application scanning tool (DAST). Manual code reviews and audits are also undertaken alongside static application security testing (SAST) for code during development. These steps are intended to identify any potential security issues in current code and code destined for the next release of the Now Platform as early as possible. New releases of ServiceNow are also subject to application penetration testing by a third-party organization prior to being made available to customers. The scope of these tests is in accordance with the OWASP Application Security Verification Standard Project (ASVS). Customers are also able to perform application penetration tests annually on an assigned instance of ServiceNow. This needs to be scheduled and approved in conjunction with relevant ServiceNow processes. ServiceNow code is stored in secure repositories accessible only to approved ServiceNow personnel. Access is logged and monitored. Code is checked in and out of this repository by named individuals and is locked once main branch development has completed for a new release.

Principle 8 – Supply chain security

"The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement."

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should seek to understand and accept: • How their information is shared with, or accessible to, third party suppliers and their supply chains • How the service provider's procurement processes place security requirements on third party suppliers • How the service provider manages security risks from third party suppliers • How the service provider manages the conformance of their suppliers with security requirements • How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with	ServiceNow does not use third-party vendors in direct provision, management, or handling of customer data. All data centre infrastructure, networks, systems, and other relevant services are built out and managed exclusively by ServiceNow. No third-party organization has logical access to ServiceNow systems or customer data. Colocation providers have access to ServiceNow colocation spaces only when authorized by ServiceNow or for emergency purposes. ServiceNow mandates specific security requirements with its vendors and seeks to ensure appropriate governance is in place for future vendor verification. A vendor security risk assessment (VSRA) process has also been implemented. The process is owned and managed by the governance, risk, and compliance (GRC) team within ServiceNow. Relevant vendors are required to complete various assessment documentation as part of the overall process. Risk is evaluated throughout the assessment process. Vendors that represent high risk according to the scoring system are not taken forward as potential vendors. Each assessment is tailored for the type of service and information assets relevant to the potential vendor and the services they are to provide. The GRC team works with that vendor and internal stakeholders to gather information on necessary controls identified as relevant. Vendor approval is contingent on any risk observations and any identified mitigating controls being addressed, completed background checks, and final management signoff. Vendor assessment is reconducted at regular intervals for relevant suppliers, e.g. those providing colocation or network services.

Principle 9 – Secure user management

"Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorized access and alteration of your resources, applications and data."

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should: • Be aware of all of the mechanisms by which the service provider would accept management or support requests from you (telephone, web portal, email etc.) • Ensure that only authorized individuals from their organization can use those mechanisms to affect their use	ServiceNow verifies customer identities automatically by means of authentication when they raise requests for support via the Now Support Portal[16]. This is the primary route for customers to make queries and request assistance from ServiceNow. Customers may also contact ServiceNow by telephone. This method ensures a customer's identity is verified, in accordance with a standard operating procedure. This procedure is documented for internal ServiceNow reference on the Now Support Portal and is described during mandatory new hire training for customer support personnel.

[16] https://support.servicenow.com/now

Goals of the principle	How does ServiceNow address the goals?
of the service (Principle 10 can help consumers consider the strength of user identification and authentication in each of these mechanisms)	ServiceNow does not accept requests for support via email and informs customers of all valid communication methods on its corporate website and documentation portal at https://docs.servicenow.com.

Principle 10 – Identity and authentication

"All access to service interfaces should be constrained to authenticated and authorized individuals."

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should: • Have confidence that identity and authentication controls ensure users are authorized to access specific interfaces	Customers control and manage access to interfaces of their instances of the Now Platform. This includes interactive Web UI access by end users and any programmatic access for APIs or integrations. Customers are able to access a ServiceNow instance using a number of standards-based authentication methods, including: • Federated identity solutions compliant with the Security Assertion Markup Language (SAML) 2.0 specification, to support single sign-on and optionally a customer's own two-factor or multifactor authentication capability • Lightweight Directory Access Protocol (LDAP) for directory-based solutions such as Microsoft Active Directory, augmented with optional ServiceNow-provided multifactor authentication • Built-in Now Platform authentication augmented with optional ServiceNow-provided multifactor authentication Where customers use their own LDAP or SAML services for authentication, passwords are not stored in their ServiceNow instance. Password policies regarding complexity or length for example, are then inherited from a customer's own services. Where a customer uses built-in Now Platform authentication, passwords are stored as one-way hashes using a SHA-2 based mechanism. Password strength, complexity, expiry, re-use, and so on can be configured by the customer. Customers are also able to restrict access to their instance from only those network addresses or ranges known to them, e.g. public or proxy addresses, corporate VPN networks, etc. Certificates may be used for outbound mutual authentication from a ServiceNow instance to an external system or web service specified by the customer. ServiceNow does not presently support the use of client certificates as a means of end user authentication to an instance of the Now Platform.

Principle 11 – External interface protection

"All external or less trusted interfaces of the service should be identified and appropriately defended."

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should: • Understand what physical and logical interfaces their information is available from, and how access to their data is controlled • Have sufficient confidence that the service identifies and authenticates users to an appropriate level over those interfaces (see Principle 10)	An instance of the Now Platform provides a common and rich set of interfaces and methods for data transfers. By design, a number of these methods are intended to assist customers in getting information into and out of a ServiceNow instance, or to integrate with other customer systems or services. Customers select and configure them in accordance with their own individual requirements or organizational security policies. Various security capabilities are inherent to the Now Platform, including HTTPS for secure SOAP or REST transactions, and SFTP and FTPS for secure file transfers. Additionally, the underlying ServiceNow cloud infrastructure provides further capabilities, such as transport layer security (TLS). These interfaces and the functionality they provide are subject to continuous testing as part of ServiceNow's secure software development program. When consuming services and information from a ServiceNow instance, authentication is required by default in most scenarios. However, there are situations where a customer may not require authentication to a resource in their instance, e.g. a specific knowledge base or articles may need to be publicly accessible. The decision to provide access in this manner is solely at the discretion of the customer. Customers are also able to transfer data to or from an external source into a ServiceNow instance over clear-text protocols such as FTP or HTTP. These protocols are not configured by default and their selection and use is determined by a customer. It therefore remains incumbent on the customer as the data controller to configure these integrations appropriately based on their requirements, and understand the risk related to information assets transferred under such circumstances. The ServiceNow response to Principle 10 provides further information in respect to authentication.

Principle 12 – Secure service administration

"Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data."

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should: • Understand which service administration model is being used by the service provider to manage the service • Be content with any risks the service administration model in use brings to the consumers data or use of the service	The majority of ServiceNow personnel have no way to access any customer instance or the underlying Cloud infrastructure. Personnel other than those directly responsible for data centre fabric do not have physical access to ServiceNow data centre locations. A two-factor management VPN is required to grant logical access to the underlying cloud infrastructure for ServiceNow employees in an appropriate role. Access can only be made via a ServiceNow endpoint configured with a valid machine certificate. Subsequent employee access and privilege within the cloud infrastructure is based on their role. Administrative and other relevant support or technical roles are subject to quarterly need review and reverification by the employee's manager. A number of approval gates must be passed before an employee is granted access to a customer instance. These include the requestor holding a relevant support role and also being assigned a current incident, problem, or change for the specific customer to which they are providing support. Access is not persistent and is removed automatically once the relevant work has been completed. At all cloud and infrastructure layers, unique credentials are necessary for access to any systems permitted by role. All access is logged and monitored via a combination of techniques, including event aggregation, alerting, and manual checks. Any commands requiring elevated privileges are authorized and monitored by a Centralized Privileged Access Management (PAM) solution. Personnel who deal with queries and issues raised by customers regarding their instances use the same web interface as customer end users and customer administrators. They could, therefore, be exposed to customer data within those instances. In order to mitigate associated risks in this regard, access is provided via a secure sandbox management environment which is deployed individually on their endpoint. This removes the ability to transfer, export, or otherwise exfiltrate customer information. This access model accords with the "Service administration via bastion hosts" systems administration architecture described at https://www.ncsc.gov.uk/guidance/systems-administration-architectures. Customers can also require ServiceNow customer support personnel to be "pre-authorized" before they are able to access a customer instance, and only have access for a defined period. This feature is provided for by the ServiceNow Access Control Plugin[17].

[17] https://docs.servicenow.com

Principle 13 – Audit information for users

"You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales."

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should: • Be aware of the audit information that will be provided, how and when it will be made available, the format of the data, and the retention period associated with it • Be confident that the audit information available will meet their needs for investigating misuse or incidents	An instance of the Now Platform generates detailed log and audit information[18]. Verbose transaction, client, event, email, and system logs are directly accessible to customer administrators of ServiceNow instances. Log data within a ServiceNow instance is retained for a maximum of 30 days and customers with longer retention periods are advised to export or transfer logs using features present in the Now Platform. Records stored in an instance of the Now Platform are also subject to audit history. This information is perpetual for the lifetime of a record in an instance. All changes to that record are maintained until its deletion. Logs and events can also be forwarded to a customer's own environment, logging system or SIEM environment. This can be achieved using a number of methods: • Use a syslog probe which utilizes the MID server to automatically transfer log events to a syslog compatible service • Use web service calls to make queries to log tables • Browse and download logs containing events of interest directly, in CSV or other common formats These techniques allow for log and audit events to be stored within a customer's environment and further retained according to their specific requirements. ServiceNow retains separate log and event information for the underlying cloud infrastructure. Whilst not shared with customers on a general basis, circumstances such as a security incident may mean relevant internal log information is shared with an affected customer.

Principle 14 – Secure use of the service

"The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected."

Goals of the principle	How does ServiceNow address the goals?
Cloud service consumers should: • Understand any service configuration options available to them and the	ServiceNow provides expansive documentation and related resources relevant to Now Platform best practice configuration, development, and use. Additionally, specific information is provided about security, including security best practice and ServiceNow instance hardening recommendations. These assist ServiceNow customers in making the most

[18] https://docs.servicenow.com/bundle/london-platform-administration/page/administer/system-logs/concept/system-logs.html

Goals of the principle	How does ServiceNow address the goals?
security implications of their choices • Understand the security requirements of their use of the service • Educate their staff using and managing the service in how to do so safely and securely	appropriate configuration choices for their needs while ensuring they are running in as secure a state as possible. Training is highly recommended for customer administrators and developers who will be managing instances of the Now Platform, as well as provision of general security awareness within an organization.