UK public sector assurance

ServiceNow security response to cloud assurance within the UK public sector
# Table of contents

Introduction ........................................................................................................................................... 3
Intended audience ................................................................................................................................. 3
ServiceNow offering .............................................................................................................................. 3
UK public sector cloud context ............................................................................................................. 3
UK public sector assurance context ..................................................................................................... 4
  Historical context: Government Protective Marking Scheme (GPMS) .............................................. 5
  The fundamental changes: Government Security Classifications Policy (GSCP) ......................... 5
GSCP OFFICIAL classification ............................................................................................................. 6
Baseline security outcomes .................................................................................................................. 7
Marking .................................................................................................................................................. 7
Common misconceptions...................................................................................................................... 7
  UK data must remain within the UK and be accessed only from the UK ........................................ 7
  Handling government data requires security cleared (SC) personnel ............................................. 7
  Aggregation increases classification level ....................................................................................... 8
ServiceNow’s public sector approach ................................................................................................. 8
Successful public sector commercial cloud adoption ......................................................................... 9
Conclusion ............................................................................................................................................ 10
References ........................................................................................................................................... 12
For more information ......................................................................................................................... 12
Introduction

Changes to UK Government security classification schemes affecting the public sector and associated industries can be challenging to implement. However, they provide opportunities to adopt less prescriptive technologies and operational processes. Many public-sector bodies have found the changes to be complex, and several of ServiceNow’s customers have asked for our advice in this area. This document provides an overview of Cloud Services in this context, and acts as a first step towards a successful public-sector adoption of ServiceNow.

Intended audience

This document is intended for use by anyone considering adoption of the Now Platform® within the UK public sector or wishing to understand more about ServiceNow in that context.

ServiceNow offering

ServiceNow is a Platform and Software as a Service (PaaS/SaaS) offering. SaaS enables organizations to exploit the power, flexibility and resilience of cloud computing. With its multi-instance design, ServiceNow’s SaaS allows a vast amount of configuration flexibility from one customer instance to another, built on a uniform infrastructure foundation, complementary tooling, and standardised delivery of those instances.

ServiceNow operates its service on a private cloud, owned and operated entirely by ServiceNow, deployed on ServiceNow-owned equipment in a dedicated, ServiceNow-managed data centre space.

This service delivery model could be considered to turn traditional procurement on its head. Rather than a customer issuing their policies and standards and asking for a product or service to meet their requirements, they instead take the service as it is and determine any risks they believe may be introduced by its use. Then, with the supplier’s help, the customer seeks to further understand how to use the controls offered to reduce any perceived risk to an acceptable level.

UK public sector cloud context

“Your service team must consider cloud purchases before any other options because of the government’s Cloud First Policy.” - Government Service Manual: Securing Your Cloud Environment

“...In future, when procuring new or existing services, public sector organizations should consider and fully evaluate potential cloud solutions first – before they consider any other option.” - Government Cloud First Policy

“...On balance we think well-engineered SaaS is better for security than the alternatives.” - National Cyber Security Centre conclusion in Debunking Cloud Security Myths

Cloud services present a leap forward in capability and value. They can also present a leap forward in security, but for many organizations, evaluating this may require a new approach. Using assurance practices and methodologies intended for on-premise solutions, commercial off-the-shelf software (COTS), or using those that are infrastructure-centric may hinder proper assessment of cloud services. Evaluating the Cloud requires an approach focused on the data, rather than one focused on the infrastructure. In this context, responsibilities for infrastructure fail

---

1 https://www.gov.uk/service-manual/technology/securing-your-cloud-environment
2 https://www.gov.uk/guidance/government-cloud-first-policy
on the cloud service provider—a customer has limited ability to impose their organization’s standards, especially in relation to infrastructure.

Mature cloud assurance guidelines are now available from the National Cyber Security Centre (NCSC, formerly CESG):

- NCSC Understanding Cloud Security
- NCSC Cloud Security Myths
- NCSC Cyber Security Principles
- NCSC Separation and Cloud Security

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.

The Government Cloud First Policy states that customers should follow the National Cyber Security Centre guidance on understanding Cloud Security. The guidance discusses Data Separation, the Cloud Security Principles, and Security Responsibilities, before taking the reader through the risk-based decision-making process. ServiceNow is happy to support customers throughout this process.

**UK public sector assurance context**

In April 2014, as a result of a review of the Government Protective Marking Scheme (the GPMS Review), the Cabinet Office reduced the existing six Business Impact Levels (BILs) to three by making the following changes:

- Removed UNCLASSIFIED
- Replaced the traditional classifications: Impact Level (IL) 2 - Protect, IL3 - Restricted, and IL4 - Confidential, with a single OFFICIAL classification
- Retained SECRET and TOP SECRET

The current Government document (which replaces GPMS) that describes the new scheme is the Government Security Classifications Policy (GSCP). The Cabinet Office’s Security Policy Framework (SPF) incorporates the post 2014 classification scheme (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.

There is no direct mapping between the old scheme’s Impact Levels 2 to 4 and the new OFFICIAL classification. It is certainly not correct to say that all existing data that was classified IL2, 3, and 4 is now classified as OFFICIAL.

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

---

3 https://www.ncsc.gov.uk/guidance/introduction-understanding-cloud-security
4 https://www.ncsc.gov.uk/blog-post/debunking-cloud-security-myths
5 https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles
6 https://www.ncsc.gov.uk/guidance/separation-and-cloud-security
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.

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.

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

The net result was that the industry tied itself up in knots trying 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.

**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 FAQ\(^9\) states that:

“All new tenders should be to the new approach from October 2013. 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.

**GSCP OFFICIAL classification**

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

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.
- Personal information 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 could have damaging consequences if lost, stolen, or published in the media, but may not be subject to a heightened 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. This may include, but is not limited to: ‘hacktivists’, single-issue pressure groups, investigative journalists, competent individual hackers, and the majority of criminal individuals and groups.

The classification is an indication of the sensitivity of 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.

---

Baseline security outcomes

- 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

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

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

UK data must remain within the UK and be accessed only from the UK

The EU defines the concept of a data transfer very broadly. This definition includes the incidental viewing of data stored in the European Economic Area (EEA) from outside of the EEA. However, no ServiceNow customer data is routinely transmitted or stored outside of the customer’s chosen data center region. In the case of the ServiceNow EMEA data center pair, customer data remains within the EEA at all times. Incidental transfers (observation) by ServiceNow Support staff from outside of the region may occur occasionally during the normal provision of technical support, as stated in customer contracts.

The government currently states\(^{10}\) that off-shoring of OFFICIAL information is permitted, but with special consideration for Personally Identifiable Information (PII). PII should remain either within the EEA, or under the protection of Safe Harbor (now Privacy Shield), or in countries with positive findings of adequacy from the European Commission.

ServiceNow is also able to contract that its provisions are adequate through the use of EU Model Clauses.

Regional changes to the statutory and regulatory frameworks and legislation (e.g. those resulting from Brexit) are monitored constantly and will be addressed in advance as relevant, in order to ensure ServiceNow’s offerings remain compliant in all relevant jurisdictions.

Handling government data requires security cleared (SC) personnel

OFFICIAL classification requires only Baseline Personnel Security Standard (BPSS), or equivalent security clearance, not the more stringent SC or SC Cleared\(^7\). The government found that Risk Assessors routinely determined infrastructure to have a higher level of classification than the data it contained, due to aggregation\(^7,10\). 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 - for example, requiring 5 years of full background checks, as opposed to 3 years of employment checks only. It is on that basis that customers using ServiceNow for OFFICIAL classified data have proceeded without the need for SC clearance.

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 believed – mistakenly – that a higher Impact Level automatically meant a higher classification. This was not the intent and the government’s wholesale changes to information security management aims to address this.

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.

ServiceNow’s public sector approach

ServiceNow’s cloud-hosted SaaS offering has been successfully deployed by UK Ministerial Departments, Public Sector bodies, and agencies handling OFFICIAL (including 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 adapted successfully 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.

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 the document titled “Qualifying ServiceNow as a Vendor” for information on our certifications and attestations, and what they mean for customers.

Successful public sector commercial cloud adoption

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 NCSC Cloud guidance, and demonstrated that to their accreditors. They will have followed the decision-making process in the NCSC document Understanding Cloud Security and taken the following journey:

5. 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.

6. 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.

7. Accepted that regular uncontrolled access to data classified as OFFICIAL only requires BPSS (the basic UK clearance) or equivalent, and not SC Clearance. 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.

8. Confirmed that aggregation of records does not automatically increase the classification from OFFICIAL to SECRET, 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.

9. Accepted that offshoring of OFFICIAL data is permitted by HMG\textsuperscript{10}, though data relating to individuals remains subject to data privacy laws such as GDPR, Safe Harbor/Privacy Shield etc. ServiceNow can demonstrate adequate controls and will enter into EU Model Clauses or other relevant or other recognized contractual mechanisms as required.

10. 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.

ServiceNow has supported that 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. The key documents in public sector assurance provision include:

- SSAE18 SOC2 Type II audits
- Responses to the CESG Cloud Security Principles
- Cloud Security Alliance Consensus Assessments Initiative and Cloud Control Matrix
- Shared Assessments Standardized Information Gathering (SIG) questionnaire
- Data Transfer Addendums/EU Model Clauses
- EU-US Privacy Shield Registration

**Conclusion**

In “Debunking Cloud Security Myths”\textsuperscript{2}, The National Cyber Security Centre makes raises a pertinent point:

"Consider whether your IT security engineering team is going to be better or worse at security management for a major commodity product, offered - as a service - by the major vendor who developed it."

ServiceNow has one service, one cloud infrastructure, one set of support processes, and one mission: to securely process and manage your data, and to make all possible efforts to this end.

The Now Platform is a robust and mature offering in which UK public sector bodies and associated organisations can store and process data at OFFICIAL classification. It is a transitional time for the industry; many contracts are operating under a legacy regime, while a new approach has been developed and strongly encouraged for several years.

The standard ServiceNow SaaS offering is eminently suitable – and is already being used – for handling OFFICIAL data. This is exactly the kind of outcome that the Government intended by introducing its changes, and major Government Departments are currently reaping the benefits of those changes by using ServiceNow.

From an Information Security perspective, moving to Cloud Services requires an assessment of the data in question, the controls available, and the risks involved. Once this has been done
and, an organization is ready to make the transition, ServiceNow will be happy to take that journey with them.
References

1. NCSC Introduction: Understanding Cloud Security
   https://www.ncsc.gov.uk/guidance/introduction-understanding-cloud-security

2. NCSC Cloud Security Myths
   https://www.ncsc.gov.uk/blog-post/debunking-cloud-security-myths

3. NCSC Cloud Security Principles
   https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

4. NCSC Separation and Cloud Security
   https://www.ncsc.gov.uk/guidance/separation-and-cloud-security

5. Securing Your Cloud Environment

6. UK Government Cloud First Policy
   https://www.gov.uk/guidance/government-cloud-first-policy

7. Government Security Classifications Policy (GSCP): the current HMG document which replaces the GPMS and describes the new scheme

8. FAQ Sheet 1: Working with Official Information: describes the official classification, what should be marked, how it should be marked, and how data should be valued

9. Introducing the Government Security Classifications Core briefing for 3rd Party Suppliers: introduces the new classifications and the spirit of the change

10. FAQ Sheet 2: Managing Information Risk at Official: goes into more specific detail about the management of risk to that date

For more information

- ServiceNow Assurance Pack (SNAP)
- Delivering Secure, Scalable, and Compliant Cloud Services eBook
- Trust and Compliance Center
- Product Documentation
- www.servicenow.com