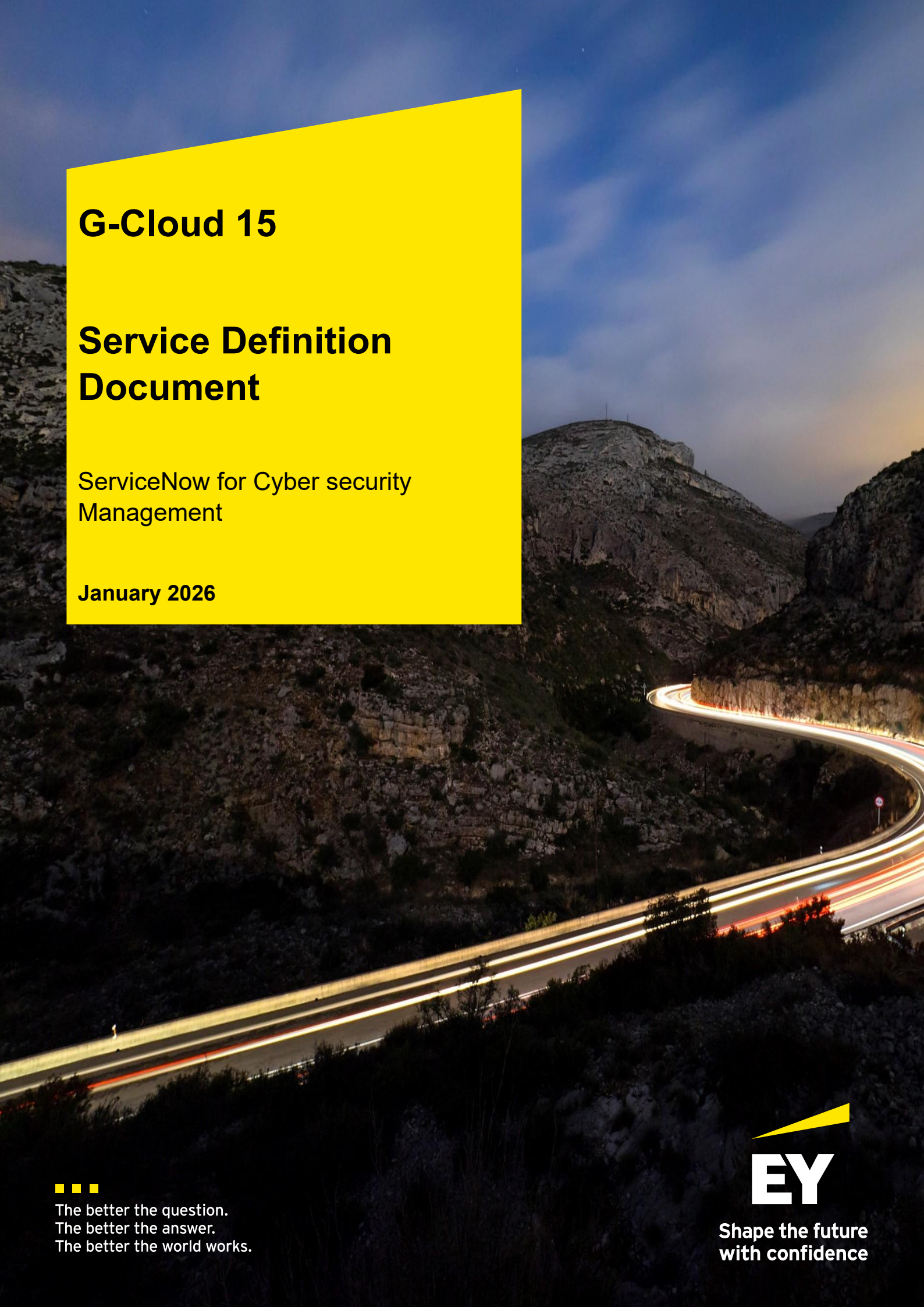

G-Cloud 15

Service Definition Document

ServiceNow for Cyber security Management

January 2026

The better the question.
The better the answer.
The better the world works.

Shape the future with confidence

Contents

1. Service detail

1.1. Introduction to the Service

EY enables organisations to rapidly kick-start their Enterprise Security Operations digital transformation journey by implementing ServiceNow Security Operations (SecOps). **ServiceNow Security Operations (SecOps)** is a comprehensive platform that bridges the gap between security and IT operations. By integrating these two critical functions, ServiceNow empowers enterprises to proactively address security issues, automate processes, enhance overall cyber resilience and maintain a robust security posture.

List of key aspects of ServiceNow SecOps implementations include:

- **Security Incident Response (SIR)**: Helps to manage organizations SOC (Security Operations Centres) more efficiently. ServiceNow SIR helps to prioritize and swiftly respond to security threats using workflows and automation by connecting existing security tools, such that:
    1. **SecOps consumes Security Information and Event Management (SIEM) alerts in real-time, correlates them with other data sources, and initiates incident response. It enhances visibility into security events.**
    2. ServiceNow SecOps also integrates with Security Orchestration, Automation, and Response (SOAR) Platforms to automate incident response workflows. It orchestrates tasks, triggers playbooks, and streamlines incident handling.
    3. **SecOps connects with Endpoint Detection and Response (EDR) solutions to detect and respond to threats at the endpoint level. It automates actions based on EDR alerts.**
    4. **SecOps enriches incident data with real-time threat context by integrating with Threat Intelligence feeds. This helps prioritize and respond effectively to security incidents.**
- **Vulnerability Response (VR)**: Align business context with asset, risk, and threat intelligence for rapid mitigation. **SecOps connects with Vulnerability scanners and assessment tools to ingests vulnerability data, correlates it with asset information, and triggers remediation workflows.**
- **Configuration Compliance (CC)**: Identify, prioritize, and remediate misconfigured software.
- **Threat Intelligence Security Centre (TISC)**: Analyse and manage threat intelligence within a dedicated Threat Analyst Workspace.
- **DLP Incident Response**: Collaborates with Data Loss Prevention (DLP) solutions to manage incidents related to data exposure. It ensures sensitive data is protected and responds swiftly to breaches.
- **Security Posture Control (SPC)**: Manage the security of all your enterprise assets, both on-premises and in the cloud.
- **Performance Analytics for Security Operations**: Anticipate trends, allocate resources effectively, and continuously improve using real-time analytics.

Key AI Capabilities include

- **AI Driven Incident wrap up**: Automatically generates closure notes, resolution codes, and post-incident summaries.
- **Correlation insights**: AI surfaces related assets, users, observables within incidents

ServiceNow security operations helps security teams scale faster, smarter, and more efficiently. Moreover, it helps enabling and automating data and process between IT, Security and Risk to effectively respond and remediate threats.

List of key benefits this service offers:

- Build Cyber Resilience: SecOps helps organizations enhance their overall cyber resilience. By streamlining security operations, automating processes, and improving incident response capabilities, it ensures better preparedness against threats.
- Enhance Operational Agility: With SecOps, teams can respond swiftly and efficiently to security incidents. The platform's smart workflows, powered by artificial intelligence (AI), accelerate incident handling, and reduce manual effort.
- Prioritize Remediation: SecOps integrates risk-based vulnerability management. It aligns business context with asset, risk, and threat intelligence, allowing organizations to prioritize and swiftly address vulnerabilities.

1.2. Service Description

The EY ServiceNow practice is comprised of a team of practitioners drawn from technology, operational, consulting and business backgrounds, who collectively have advised and supported all types of clients implementing effective ServiceNow Cyber Security. This level of collective knowledge, experience and expertise is critical in providing recommendations, best practices and identifying any gaps and weaknesses and to propose strategic improvements that will drive improved project delivery and more sustainable steady state operations. EY maintains relevant accelerates (policies, procedures, and processes) that can be quickly modified to reflect a client's specific circumstances to accelerate the transformation.

This Service provides experienced ServiceNow professionals to support clients via a variety of engagement models:

- **Staff Augmentation:** providing EY consultants to join and support a client team which does not have at present, or need in the long term, specific ServiceNow experience, skills and knowledge (e.g. solution architect, integrations specialist, process configuration specialist, business change lead)
- **Project Team:** a group of EY consultants who take responsibility for a particular client project deliverable or operational improvement outcome (e.g. resourcing, training and standing up a dedicated ServiceNow Centre of Excellence)
- **Client Position Backfill:** providing a suitable experienced EY resource to act in a client role while that position is established and recruited or otherwise resourced (e.g. Platform Owner, Platform Architect, Data Manager, Process Manager)
- **Operational Support Agreements:** access to a team of EY ServiceNow staff providing operational support for existing platforms, higher-level technical support, hypercare for new releases or an "operate then transfer to client" model for new deployments (e.g. virtual admin, data migration, request catalogue configuration)

EY can provide staff at all levels of ServiceNow certification (all the way up to the highest level of Certified Master Architect) with a wide range of experience across all platform

capabilities. For those clients which require it, we have consultants who are BPSS, and SC cleared to work on projects requiring that level of security clearance.

EY's approach to providing ServiceNow services to clients goes beyond the more common technical platform implementation and configuration aspects. In reviewing and improving an organisations ServiceNow Cyber Security our approach can, if required, encompass the following aspects:

- **People:** are the required roles in place, is the security model effective, is governance working
- **Processes:** are processes measured and manged, do they have owners, do processes work end-to-end, are processes unnecessarily heavily customised
- **Systems:** is ServiceNow optimally configured, or are unnecessary customisations or other specific aspects driving higher support and maintenance costs, are all the available modules being used
- **Data:** is foundational data like assets, account and locations available, accurate, complete and up-to-date, is personal data suitably protected, are technology elements correctly associated with the business services they support to allow process automation and automatic incident priority assignment
- **Controls**: what IT General Controls and others such as SoX need to be applied to ServiceNow, how are they evidenced and what automation is possible
- **Integration:** how does ServiceNow interoperate with other systems, are there manumatic interfaces, are there functionality overlaps, can systems be consolidated and automated
- **Affordability:** how do the measurable business value benefits resulting from using ServiceNow measure up against the total cost of ownership, where can costs be reduced and where can value be increased
- **Reliability:** are ServiceNow's operational performance, resilience, and recovery adequate in terms of the business risk and impact of degradation, outages and failures, what can be done to improve these factors
- **Security:** is access to the platform adequately manage, is there an authoritative Identity and Access Management system connected, are the Access Control Lists for accounts and groups correct, is personal and company confidential data adequately protected
- **Experience:** can staff easily find the information, knowledge, assets and support they need to be as productive as possible, are customers recommending your support portal to others, is there a one-stop-shop portal, is experience measured, what can be done to delight staff and customers
- **Speed:** how quickly can business units release new B2C applications via the formal Change Control process, how quickly can items be changes in the request catalogue, can change and request approvals be automated under agreed circumstances

1.3. Pricing

This service is priced in accordance with the SFIA rate card provided and can be modelled using a range of commercial approaches e.g. time & materials, fixed price, etc. 'Ordering and Invoicing' and 'Termination' are to be undertaken in accordance with G-Cloud 15 contract terms unless varied by mutual agreement and detailed within a call-off contract.

2. Key contacts

For further information please get in touch via the email address below.

Chris Fowler

Partner, Technology Consulting (ServiceNow)

Email: eytenders@uk.ey.com

EY | Building a better working world

About EY

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organisation, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organisation, please visit ey.com.

Ernst & Young LLP

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.

In line with EY’s commitment to minimise its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/uk