SECURING SERVICENOW

A CISO's Field Guide

Rachid Harrando

Former Principal Security Advisor,
ServiceNow

Founder, Nowisor

2026

While every precaution has been taken in the preparation of this book, the author assumes no responsibility for errors or omissions. Product features, interfaces, and capabilities described in this book may change after publication.

First edition, 2026.

nowisor.com

Disclaimer

This book is written for information and educational purposes only. It does not constitute legal, regulatory, or professional cybersecurity advice. Every organization's ServiceNow environment, regulatory posture, and risk profile is different. The guidance in these pages reflects the author's experience and professional judgment — it is not a substitute for a qualified assessment of your specific situation.

You should not act on anything in this book without first validating it against your own instance configuration, your organization's legal and compliance requirements, and the advice of qualified professionals — legal counsel, your DPO, your compliance team, and your ServiceNow administrators. Regulatory interpretations of NIS2, DORA, the Cyber Resilience Act, and the EU AI Act continue to evolve. What is described here reflects the regulatory landscape as of early 2026. Enforcement guidance, national transpositions, and court rulings may change the practical application of these requirements after publication.

ServiceNow platform features, product names, capabilities, and release contents described in this book are based on

publicly available documentation and the author's professional experience as of the time of writing. ServiceNow, Inc. may modify, rename, deprecate, or retire features at any time. The Australia release (GA: May 5, 2026) features discussed in several chapters were based on documentation available as of Knowledge 26 and may differ from the final shipped product in specific implementation details. Always verify current functionality against ServiceNow's official documentation for your specific release version.

This book is an independent publication. It has not been authorized, sponsored, endorsed, or reviewed by ServiceNow, Inc. The opinions expressed are the author's alone. References to ServiceNow products and features are made for educational purposes and do not imply any affiliation with or endorsement by ServiceNow, Inc.

The author and publisher disclaim all liability for any direct, indirect, incidental, or consequential damages arising from the use or misuse of the information contained in this book. Security is a continuous process, not a destination. No book, framework, or 90-day roadmap can guarantee that your organization will not experience a security incident. What this book can do is help you build a defensible posture —

but the responsibility for implementing, maintaining, and verifying that posture remains yours.

If any of this makes you uncomfortable, good. That discomfort is the beginning of taking your ServiceNow security seriously.

Table of Contents

Foreword: Why I Wrote This

I spent nine years inside ServiceNow as Principal Security Advisor. The CISOs I met were universally the same: blindsided.

ServiceNow had arrived as an IT ticketing system years ago. Somewhere between then and now, it became the operational backbone of their enterprise. HR onboards through it. Legal manages contracts there. Finance runs procurement. It holds more data than almost any other system they own.

No one told the security team.

I remember one conversation more than any technical failure. A CISO at a European financial institution—experienced, well-resourced, careful. He'd never heard of ServiceNow's shared responsibility model. Not because he was careless. Because nobody had ever explained it. His team had assumed ServiceNow handled security end to end. In nine years, I never once met a CISO who understood where ServiceNow's responsibility ends and theirs begins.

These same CISOs could talk for hours about their cloud infrastructure, their endpoints, their identity layer. They had

threat models for systems built five years ago. ServiceNow had been running for ten.

The real problem: ServiceNow doesn't look like a security problem. It looks like an IT operations tool. Implementation documentation talks about uptime and feature adoption. It never mentions the 1,500 access control rules that determine who can read your salary data via API.

I wrote this for the CISO who just realized they should care about ServiceNow. Who looked at the platform through a security lens and found nothing but questions. Who's facing a NIS2 or DORA audit and has no idea if ServiceNow is even in scope.

This isn't a technical manual. Your administrators can handle technical fixes once they know what to fix. This is the strategic briefing I wish someone had given every CISO I sat across from before the audit started.

By the time you finish this book, you'll know what your exposure actually looks like, what regulators will ask, and what a real security program for ServiceNow looks like.

Start with the twenty questions. Ask your admin this week. The answers will tell you what you need to know.

One thing I want to be clear about: this book is not a critique of ServiceNow. It is the opposite. The reason I could write it with this level of specificity is that ServiceNow genuinely listens. Over nine years, every gap I brought to the platform — every question a CISO asked that had no good answer — became a conversation. Many of those conversations became features. The Security Center, the Machine Identity Console, the AI Control Tower, the three-layer REST authorization model: these exist in part because practitioners pushed on the gaps and the product teams took it seriously. That culture of openness is rare. This book exists because of it. What it describes is not a broken platform. It is a mature, well-engineered platform that places significant security responsibility on its customers — and those customers deserve to understand exactly what that means.

— Rachid Harrando

Former Principal Security Advisor, ServiceNow

Founder, Nowisor

Acknowledgements

This book would not exist in its current form without the people who gave their time to read early drafts and push back where it needed pushing.

Martin Jensen, ServiceNow MVP, reviewed an early draft and provided sharp, specific feedback that improved the book meaningfully — from the opening hook through the conversation starters. His practitioner's perspective shaped the final version of several key sections.

Nick Sessa, ServiceNow MVP, CISSP, and founder of EntruLabs, provided technical review and feedback. Nick's work in the field — including the EntruLabs Top 10 ServiceNow Security Risks and the Damn Vulnerable ServiceNow Instance — represents some of the most rigorous public research on ServiceNow platform security available today. His input strengthened the technical accuracy of this book considerably.

Additional thanks to the broader ServiceNow security community, whose questions, war stories, and honest assessments over the years gave me the material to write this in the first place.

Chapter 1: The Platform Your Security Team Doesn't Understand

Ask yourself one question: if a regulator, an auditor, or your board asked you tomorrow to demonstrate control over the system that holds your employee data, your HR cases, your security incidents, your vendor contracts, and your IT access requests — could you answer?

For most CISOs, that system is ServiceNow. And for most of them, the honest answer is no.

Not because they're negligent. Because ServiceNow doesn't look like a security problem. It looks like the ticketing system. It was procured by IT operations. It was never included in the security team's scope. Nobody briefed the CISO on what it actually contains or how it actually works.

This book is that briefing. This chapter gives you the mental model you need — not the technical details of the platform, but the risk framing that changes how you think about it. The conversation with your administrator. The questions you should have been asking for the last three years.

If you leave this chapter with one thing, it's this: ServiceNow is not a SaaS application your vendor secures on your behalf. It's a custom application your organization built. And your organization is responsible for its security.

It Is Not a SaaS Application

Start here: ServiceNow is not Salesforce. It's not Workday. It's not the SaaS apps your security team has spent a decade learning to evaluate.

Those are relatively fixed systems. Fixed data models. Fixed integrations. Fixed UIs. You configure within boundaries the vendor set. The vendor owns the code. You pick the settings.

ServiceNow is fundamentally different. ServiceNow itself calls it an **aPaaS — Application Platform as a Service**. They provide the infrastructure, the runtime, and a set of base capabilities. Everything else — the data model, business logic, integrations, UIs, workflows — your team built. Or consultants built. Or former employees left behind three years ago.

That distinction — aPaaS, not SaaS — is the most important thing to understand about your security posture on this platform. You're not configuring a vendor's application

within defined limits. You're building your own application on their cloud. And like any custom application, its security is determined almost entirely by the choices made during development and configuration.

This matters because your SaaS security thinking doesn't apply. The questions that worked elsewhere — "Does it support SSO?", "Data encrypted at rest?", "What's their SOC 2 rating?" — are necessary. They're also completely insufficient. They address infrastructure. They don't touch the application layer you built.

Your exposure lives in that application layer.

Five Layers, Five Attack Surfaces

Your ServiceNow instance has five distinct layers. Each has its own security model, its own ways it breaks, and its own monitoring needs.

Layer 1: Identity and Access

ServiceNow sits on top of your corporate identity provider. SSO gets users in. Once they're inside, ServiceNow's RBAC determines what they see, what they do, what they export.

This is where most organizations leak their worst secrets. Roles pile up. Users get access for one project and keep it forever. Admins grant broad roles because scoping takes time. Integration accounts get admin because it's easier.

The result: role explosion. The actual access model bears no resemblance to what anyone intended. A mature enterprise instance has hundreds of users with access they shouldn't have, dozens of service accounts with way too much, and no trail showing how it happened.

The answer to role explosion is not simply removing access — it's replacing broad grants with purpose-built ones. ServiceNow provides a granular admin role model specifically for security functions: roles like sn_vsc.security_center_admin (Security Center access), mi_admin (machine identity governance), access_analyzer_admin (access comparison and simulation), identity_access_audit_viewer (ACL and audit trail review), and security_admin (security operations). A security engineer who needs to run access reviews and manage the Security Center does not need the admin role. They need two or three of these. The granular model exists. Most organizations never use it because nobody made the mapping.

ServiceNow's Security Center now includes an Access Analyzer — shows permissions for any user, role, or group, compares access between entities. It's powerful for finding role drift and permission creep. Whether your organization activated it and uses it in access reviews is the difference between actually seeing your exposure and guessing.

Your SSO doesn't protect you here. It can't see this. SSO knows who's authenticated. It doesn't know what they can access once they're inside.

Layer 2: The Data Layer

Ask your ServiceNow admin what's in your instance. Watch what happens. If you have a typical team, the answer is: "Well, ITSM started it, then HR joined, then Legal wanted contract management, then someone plugged in Finance for procurement… and yeah, it just kept going."

Data gravity. ServiceNow's designed to become your operational backbone. It integrates. It's extensible. It's convenient. So more and more processes move onto it. More and more sensitive data follows.

Your average enterprise instance holds five to eight different data classifications at once — routine IT tickets through

highly confidential HR — in one platform with one access control layer. That layer was probably designed when it only held tickets.

Knowing what's in your instance and whether its access controls match is one of the most important security things you can do. Most organizations haven't done it.

Layer 3: The Scripting Engine

ServiceNow runs a server-side JavaScript environment — Rhino-based historically, with ES2021+ support added from the Xanadu release onwards — executing with elevated platform privileges. Your team uses it constantly, usually without thinking about security. Business Rules on record creates. Script Includes for code libraries. Scheduled Jobs. Client Scripts in browsers.

Humans wrote all of it. Some of it was written years ago by developers long gone. Some copied from the community forum. Some contains logic errors that create vulnerabilities. Almost none has had a security review.

From an attacker's view — especially an insider or someone with compromised admin — this engine is incredibly useful. Server-side scripts run in system context by default, which

means they bypass the ACL framework that protects data from regular users. Execute arbitrary logic. Read any table. Exfiltrate through legitimate-looking channels. This isn't a flaw — it's how server-side scripting works on every enterprise platform. The flaw is having no visibility into what's actually running.

Your security team has no visibility into what code is running, when it changed, or what's dangerous in it.

Layer 4: The Integration Fabric

Your large enterprise instance probably has 200-400 active integrations. Each is a trust relationship — a system with permission to read or write your ServiceNow data.

Some were carefully designed. Many were quick fixes by admins solving right-now problems. Some talk to systems you don't use anymore. Some use credentials from years ago that nobody's rotated. Some use OAuth tokens that never expire.

These are non-human identities (NHIs). Applications, workloads, APIs, bots authenticating without a person at the keyboard. They don't follow human identity lifecycle rules. They don't change roles when someone moves. They don't

disable when people leave. MFA doesn't apply. Most organizations have no governance process for them.

Each integration is an entry point. Compromise the target system, you get that integration's permissions in ServiceNow. Compromise the credentials, you have API access to your data from anywhere on the internet.

MID Servers compound this. Java-based agents you install inside your own network so ServiceNow can reach on-premise systems. ServiceNow's cloud manages them, but they run inside your firewall with bidirectional access to both ServiceNow and your internal network.

Most organizations don't monitor MID Servers. They talk to ServiceNow over ports firewalls typically allow. In attacker terms: a perfect pivot point. A box inside the perimeter maintaining a persistent outbound channel to an external orchestrator.

Layer 5: The API Surface

ServiceNow exposes a comprehensive REST API for programmatic access to nearly everything in the instance. By design, it's powerful and flexible — that power is exactly what makes the integrations and automations enterprises

depend on possible. Configuring the authorization layer on top of it is the customer's responsibility, and it's one most organizations haven't fully addressed.

The Table API is your primary data mechanism. Authenticated users query tables they have ACL access to. In a poorly configured instance, any authenticated user can enumerate employee records, export security incidents, or pull credentials from catalog variables.

Your SOC can't tell the difference. An attacker pulling 50,000 users via Table API generates the same log entry as your ITSM sync. Without platform context — knowing what normal API patterns look like for each integration — your SIEM can't tell them apart.

Most SIEMs aren't configured for that. Most organizations haven't even tried.

ServiceNow's REST security model is evolving, and you need to understand where it's headed. Historically: table-level ACLs controlled data access. Zurich added a second layer: REST API Access Policies — control not just who accesses an endpoint but how (OAuth only, no Basic Auth), from where (IP ranges), and what specific resources and HTTP methods they can call. Australia adds a third: path-

based REST ACLs for individual endpoint and method authorization. A REST_Endpoint ACL can now restrict a Scripted REST API path to specific roles for specific HTTP methods — http_get, http_post, http_put, http_patch, http_delete — without modifying the API itself. All three layers are required: a request passes all or none. The model shifts from "who are you?" to "who are you, how are you connecting, and exactly what are you calling?" It's significant hardening. If you've configured it. Most organizations haven't, because they don't know it's there.

What Your Security Team Is Missing

If your security team has thought about ServiceNow, they've probably focused on perimeter security — ensuring SSO is set up, the instance isn't publicly accessible, vendor certifications are current.

Necessary. Not sufficient.

The real exposure isn't at the perimeter. It's inside — in configuration decisions accumulated over years, in ACL rules nobody's reviewed since they were written, in integrations nobody remembers approving, in code nobody's audited.

This interior exposure is invisible to standard security tools. Vulnerability scanners can't see it. SIEMs don't understand it. Pentesters probably didn't include it. Your cloud security posture tool doesn't have a ServiceNow plugin.

ServiceNow provides one native tool that helps. The Security Center — free from the Store, included by default from Vancouver onward — evaluates your instance against 200+ hardening settings and 50 metrics, producing a scored finding list for authentication, logging, access control, and configuration. It's queryable through scan_finding and gives you an objective baseline. But its scope is deliberately limited to platform-level config. It'll tell you if your session timeout is too long, if critical security plugins are disabled, if system properties are off best practice. It won't tell you if your ACL model fits your data sensitivity, if your Business Rules have exploitable logic, if integration accounts are over-provisioned, or if credentials are in catalog variables. That interior exposure — the attack surface you built on top — is beyond its scope. That's where your real risk is.

Your ServiceNow admins understand it best. They're focused on operations, not security implications.

That gap is where you leak.

The Five Questions to Ask This Week

Ask your admin these five questions before you read another page. The answers matter more than any assessment framework.

Question 1: "How many users have the admin role right now, and when was that list last reviewed?"

Well-managed instances have fewer than five admins, all named with documented business justifications. If you hear "I'm not sure" or the number's above ten, you have a role governance problem.

Question 2: "What systems have API access to our instance, and when were those credentials last rotated?"

This question always makes people pause. If your admin can't produce a complete list in 24 hours, your integration inventory is broken.

Question 3: "Which tables hold personally identifiable information, and what ACLs protect them?"

This maps your data exposure. You want a specific list — sys_user, sn_hr_core_case, others depending on your setup — and clear descriptions of who accesses them and how.

Question 4: "When was the last time someone reviewed your Business Rules and Script Includes for security issues?"

Most organizations: never. Custom ServiceNow code rarely gets security review. It gets written, deployed, forgotten.

Question 5: "Do you have MID Servers, and if so, what network segments can they reach?"

MID Servers get installed and ignored. Knowing their network access tells you a lot about lateral movement risk.

You don't need to be a ServiceNow expert. You need to be a CISO who knows the answers matter.

The Reframe

You've been thinking of ServiceNow as a vendor-managed SaaS app. A system where your security responsibility is limited to configuration within vendor-set boundaries.

That's wrong. It's a custom application you built on their cloud. It holds some of your most sensitive data. It has a scripting engine, an API surface, an integration fabric, an identity model. Your team configured all of it. Each can be misconfigured in ways that create serious risk.

The vendor secures the platform. You secure everything you built on it.

Most organizations aren't doing this. Not from carelessness. Because nobody framed it that way until now.

The rest of this book shows what doing it looks like. Chapter 2 starts with the first question: what's your actual attack surface, and how do you map it so your security team can act on it?

Chapter 6: NIS2, DORA, CRA, and the EU AI Act — What They Actually Require From Your Instance

European boardrooms. Past two years. A particular meeting type. CISO presenting regulatory compliance. ISO 27001 cert, SOC 2, GDPR records, cloud security tooling. Board satisfied. Questions routine.

Then someone asks about ServiceNow.

CISO pauses. ServiceNow is on the next slide. Under "Enterprise Applications." Listed as managed SaaS. Covered by vendor's SOC 2. Clear implication: vendor responsibility. Vendor is certified. Organization is compliant.

Wrong. And in 2025, regulators are beginning to notice this wrong.

NIS2, DORA, CRA don't care that you use ServiceNow. They care that you can demonstrate, at the configuration level, that your systems managing critical business processes meet specific security requirements. ServiceNow's SOC 2

covers ServiceNow infrastructure. Says nothing about your ACL configuration, integration security, data export controls, or incident response capability within the platform.

This chapter explains what each regulation actually demands from your ServiceNow instance. Not abstract regulatory language. Concrete: platform configuration and evidence generation.

Why These Three Regulations Matter Now

NIS2, DORA, CRA: generational shift in European cybersecurity regulation. Previous frameworks—ISO 27001, SOC 2, early GDPR—focused on policies, processes, organizational controls. Auditors asked: policy exist? Process exist?

New generation asks: can you prove it technically?

NIS2 Article 21: "appropriate and proportionate technical and organisational measures." The implementing rules specify those measures in detail previous frameworks didn't. DORA Articles 6–11: ICT risk management framework that must be demonstrably implemented, not just documented.

CRA: products with digital elements must meet verifiable security requirements, not just claim them.

The shift from policy-based to evidence-based compliance is what makes ServiceNow configuration suddenly visible to regulators. Policy saying "access to sensitive systems is governed by RBAC" is easy to write, easy to attest. Demonstrating that the 1,500 ACLs in your ServiceNow actually implement that policy—that no sensitive table is accessible to the wrong users, that no integration account has excessive permissions, that no credential data sits in unprotected variables—that requires technical evidence most organizations can't currently produce.

NIS2: Article 21 and Your ServiceNow Instance

NIS2 transposition deadline: 17 October 2024 across EU member states. Applies broadly: energy, transport, banking, financial infrastructure, health, digital infrastructure, public admin, others. If you operate in any of these sectors in the EU, or provide digital services to EU organizations, confirm with legal or compliance whether you're an "essential entity" or "important entity"—determines specific obligations and which supervisory authority you report to. In scope? Your

ServiceNow instance is almost certainly relevant to your compliance posture.

Article 21: core technical requirement. Ten specific domains. Five have direct implications for ServiceNow.

Article 21§2(a): Risk Analysis and Information System Security

Not just having a risk analysis policy. Having one that covers your actual systems including ServiceNow. Organization that has thoroughly assessed cloud, endpoints, network, but never formally assessed ServiceNow security posture? You have a compliance gap.

Evidence requirement: documented risk assessment that addresses ServiceNow as a distinct system, identifies the data it holds, maps access control, evaluates exposure patterns from Chapters 2 and 3. Generic IT risk framework document doesn't cut it unless it addresses platform-specific risks of your configuration.

Article 21§2(b): Incident Handling

NIS2 requires documented incident handling. Article 23 adds notification requirements. ServiceNow security

incident occurs—authentication bypass, compromised integration, malicious insider—you must detect, contain, assess impact, notify authorities within defined timeframes.

Article 23 timelines: early warning to national CSIRT within 24 hours of awareness, full notification within 72 hours, final report within one month.

Detection is where organizations have their ServiceNow gap. As Chapter 4 describes, ServiceNow incidents are hard to detect with standard SIEM tooling. If your incident capability relies on SIEM alerting on anomalous ServiceNow activity, and your SIEM doesn't have ServiceNow-specific detection logic, your compliance is theoretical, not actual.

Article 21§2(i): Access Control and Asset Management

Most direct regulatory requirement for your ServiceNow access control model. Article 21§2(i): documented access control policies and their implementation. For ServiceNow, demonstrate that:

Role model is documented, reflects least privilege. Role assignments reviewed within defined period. Service

accounts have documented owners and scoped permissions. Access removed promptly when employees change roles or leave. ACL configuration on sensitive data tables has been reviewed and validated.

Each demands evidence. Not policy documents. Technical records showing the review happened, who did it, what they found, what changed. Most organizations can't currently produce this for ServiceNow.

Article 21§2(g): Cyber Hygiene and Patch Management

Core hygiene practice: patch management. Chapter 4 discussed this—ServiceNow provides patches promptly when vulns are found. Your obligation: apply patches within defined timeframe and demonstrate you did.

Document your patch process for ServiceNow. Record when patches available, when applied, target SLA for critical security patches. Organization that patched the authentication bypass three days after release, without documented process or timeline? Weaker compliance posture than one with structured patch management and clear SLAs.

Article 21§2(f): Effectiveness Assessment

Continuous verification requirement. NIS2 doesn't just require implementing security measures. Requires assessing whether they work. For ServiceNow: periodic reassessment of configuration posture. ACL reviews, integration audits, access validations, export monitoring reviews on defined schedule, documented with findings and remediation.

One-time assessment satisfies the assessment period. Doesn't satisfy continuous verification. Demonstrating compliance requires repeatable assessment process, not point-in-time audit.

DORA: ICT Risk Management and Your ServiceNow Instance

Digital Operational Resilience Act: financial entities—banks, insurers, investment firms, payment institutions—and their critical ICT third-party providers. Financial entity operating in the EU? DORA enforceable since January 2025.

For most financial entities using ServiceNow, it's a critical ICT system. Manages IT service delivery, HR, vendor relationships, risk management, compliance tracking.

Unavailability or compromise has material impact. That makes it relevant to your DORA obligations.

Articles 8–11: ICT Risk Management Framework

DORA Articles 6–11: implement comprehensive ICT risk management framework. Articles 8–11 structure around four pillars with direct ServiceNow implications.

First, identification (Article 8): identify and document ServiceNow as an ICT asset, classify its data, map connections to other systems. The integration inventory from Chapter 2 is a DORA Article 8 prerequisite—can't manage integration risk without inventory.

Second, protection (Article 9): implement protective measures proportionate to risk. ACL configuration, access governance, credential management throughout this book are the technical implementation. Measures must be documented, implemented, verifiable.

Third, detection (Article 10): capabilities to detect anomalous activity in your ServiceNow instance. SIEM gap becomes regulatory issue here. DORA Article 10 requires detection—detecting ServiceNow-specific threats requires

ServiceNow-specific monitoring logic most SIEMs don't have.

Fourth, response and recovery (Article 11): documented response procedures for ICT incidents affecting ServiceNow, including recovery time objectives and tested procedures. No ServiceNow-specific section in your incident runbook? Your Article 11 documentation is incomplete.

Fifth, incident reporting (Articles 17–19): report major ICT incidents to competent authorities using structured classification and framework. Australia release introduces Digital Resilience Incident Reporting Export—JSON export of incident action tasks with automatic currency conversion, designed for DORA reporting. Run incident management on ServiceNow? This feature provides native path from incident record to regulatory submission, eliminating manual translation.

Article 28: ICT Third-Party Risk Management

DORA Article 28: risk of ICT third-party providers. ServiceNow, as cloud platform running critical processes, is in scope. Financial entities must assess concentration risk of critical ICT dependencies, maintain contracts with specific

security requirements, monitor third-party providers ongoing.

ServiceNow specifically: Article 28 requires understanding and documenting the shared responsibility model. Chapter 5's exercise, exactly. Contracts with ServiceNow should address security obligations. Monitoring includes Trust Portal, security advisories, patch releases. Assumption that ServiceNow handles all security isn't compliant. Understanding and documenting the boundary is.

The Cyber Resilience Act: A Different Kind of Obligation

CRA (Regulation (EU) 2024/2847): entered force 10 December 2024. Manufacturer reporting from September 2026. Full applicability from December 2027. Distinct from NIS2 and DORA in important ways.

NIS2 and DORA regulate organizations by sector. CRA regulates products—specifically products with digital elements placed on the EU market. Primary targets: manufacturers and developers of software and hardware.

For ServiceNow customers: two distinct obligations worth understanding separately.

ServiceNow as a product manufacturer. ServiceNow, Inc. manufactures a product with digital elements—the ServiceNow platform. CRA requires ServiceNow to demonstrate their product meets security requirements: security by default, documented vuln handling, security updates for defined support period, customers receive security information needed to use it securely.

That obligation is ServiceNow's, not yours. ServiceNow's existing practices—vulnerability disclosure, patch cadence, Trust Portal transparency—align well with CRA. Your obligation: verify vendor meets CRA requirements and document it.

Your organization as a product user with obligations. If you use ServiceNow to build products or services you place on the EU market—software company using ServiceNow for customer support with EU customers, for example—CRA requirements for your products may extend to infrastructure security supporting them.

More directly: if you develop software or hardware products and use ServiceNow to manage security vulnerability

handling for those products—tracking vulns, managing patches, coordinating disclosure—CRA requires that process meet specific standards. ServiceNow is excellent for implementing CRA-compliant vulnerability management. Implementing correctly requires the access control and data governance practices throughout this book.

The EU AI Act: Deployer Obligations for AI-Enabled Platforms

EU AI Act (Regulation (EU) 2024/1689): entered force 1 August 2024. Risk-based framework for AI systems across the EU. NIS2, DORA, CRA regulate cybersecurity. AI Act regulates AI use, deployment, governance itself. Enabled Now Assist? Deployed AI Agents? Using generative AI? Act creates obligations alongside your existing regulatory requirements.

AI Act classifies into four risk tiers: unacceptable (prohibited), high (comprehensive requirements), limited (transparency), minimal (none). Timeline staggered: prohibited practices and AI literacy from February 2025, General-Purpose AI models from August 2025, full high-risk requirements from August 2026.

For ServiceNow: most consequential question is whether your AI workflows fall into high-risk. Annex III defines high-risk use cases. Several directly relevant to ServiceNow. Use Now Assist or AI Agents in HR to make or materially influence employment decisions, worker management, task allocation, performance monitoring? Those are high-risk under Annex III, Category 4. AI workflows influencing essential services access, credit decisions, insurance assessment through ServiceNow? May qualify as high-risk under other Annex III categories.

Article 26: The deployer's obligations. AI Act distinguishes providers (develop AI systems) from deployers (use them). ServiceNow is the provider. You are the deployer. Article 26 places specific obligations on deployers of high-risk AI that can't be delegated.

First: use the AI system per instructions that accompany it. Your teams understand and follow ServiceNow's documented guidance for Now Assist and AI Agent config. Don't just enable and hope. Second: human oversight by competent, trained, authorized persons who can effectively oversee AI operation. Third: monitor for risks and report serious incidents to provider and market surveillance authority. Fourth: when AI makes decisions affecting natural

persons—your employees in HR scenarios—inform them they're subject to AI and provide ability to request human review.

AI literacy: an obligation that applies now. Article 4: organizations deploying AI systems must ensure sufficient AI literacy among staff, proportionate to use context. This obligation applied February 2025. Not future. ServiceNow admins configuring Now Assist skills, process owners deploying AI Agents, HR teams using AI-assisted case resolution must have documented training on how AI features work, limitations, how to interpret outputs. Training gap is compliance gap.

ServiceNow's positioning as provider. ServiceNow has moved toward AI Act alignment. ISO 42001 certification for AI management systems. Signed EU AI Code of Practice in 2025. Both strengthen your provider compliance position. AI Control Tower, especially with Australia enhancements, provides operational infrastructure for deployer obligations: AI agent inventory supports risk classification, Quality and Safety scoring enables monitoring, anonymous reporting capability designed for EU AI Act readiness provides incident and concern reporting mechanism. These don't

automatically make you compliant, but provide platform-native capabilities to implement required controls.

Practical implication: EU AI Act adds governance layer on top of security controls in this book. Securing Now Assist and AI Agents is necessary but insufficient. Also classify by risk tier, implement human oversight, ensure transparency to affected individuals, maintain logs, monitor for AI-specific risks. Chapter 7 addresses these as extension of Control 10.

Data Residency and Cross-Border Transfers

European and Middle Eastern CISOs ask this in nearly every ServiceNow conversation, cuts across NIS2, DORA, GDPR: where is our data and where does it go?

ServiceNow operates data centers in multiple regions. Customers select hosting region at contract. Most European customers: EU-based instance. They publish data center locations, sub-processor list, DPA addresses GDPR Chapter V transfer requirements. At infrastructure level, commitments are clear and documented.

Hyperscaler architecture available from Zurich gives customers more regional flexibility. Host on AWS, Azure, GCP in specific regions: UAE on Azure, Saudi Arabia, Qatar, Israel on GCP. Customer app nodes and databases in chosen Hyperscaler region. But the architecture isn't pure Hyperscaler: edge network services including load balancers, DNS, key management, identity infrastructure, SIEM integration route through ServiceNow's colocation facilities. Middle East regions: ServiceNow Cloud Network maps to Germany, so edge traffic for KSA-hosted GCP transits German infrastructure. Not a data residency violation per se—customer data at rest stays in chosen region—but data flow detail your DPO and legal should know when documenting transfers.

Hyperscaler introduces a fourth party to shared responsibility. Standard Commercial Cloud: customer and ServiceNow. Hyperscaler: four-party—you as data controller, ServiceNow as processor, colocation operator, Hyperscaler CSP. Each has documented responsibilities. ServiceNow publishes responsibility matrix. For CISOs: your third-party risk assessment must account for Hyperscaler as distinct entity in your ICT supply chain. Directly relevant to DORA Article 28.

The gaps CISOs miss aren't at infrastructure level. They're in the operational data flows above it.

Transfer mechanisms and their limits. ServiceNow's DPA governs cross-border transfers through EU Standard Contractual Clauses. Module Two (controller-to-processor) when you're a controller, Module Three (processor-to-processor) when you're a processor. UK International Data Transfer Addendum and Swiss provisions separate. DPA also allows alternative mechanisms like Trans-Atlantic Data Privacy Framework if available. Your obligation: confirm which module applies, verify SCCs properly executed in your ServiceNow agreement, document in your GDPR Article 30 records. DPO hasn't confirmed your SCC module? That's a documentation gap.

Sub-processor awareness. ServiceNow uses sub-processors for platform functions—support tooling, infrastructure ops, analytics. Each potential data transfer. DPA requires 30 days' notice before new sub-processor engagement, grants you right to object if sub-processor can't process personal data per DPA. Unresolved objection remedy: termination with refund of unused fees. Meaningful right, but requires someone monitoring sub-processor notifications from Support Portal. Most organizations

reviewed the list during procurement and haven't touched it since. Sub-processors change. Keep your assessment current.

AI and generative model data flows. Data residency question that's changed fastest. Now Assist processes in ServiceNow data centers by default, but during high demand may "burst" inference to Microsoft Azure to maintain performance. Behavior customers can opt out of through Now Assist Admin Console, but enabled by default. Third-party LLMs: more complex. Documentation notes providers may dynamically route globally, regional processing may differ from order form. Data sent to external provider for inference creates distinct cross-border transfer from instance hosting. Legal mechanism governing—covered by existing DPA, separate AI addendum, or model provider terms—explicitly confirm with your account team and review with DPO. Customers can enable Data Privacy for Now Assist using real-time anonymization through Generative AI Controller, strips sensitive patterns from prompts before LLM, and Now Assist Guardian monitoring for prompt injection and harmful content. Protective controls, not defaults. Enabling is customer-side decision. Not theoretical: GDPR Article 44 requires lawful transfer

mechanism for every cross-border flow, regulators increasingly scrutinize AI transfers.

Instance clones and disaster recovery. Production clone hosted where? ServiceNow disaster recovery failover in same jurisdiction? Hyperscaler: backups retained in Hyperscaler environment, failover instance under Advanced High Availability in second Hyperscaler region, possibly different jurisdiction. Answers are in your contract but most security teams never verified against data residency requirements. Middle East organizations with data localization obligations (UAE PDPL, Saudi PDPL, Bahrain PDPA): Hyperscaler option provides in-region app nodes and databases, but edge services and ServiceNow Cloud Network location map to Germany or APAC, meaning operational traffic crosses jurisdictional boundaries.

Log and telemetry data. When ServiceNow logs export to your SIEM or Log Export Service forwards platform telemetry, destination is your infrastructure. ServiceNow's operational telemetry—data they collect for platform monitoring, performance analytics, support—may process in different region. Understanding which operational data ServiceNow retains, where, how long is part of your GDPR Article 30 records obligation.

Straightforward practical steps: get your current DSA and DPA from ServiceNow (publicly available but confirm your executed versions), verify applicable SCC module. Request current sub-processor list. Confirm production and sub-production hosting locations. Register designated security contact in Support Portal for breach notifications. Ask your account team explicitly where AI inference happens. Access CORE portal to review latest SOC 2 Type 2 and pentest executive summary. Available at no cost under DSA Section 2.2, most customers never accessed them. Document everything. This documentation is the foundation of your data residency and vendor governance evidence. Regulators in Europe and Middle East increasingly ask to see it.

The Evidence Gap: What Regulators Will Ask

Understanding regulatory requirements is necessary. Understanding what auditors and regulators will ask for is equally important. The gap between regulations and what you can evidence is where compliance risk actually lives.

Based on NIS2 Article 21, DORA Articles 8–11, CRA guidance, and EU AI Act deployer obligations, here's what

a regulator examining your ServiceNow posture will want to see:

Access control evidence. Current list of all privileged users with documented business justification for each. Record of most recent access review: date, reviewer, scope, findings. Evidence that departed employees' access was removed per your offboarding SLA.

Integration security evidence. Current inventory of all API integrations: tables each can access, credentials in use, last credential rotation date. For integrations without documented owner, evidence that access was reviewed and confirmed still required.

Configuration review evidence. Documentation of most recent security review of ACL config: scope of tables reviewed, methodology, findings, remediation taken or planned.

Patch management evidence. Record of security patches from ServiceNow, date applied to production, target SLA for critical patches.

Incident detection evidence. Documentation of your monitoring capability for ServiceNow security events: what

logs collected, where sent, what alerting configured. Evidence testing has occurred.

Data classification evidence. Documented inventory of categories of personal and sensitive data in ServiceNow, with ACLs governing access to each.

Most organizations asked to produce this evidence today cannot. Not because controls don't exist—many do—but because they've never been documented, consolidated, or produced as a coherent compliance package.

Producing this is not a compliance project. It's an operational security project that happens to satisfy compliance. The controls generating this evidence are the ones that reduce actual risk. They're in Chapter 7. The 90-day roadmap in Chapter 8 is designed to implement them.

The Conversation to Have This Week

Before the next chapter, one practical step worth taking now.

Ask legal or compliance whether your organization is in scope for NIS2, DORA, CRA, or EU AI Act. If so, which articles are relevant to ICT risk management and AI governance.

Then ask your ServiceNow administrator: "If a regulator asked tomorrow whether our ServiceNow meets Article 21 access control obligations, what evidence could we produce?"

The gap between the requirement and the honest answer is your compliance risk. It's also the risk the second half of this book is designed to help you close.