Synechron

Whitepaper

The Surprising Journey to a Trusted Instance

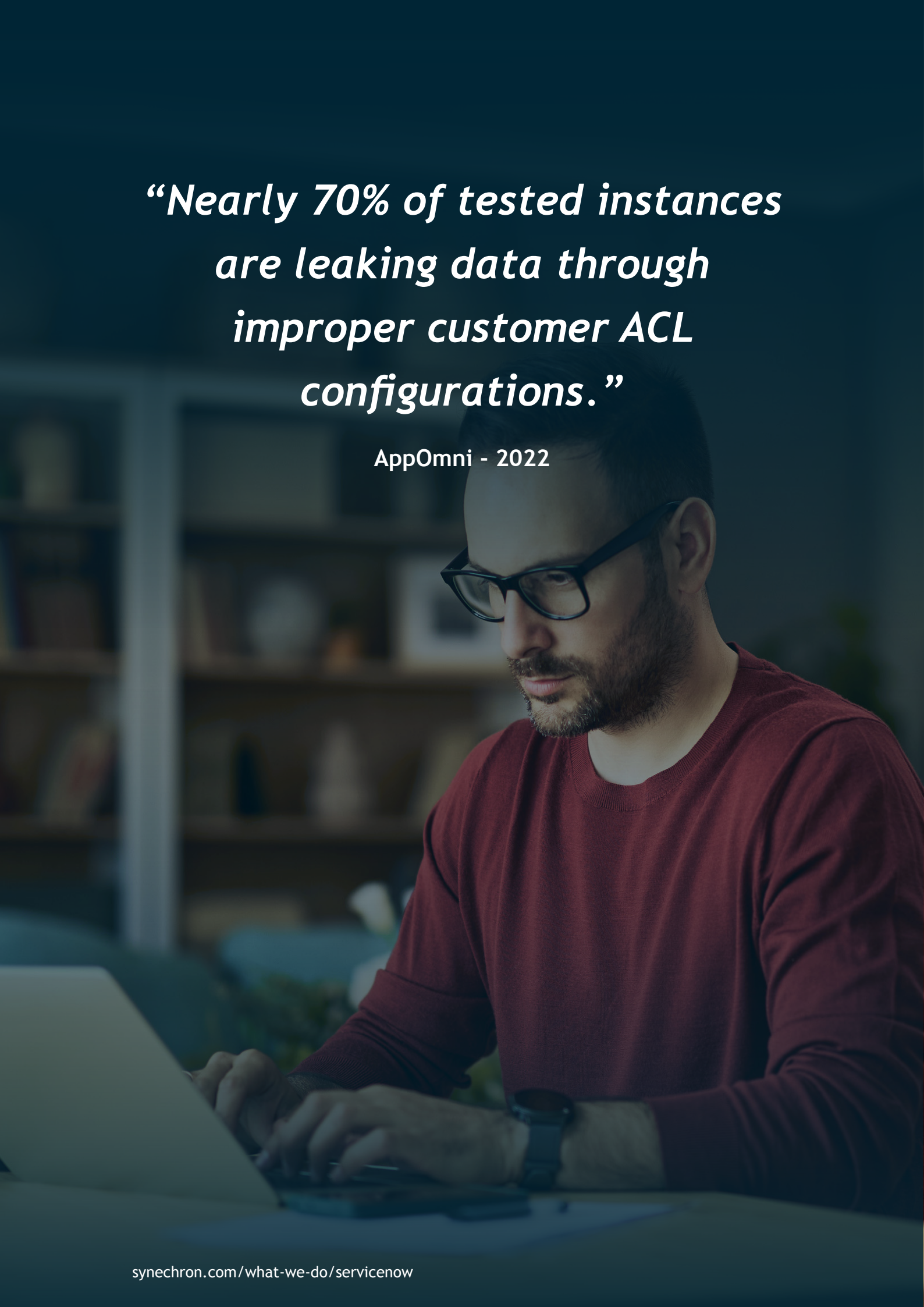
Creating sound foundations for avoiding breaches and penalties.

Richard Taylor

Head of Resilience,
Synechron | ServiceNow

“Nearly 70% of tested instances are leaking data through improper customer ACL configurations.”

AppOmni - 2022



The criticality of sound foundations

In an era where Personal Identifiable Information (PII) and critical operational data are increasingly present, processed, and reliant on ServiceNow instances, the necessity for robust data protection and resilience is more pressing than ever.

Heightened regulatory requirements and a rapidly evolving threat landscape underscore the urgency of elevating and sustaining anomaly detection, continuity verification, and robust protection well beyond the current state for most organisations.

Insights from leading Configuration and Compliance Scanning vendors, such as AppOmni, reveal vulnerabilities that expose organisations to concentration risk and potential continuity disruptions, which threat actors may soon exploit. This whitepaper recommends actionable steps that can shield your organisation from these risks, strengthening resilience at each layer.

Strengthening foundations

Imagine owning an estate in rural France as a friend of mine once did. Contrary to the romantic TV depictions, estates are costly and challenging to maintain. But the true surprise for my friend revealed itself with the first really heavy rainfall, when he experienced water rising-up through the floor—an issue unimaginable with modern building standards.

This unexpected flooding was due to the lack of any real foundations! Historical buildings, like his converted Napoleonic era coaching inn, often lacked firm foundations, which at the time were reserved for significant buildings such as a large chateaux. Everyday homes were simply built directly on the ground without the necessary structural integrity below.

Does this construction approach "work"? If by "work" we mean the structure doesn't result in immediate structural failure, then yes, it works. But if "work" means a secure, resilient structure in all conditions, then it certainly does not achieve any level of dependability.

Many organisations today find themselves in a similar situation with their security foundations—functioning adequately under normal circumstances but lacking resilience to withstand serious threats. ServiceNow's integrated hardening and penetration testing offers a foundational level of security compliance, yet this typically addresses a layer beneath where the client operates and where critical configurations reside. Strengthening this foundation is imperative for safeguarding sensitive data and ensuring operational continuity at every level.

"'Work' means a secure, resilient structure in all conditions."

Strengthening your ServiceNow security framework

ServiceNow’s built-in security, known as its CORE methodology, offers a foundational level of hardening. However, while this system provides essential compliance on one level, clients bear the responsibility for the configurations, applications, and custom data layers within their operational domain. Consequently, organisations must engage in proactive measures and strategic oversight to extend protection to these layers.

The following diagram from Securing the Now Platform (servicenow.com) illustrates the shared responsibility model essential for ensuring the security and resilience of your ServiceNow instance. This model establishes a “triality” of responsibility, where accountability is distributed among three key stakeholders: ServiceNow, any applicable data centre providers, and you, the customer.

Area of Responsibility	Responsibility		
	Customer	ServiceNow	Colocation (Data center providers)
Secure configuration of instance	●		
Authentication and authorisation	●		
Data management (classification and retention)	●		
Data encrytion at rest	●		
Data encryption in flight	●	●	
Encryption key management	●	●	
Security logging and monitoring	●	●	
Secure SDLC processes	●	●	
Penetration testing	●	●	
Vulnerability management	●	●	
Privacy	●	●	
Compliance: regulatory and legal	●	●	●
Employee Vetting or Screening	●	●	●
Physical Security & Environment Controls		●	●
Cloud infrastructure security management		●	
Infrastructure management		●	
Media disposal and destruction		●	
Backup and restore		●	
Business continuity and disaster recovery		●	

ServiceNow’s role encompasses platform-level hardening, compliance, and baseline protections. Data centre providers, where relevant, are responsible for the physical infrastructure and underlying cloud services. Finally, the customer holds responsibility for safeguarding their specific configurations, data integrity, and operational processes within the instance. This division underscores the need for each party to uphold its responsibilities to maintain a secure and resilient operational environment.

Beyond “Best Practice”: Regulatory requirements and the essential role of ServiceNow instances.

The question of whether securing ServiceNow and third-party configurations is merely a “best practice” — an often-overused term — is both common and critical. Some users may assume that minimal effort will suffice, with proactive actions being unnecessary until an incident occurs. However, Synechron strongly advises against this approach, particularly in light of stringent regulatory frameworks, which hold organisations accountable for lapses in data security and resilience. Regulatory bodies, such as those overseeing the EU Digital Operational Resilience Act (DORA), GDPR, and the NIS2 directive, impose substantial fines — up to 4% of global turnover, as well as potential criminal liabilities for non-compliance.

The responsibility of data protection and organisational resilience.

The GDPR directive, including Articles 25.1 and 28.2, mandates the application of “technical and organisational measures” to protect data. The onus of this responsibility falls on designated role holders (such as the Data Protection Officer, Controller, and Processor) rather than on ServiceNow alone. In essence, the security of your data is ultimately your responsibility.

From an operational resilience standpoint, international regulatory authorities provide specific guidance to ensure organisations establish robust resilience postures:

- **Bank for International Settlements (BIS):** The BIS Principles for Operational Resilience (Sections 3, P8 & P9) outline that service providers must be integrated into an organisation’s resilience strategy, closely understood, and actively monitored to support Business Continuity and Risk Management initiatives.
- **Bank of England/FCA (UK):** UK regulations (PS21/3, FCA Handbook) require organisations to actively manage relationships with third-party providers, particularly those delivering essential services. Organisations must understand that any failure to remain within impact tolerance is their own responsibility, not that of the provider.

- **EU Directives – NIS2 & DORA:** The NIS2 Directive requires each Member State to adopt national strategies for achieving high cybersecurity standards in critical sectors, including policies for supply chain security. DORA (Article 63) expands this scope, covering a wide array of ICT third-party service providers, including cloud computing, software, data analytics, and data centre services.
- **US Federal Reserve – Operational Resilience Guidance:** This guidance emphasises that firms should identify critical operations and dependencies, including those related to third-party providers, within their resilience and recovery plans.
- **Australian Prudential Regulation Authority (APRA):** APRA's CPS standards mandate that regulated entities maintain continuity of critical operations within defined tolerance levels during severe disruptions. This includes having a credible Business Continuity Plan (BCP), as well as effective risk management policies, formal agreements, and continuous monitoring for service providers.

Given the increasing criticality of ServiceNow instances, they are rapidly evolving their role to serve as pivotal third-party providers. This shift demands that organisations address ServiceNow security with the same rigour applied to other high-impact third-party services for compliance, aligning with internal and external standards.

The structure of a typical ServiceNow instance (servicenow.com)

ServiceNow security framework: Layering protection across the platform

To better understand the significance of securing your ServiceNow instance we need to explore the components of a standard ServiceNow setup. This will clarify the importance of each layer in maintaining data security, operational continuity, and regulatory compliance.

At its core, the ServiceNow platform is supported by the NonStop Cloud infrastructure and data centres, collectively enabling the APaaS offering. These foundational layers are managed with protective measures aligned to ISO27002 standards, along with other global standards such as US federal guidelines (https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf). However, as customers, your operational environment extends beyond the platform's foundation into additional layers that encompass:

- **Backup and recovery configurations**
- **Platform-specific configurations**
- **Custom applications and integrations**
- **Data integrity and security for both organisational and customer data**
- **The collective environment of people, processes, partners, and tools**

Laying the foundations: A Zero Trust approach.

To build resilience across these layers, we recommend a methodical, "Zero Trust" approach. This methodology extends beyond Network Access Control and encompasses the broader organisational mindset of "trust nothing, test everything." Principles of RACI, least privilege, and separation of duties are essential. Implementing these across all layers will form a strong, evidence-based approach, driving security culture throughout the enterprise.

Layered security approach: A multi-floor structure.

This layered approach can be visualised as a multi-storey building, where each floor represents a critical area of your ServiceNow instance that requires targeted protection:

1. Foundations – Zero Trust and low technical debt
Start with an outcome-focused and Zero Trust-centric mindset. This should guide every layer above. Lever out of the box (OOTB) capabilities to minimise technical debt and reduce the risk surface. Built-in tables, dashboards, and tools like the Instance Security Centre can provide actionable insights for proactive protection.

2. Ground Floor – Physical and configuration security

- Backup and recovery capabilities: Integrate comprehensive backup and recovery measures beyond the basic 14-day ServiceNow platform backup. For example, OwnBackup (a ServiceNow partner) provides data continuity and regulatory evidence for both internal policies and external obligations, ensuring your operational resilience.
- Regulatory compliance: Demonstrating backup configuration and business continuity is essential, especially in regulated industries, where historical point-in-time recovery and data audit trails may be mandatory.

3. **First floor – Configuration and application security**

- Configuration scanning and security posture: Assess platform configurations regularly using a Security Configuration Analysis tool to identify any vulnerabilities. For example, AppOmni can detect potential configuration gaps that expose your instance to external access risks. It provides automated evidence for both internal and regulatory obligations.
- Regulatory compliance: Regular scans are crucial to continuously maintain a secure configuration and to provide documentation required by both internal policy and external regulations.

4. **Second floor – Application and data security**

- Code scanning: Scan custom code for vulnerabilities that may introduce compliance or security risks. QualityClouds, another ServiceNow partner, supports automated scans of developed applications to ensure they meet compliance requirements and avoid common security pitfalls.
- Regulatory compliance: QualityClouds facilitates ongoing verification for compliance, aligning with internal and external standards.

5. **Penthouse – Data and insights**

- Outcome and value-driven analytics: Lever your Digital Twin/CMDB /Unified Industry Data Model, linking it to enterprise objectives, from back-up status to vulnerabilities and compliance metrics. This alignment allows for real-time insights and enhances risk visibility for executive leadership.
- Human-centred experience: Ensure insights are accessible through AI or natural language queries, enabling non-technical stakeholders to interpret data effectively without requiring coding expertise.

Achieving trusted outputs through Zero Trust inputs.

By adopting this Zero Trust framework, organisations can achieve fully trusted, resilient outputs across their ServiceNow environment. Addressing Concentration Risk is particularly vital, as organisations increasingly rely on ServiceNow for essential functions such as:

- **Policy & compliance management**
- **Risk and audit management**

- **Business continuity management**
- **Security and vulnerability response**
- **Financial services operations**

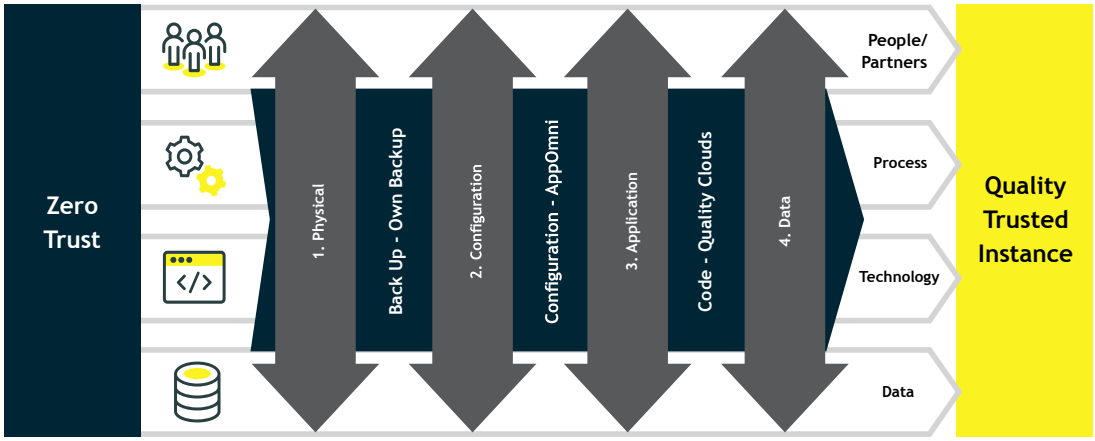
This holistic approach mitigates concentration risks inherent in a single platform by providing comprehensive systemic protections, including:

- **Backup and recovery**
- **Security safeguards**
- **Compliance controls**
- **Auditing**
- **Monitoring and observability**

"By adopting this Zero Trust framework, organisations can achieve fully trusted, resilient outputs across their ServiceNow environment."

Get started on your journey to a trusted instance

The essence of this whitepaper is simple: Identify, Define, Analyse, and Protect/Prevent. Relying on security through obscurity is insufficient, as it offers only fleeting protection with costly consequences when it fails.



A multi-layered, integrated, and defence-in-depth strategy is essential to protect your ServiceNow instance. This approach, leveraging the platform's out-of-the-box (OOTB) capabilities and tables alongside tailored tooling, is the only sustainable solution to meet today's threat landscape and rigorous regulatory requirements. Implementing this in a phased, pragmatic manner minimises disruption and optimises cost-efficiency while aligning to both internal policies and external regulatory standards.

The investment in a structured resilience strategy is far less than the potential costs of regulatory fines, reputational damage, customer attrition, and the internal pressures resulting from security incidents. A proactive approach not only protects organisational assets but also strengthens trust and operational confidence, providing a solid foundation for long-term resilience. Future options to failover ServiceNow instances, to non-ServiceNow cloud raises other intriguing continuity possibilities. These will be considered in future updates of this whitepaper.

Sources:

1) AppOmni misconfiguration estimates - AppOmni Discovers Security Misconfiguration Impacting ServiceNow
2) General Data Protection Regulation - Regulation - 2016/679 - EN - gdpr - EUR-Lex (europa.eu)
3) IBM Data Breach costings 2023 - Cost of a data breach 2023 | IBM
4) Bank for International Settlements (BIS) - Principles for operational resilience (bis.org)
5) FCA Position Statement on building Operational Resilience PS21/3 - PS21/3 Building operational resilience | FCA
6) EU Network & Information Security Directive - EUR-Lex - 02022L2555-20221227 - EN - EUR-Lex (europa.eu)
7) Federal Reserve - The Fed - Supervisory Policy and Guidance Topics - Operational Resilience (federalreserve.gov)
8) APRA - Operational risk management | APRA

Synechron

Capture your future faster.

Synechron is an elite ServiceNow partner, experienced in delivering major transformations at scale for clients operating in complex and highly regulated environments - all delivered by our world-class team.

- Transform at scale
- Engineer expertly
- Build in resilience
- Accelerate with AI

servicenow
PREMIER
Partner
Consulting & Implementation

Richard Taylor

Head of Resilience, Synechron | ServiceNow

Richard is a highly experienced ServiceNow veteran and well known in GRC/IRM circles. He has a real passion for embedding resilience early and effectively into the heart of every organisation.

Contact us:

Synechron Limited, 95 Gresham Street,
London - EC2V 7NA, United Kingdom

servicenow@synechron.com