



Asset Management (IT/OT) & Vulnerability Management



01

IT Asset Management

What it is:

A service to establish trusted visibility and control across technology assets

CIOs, CISOs



IT Asset Managers & Specialists



Software & Hardware Asset Managers



Why it matters

Fragmented asset records, incomplete discovery and unclear ownership create security blind spots, cost leakage and compliance risk.

As technology estates expand across endpoints, cloud, SaaS, IoT, OT and AI, organisations need reliable asset context to identify exposures, prioritise remediation and make informed lifecycle decisions.

Strengthen asset visibility, governance and lifecycle control, enabling risk-informed technology and investment decisions.

What it does: Establish visibility, control and lifecycle intelligence

Discover technology assets,

Establish trusted visibility.

Connect ownership and dependencies

Enable accountable decisions.

Govern asset lifecycles

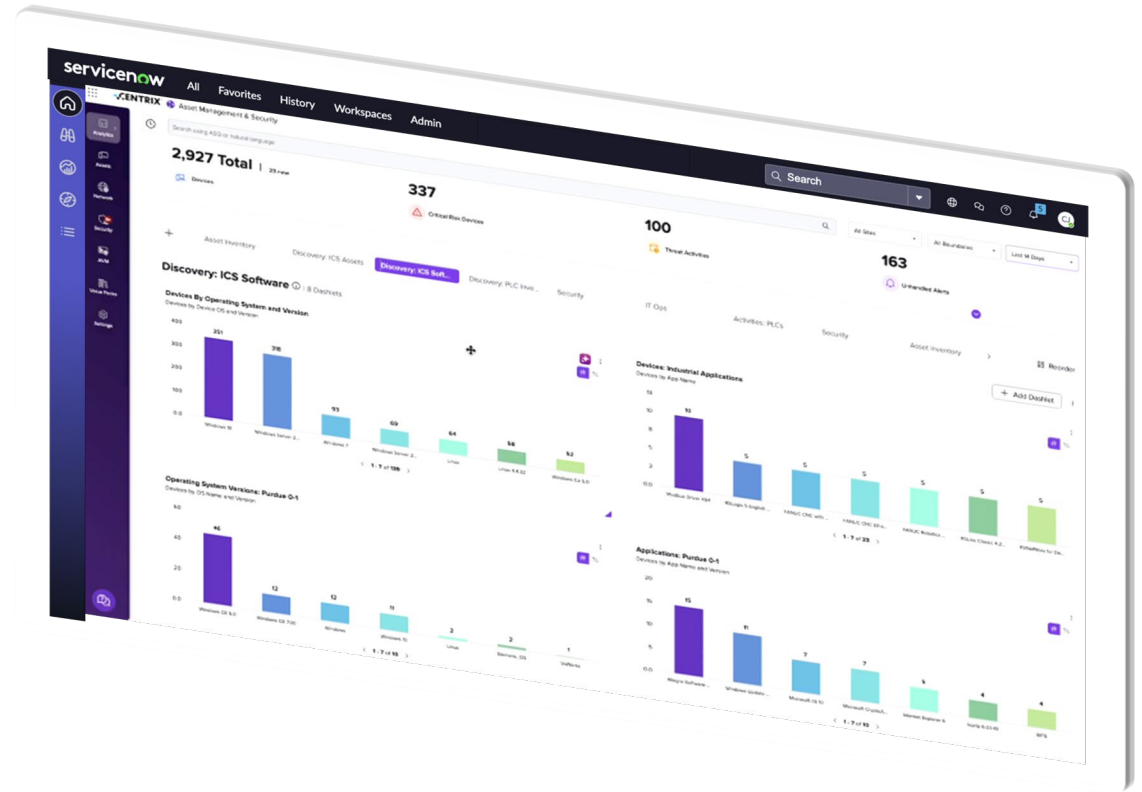
Control cost, risk and compliance.

Apply asset intelligence

Prioritise security and investment actions.

Benefits

- Reduced technology waste and unnecessary renewals
- Faster vulnerability and incident decision-making
- Stronger lifecycle governance and audit readiness



How it works: **Build trusted asset intelligence**

Input

Existing inventories, tools, policies, asset data and governance arrangements.

Action

Assess asset visibility, data quality, ownership, processes and maturity gaps.

Output

A target-state roadmap and prioritised improvement initiatives.

Impact

Trusted asset intelligence that strengthens governance, lifecycle control and investment decisions.



Build a trusted foundation for cyber resilience

Discover how complete asset visibility can strengthen security, governance and technology decisions.

Consider a discussion if your organisation is:

- Assessing fragmented or incomplete asset inventories
- Improving vulnerability and patch prioritisation
- Planning cloud, SaaS or technology transformation

Speak to us to establish trusted visibility across your technology estate.



Matt Loong

Director, Cyber,
KPMG in Singapore

mattloong@kpmg.com.sg

02

Vulnerability and Exposure Management

What it is:

A solution to prioritise and remediate vulnerabilities before attackers exploit them

CISOs



Vulnerability
Administrators &
Analysts



Remediation Related
Stakeholders



Identify exploitable exposures, prioritise remediation
and reduce risk across the attack surface.

Why it matters

Vulnerabilities span IT, OT, cloud, applications and code, while fragmented scanners generate overlapping findings and operational noise. AI-assisted vulnerability discovery is further compressing the time between discovery and exploitation. Organisations need continuous visibility, business context and prioritised remediation rather than relying solely on traditional patch queues.

What it does: Focus remediation on exploitable business risk

Detect exposures continuously

See risk across environments.

Enrich findings with context

so they can understand true exploitability.

Consolidate remediation actions

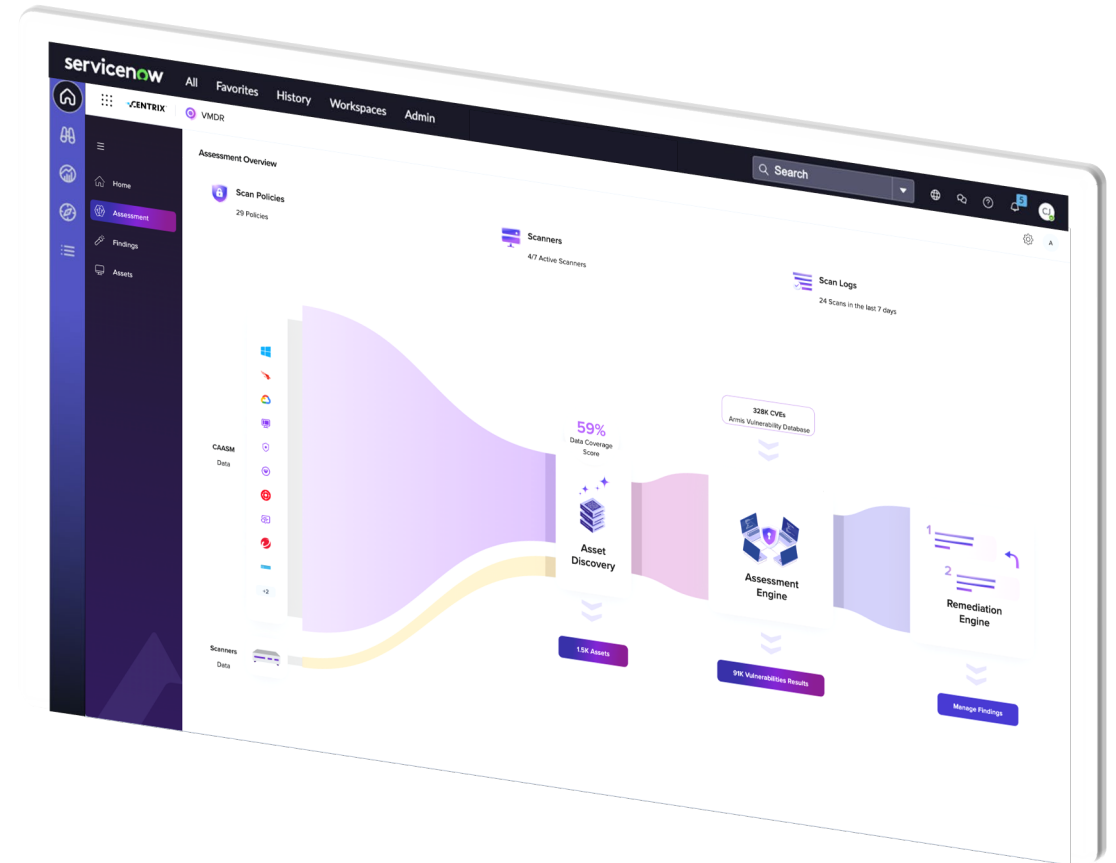
so they can reduce operational noise.

Assign and track fixes

so they can accelerate accountable remediation.

Benefits

- Fewer duplicate and low-value findings
- Faster action on business-critical exposures
- Clearer ownership and remediation tracking



How it works: Turn fragmented findings into focused remediation

Input

Asset data, scanner findings, detected exposures and security alerts.

Action

Normalise, deduplicate, contextualise and group exposures by common fixes.

Output

Prioritised remediation actions with ownership and business context.

Impact

Teams focus remediation on reachable, exploitable and business-critical risks.



Focus remediation on the exposures that matter most

Identify which vulnerabilities present material risk and require priority action.

Consider a discussion if your organisation is:

- Managing growing vulnerability backlogs
- Identifying external and inherited exposures
- Accelerating remediation across IT, OT, cloud and code

Request a consultation to turn exposure data into focused remediation.



Matt Loong

Director, Cyber,
KPMG in Singapore

mattloong@kpmg.com.sg

03

Cyber Risk, Compliance and CCoP Readiness

What it is:

A service to operationalise cyber risk, compliance and regulatory readiness

CISOs



Risk Leaders



Compliance Teams



Why it matters

Cyber risks, controls and evidence often remain fragmented across teams and tools. Manual assessments provide point-in-time views, while recurring regulatory requirements demand sustained execution and audit readiness. CII owners also need to coordinate risk assessments, vulnerability assessments, penetration testing, threat hunting and cybersecurity exercises at defined intervals.

Manage assessments, controls, remediation and evidence through coordinated process and technology support.

What it does: Operate risk and compliance with confidence

Maintain risk and control data

Strengthen confidence in compliance reporting.

Monitor controls continuously

Identify compliance gaps earlier.

Coordinate remediation

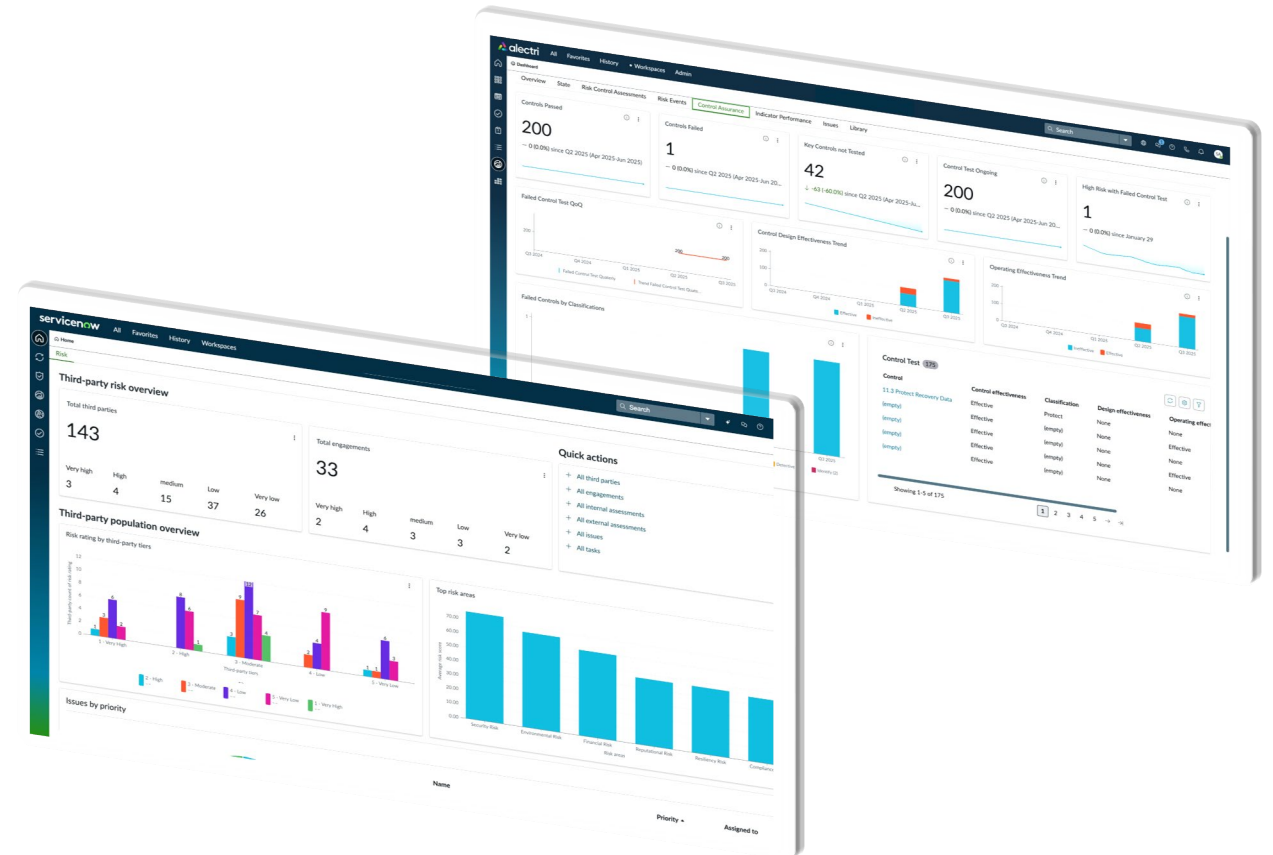
Manage findings and exceptions consistently.

Plan recurring requirements

Maintain regulatory readiness.

Benefits

- Reduced manual evidence collection
- Improved visibility of compliance gaps
- More consistent remediation and reporting



How it works: Connect requirements, evidence and remediation

Input

Applicable requirements, controls, assets, findings and compliance evidence.

Action

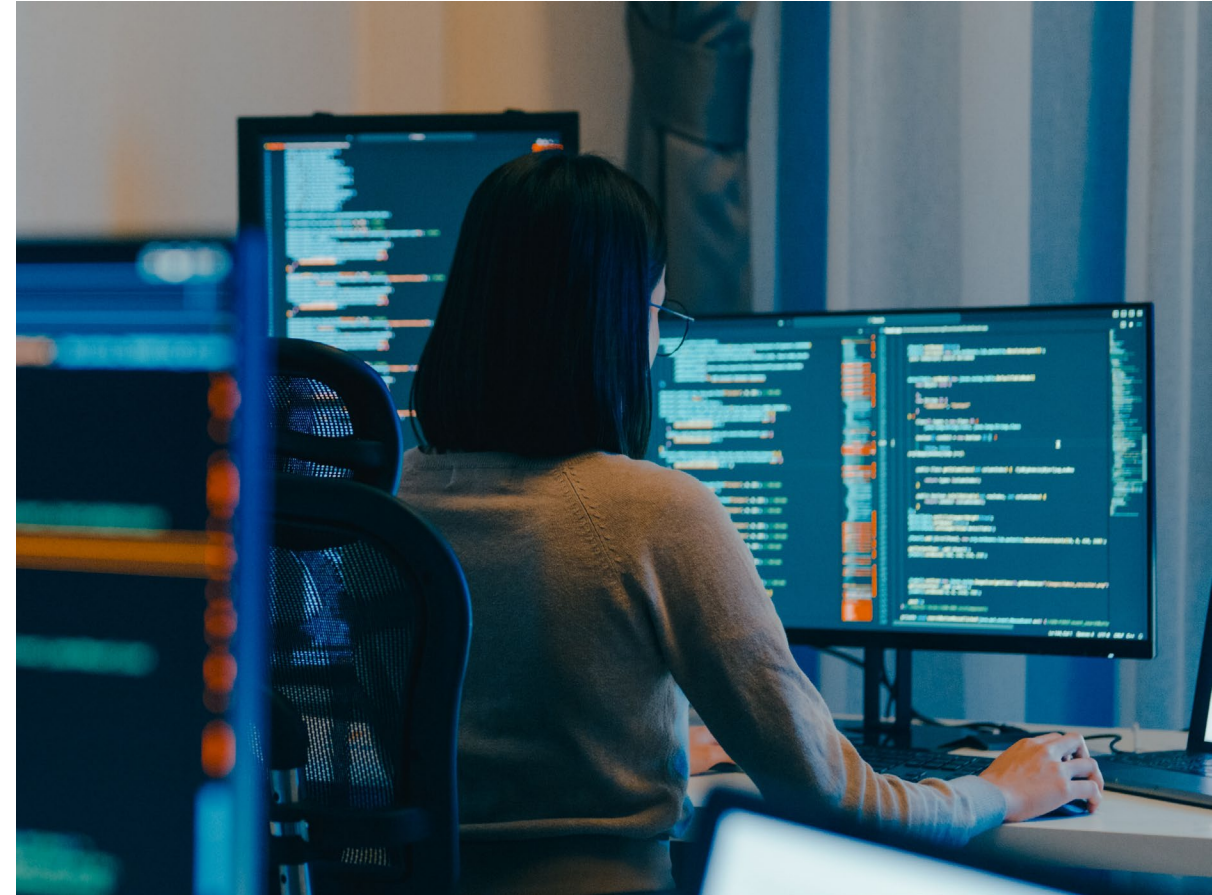
Assess obligations, maintain risk data and coordinate recurring activities.

Output

Compliance status, remediation plans, reports and audit evidence.

Impact

Sustained regulatory readiness with clearer ownership and fewer execution gaps.



Stay ahead of evolving cyber obligations

Discover how coordinated services can simplify recurring compliance and strengthen cyber resilience.

Consider a discussion if your organisation is:

- Preparing for recurring CCoP requirements
- Managing findings, remediation plans and exceptions
- Improving continuous control and evidence monitoring

Request a consultation to make cyber compliance an ongoing operational capability.



Matt Loong

Director, Cyber,
KPMG in Singapore

mattloong@kpmg.com.sg

04

Incident Response and Security Operations

What it is:

A service to prepare for, contain and recover from cyber incidents

CISOs



Security Incident
Managers & Analysts



Extended Cross-
Functional & IT
Partners



Respond to cyber incidents through forensic expertise,
coordinated containment and remediation support.

Why it matters

During an incident, organisations must rapidly understand what happened, preserve evidence, contain the threat and coordinate stakeholders. Fragmented threat information and limited identity or business context slow investigation and prioritisation. Pre-established response arrangements give organisations access to specialist resources and defined activation channels when rapid action is required.

What it does: Accelerate investigation, containment and recovery

Prepare response arrangements

Activate support quickly.

Investigate incidents

Understand scope and root cause.

Contain and eradicate threats

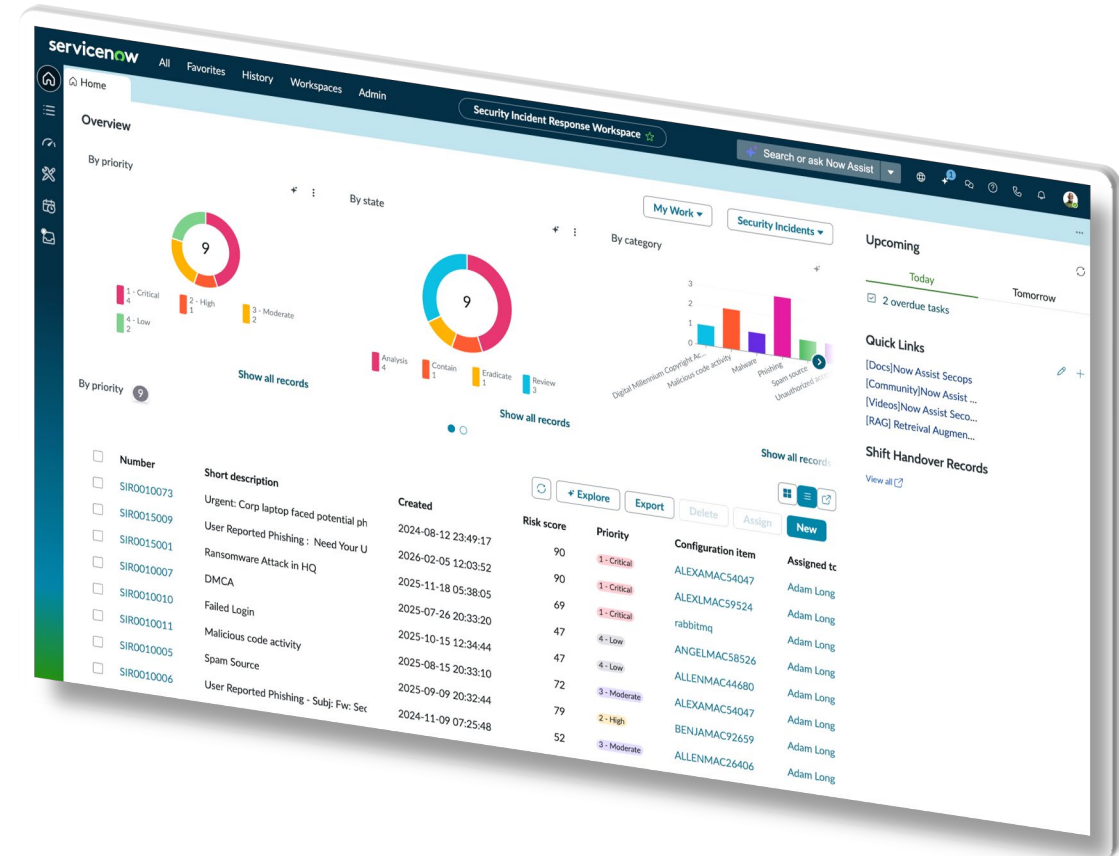
Limit further impact.

Identify improvements

Strengthen future resilience.

Benefits

- Faster access to specialist response support
- More coordinated containment and stakeholder action
- Actionable improvements following an incident



How it works: Coordinate response from activation to recovery

Input

Incident notification, available evidence and affected-system information.

Action

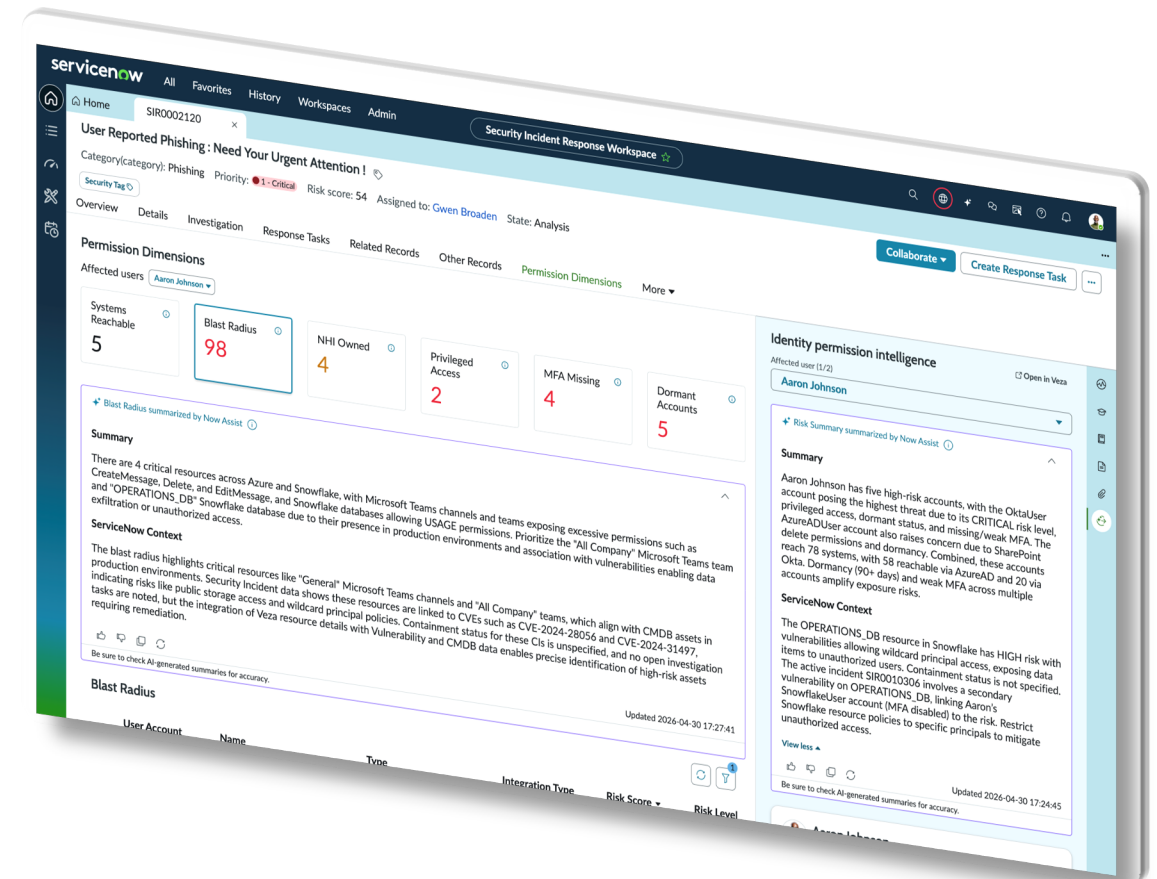
Preserve evidence, investigate, contain, remediate and support communications.

Output

Findings, response actions, reporting and improvement recommendations.

Impact

Faster containment, informed recovery and strengthened future preparedness.



Prepare before critical response decisions become urgent

Discover how established response arrangements can improve containment, investigation and recovery.

Consider a discussion if your organisation is:

- Preparing before a material cyber incident
- Responding to an active compromise
- Strengthening controls after an investigation

Request a consultation to build readiness before the next incident occurs.



Matt Loong

**Director, Cyber,
KPMG in Singapore**

mattloong@kpmg.com.sg

05

AI Governance and Security

What it is:

A solution to govern and secure AI across its lifecycle

CISOs



AI Leaders



Risk & Compliance
Teams



Why it matters

Models, agents, prompts, datasets and AI-enabled services are being deployed across cloud, SaaS and development environments. These systems can access sensitive data, take actions and operate with varying autonomy. Without a unified inventory and lifecycle governance, organisations may struggle to understand ownership, permissions, regulatory exposure, runtime behaviour and business value.

Discover, govern and monitor AI systems, enabling responsible deployment and continuous oversight.

What it does: Govern every AI system with confidence

Discover AI systems

Establish complete ownership and visibility.

Classify AI risk

Apply proportionate governance and oversight.

Control access and behaviour

Contain policy violations.

Monitor performance and value

Sustain trusted AI outcomes.

Benefits

- Unified visibility of approved and shadow AI
- Continuous monitoring of AI risk and behaviour
- Traceable governance across the AI lifecycle



How it works: Connect AI discovery, governance and oversight

Input

AI use cases, models, agents, data sources and operating context.

Action

Discover, classify, govern, secure and monitor AI across its lifecycle.

Output

AI inventory, risk classifications, controls, workflows and performance insights.

Impact

Responsible AI adoption with clearer accountability and continuous oversight.



Bring every AI system under control

Discover how unified AI governance can strengthen visibility, security and accountability.

Consider a discussion if your organisation is:

- Scaling AI use across business functions
- Governing autonomous agents and sensitive data access
- Reviewing readiness for AI-driven cyber risks

Request a consultation to govern AI innovation without losing visibility or control.



Matt Loong

**Director, Cyber,
KPMG in Singapore**

mattloong@kpmg.com.sg

Trusted AI at scale, powered by KPMG and ServiceNow

Value KPMG Brings

- 1 We are consistently recognised as leaders in AI/Gen AI
- 2 We have been on this path having delivered 1000s of successful AI projects
- 3 We apply our understanding of Financial Services into AI capabilities we build
- 4 We recently announced one of the most ambitious alliances with Microsoft globally
- 5 We developed one of the most trusted AI security solutions in market (with Cranium)
- 6 We practice what we preach. We are early adopters and explorers of Gen AI
- 7 KPMG currently holds three AI related patents
- 8 Both Microsoft and Google trust us with implementing their Gen AI solutions

Eight reasons to choose KPMG

Our Technology & AI practice



Architecture

Integrate and incubate complex technology solutions that solve problems, now and in the future.



Cloud

Accelerate cloud modernization with industry-leading offerings that truly transform the way you do business.



Data

Modernize the way you master, manage, move, structure, and store data.



Analytics, AI, & GenAI

Harness the transformative power of advanced analytics, artificial intelligence and Generative AI.



Quality & Assurance

Find gaps early in the development process to mitigate risks and avoid problems with tech transformation.

20,000+

Technology Professionals Across the Globe

2,600+

Data Scientists

5,600+

Data Engineers

8,900+

Developers

600+

Pre-built Solutions

20

Insights Centers to show how data and analytics solutions come to life in ways never imagined

\$300m

AI Investments FY21-23
In our people, our innovative tools, and our technology

\$2B+

Additional investment designated for GenAI over the next five years

7,000+

Engagements Annually



236,000 professionals



700+ offices



145 countries



\$32.13 B in combined global revenues

Why leading organisations trust us



Highest Partner Status

KPMG is one of only six ServiceNow Global Elite Partners across Consulting & Implementation, Build, Service Provider and Reseller categories.



Proven Methodology

An official Built with ServiceNow offering available on the ServiceNow Store that helps accelerate business outcomes.



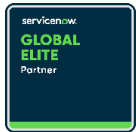
High Customer Satisfaction

KPMG has one of the highest CSAT scores among ServiceNow partners, with an overall score of 4.49, including ITSM 4.69, HRSD 4.89 and App Engine 4.75.



Strategic Implementation Partner

We are a strategic implementation partner for one of the world's largest ServiceNow customers, supporting its end-to-end transformation journey.



Strategic Partnership

KPMG and ServiceNow maintain CEO-level sponsorship, supported by a multi-year services investment plan exceeding US\$1 billion.



Official Build-Partner

KPMG is the official Build Partner for ESG, Operational Resilience, DORA, Finance & Supply Chain and AI in Control solutions.



100+ Deployments per year

KPMG delivers more than 100 ServiceNow deployments annually and maintains over 250 active deal registrations.



KPMG as a Customer

KPMG is the 13th largest ServiceNow customer globally, using the platform across ITSM, SecOps, HRSD, Risk & Compliance and custom application development.

KPMG ServiceNow practice at a glance



Our partnership



Awards



KPMG ServiceNow practice in numbers

1,800+

Global ServiceNow professionals

4.5 / 5

Customer satisfaction score

500+

ServiceNow certified developers in India

45

Countries with ServiceNow capabilities

21

ServiceNow Certified Master Architects

18

ServiceNow Certified Technical Architects

Our certifications

IT Service Management

492 CIS* – IT Service Management

195 ITSM Professional

IT Operations Management

83 CIS* – ITOM Discovery

40 CIS* – Event Management

HR Service Delivery

129 CIS – HR Service Delivery

83 HR Professional Plus Suite Certifications

Now Platform App Engine

9 CIS* – Service Provider

1,479 ServiceNow Certified Application Developer

Governance, Risk and Compliance

122 CIS* – Risk and Compliance

55 CIS* – Third Party Risk Management

*CIS = Certified Implementation Specialist

Recognition



Research
www.hfsresearch.com



Ability to execute

#1

Enterprise Service Management

#1

Verticalized solutions & capabilities

#2

Account Management capabilities



Innovation capability

#1

Consulting & Thought Leadership

#2

Vision for investments



© 2026 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Document Classification: KPMG Public

29



KPMG Services Pte. Ltd.

© 2026 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

General disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Document Classification: KPMG Public