



Securing Digital Transformation



What it is:

A solution to secure cloud, AI and enterprise technology transformation

CIOs



CISOs



Risk Leaders



Secure cloud, AI and Oracle-enabled transformation through integrated governance, controls and continuous assurance.

Why it matters

The enterprise perimeter no longer defines where work, data and systems operate.

Remote users, vendors, cloud services and non-human identities have expanded exposure, while governance and accountability still assume older boundaries. A combined advisory and technology approach helps translate board-level governance into integrated controls across identity, data, cloud, ERP and security operations.

What it does:

Secure transformation across the technology estate

Prioritise risks across identity, data, ERP, cloud and operations

Focus investment where it matters most.

Translate governance and regulatory requirements into enforceable controls

Demonstrate accountability and assurance.

Secure transformation across Oracle and hybrid environments

Adopt cloud and AI with greater confidence.

Sustain control through continuous monitoring and managed services

Respond faster as risks evolve.

Benefits

- Reduced security, fraud and compliance exposure
- Faster transformation with documented assurance
- Clearer visibility and accountability across the estate

How it does it: Demo

Input

Business priorities, regulatory obligations and current risks across identity, data, Fusion ERP, cloud and security operations.

Action

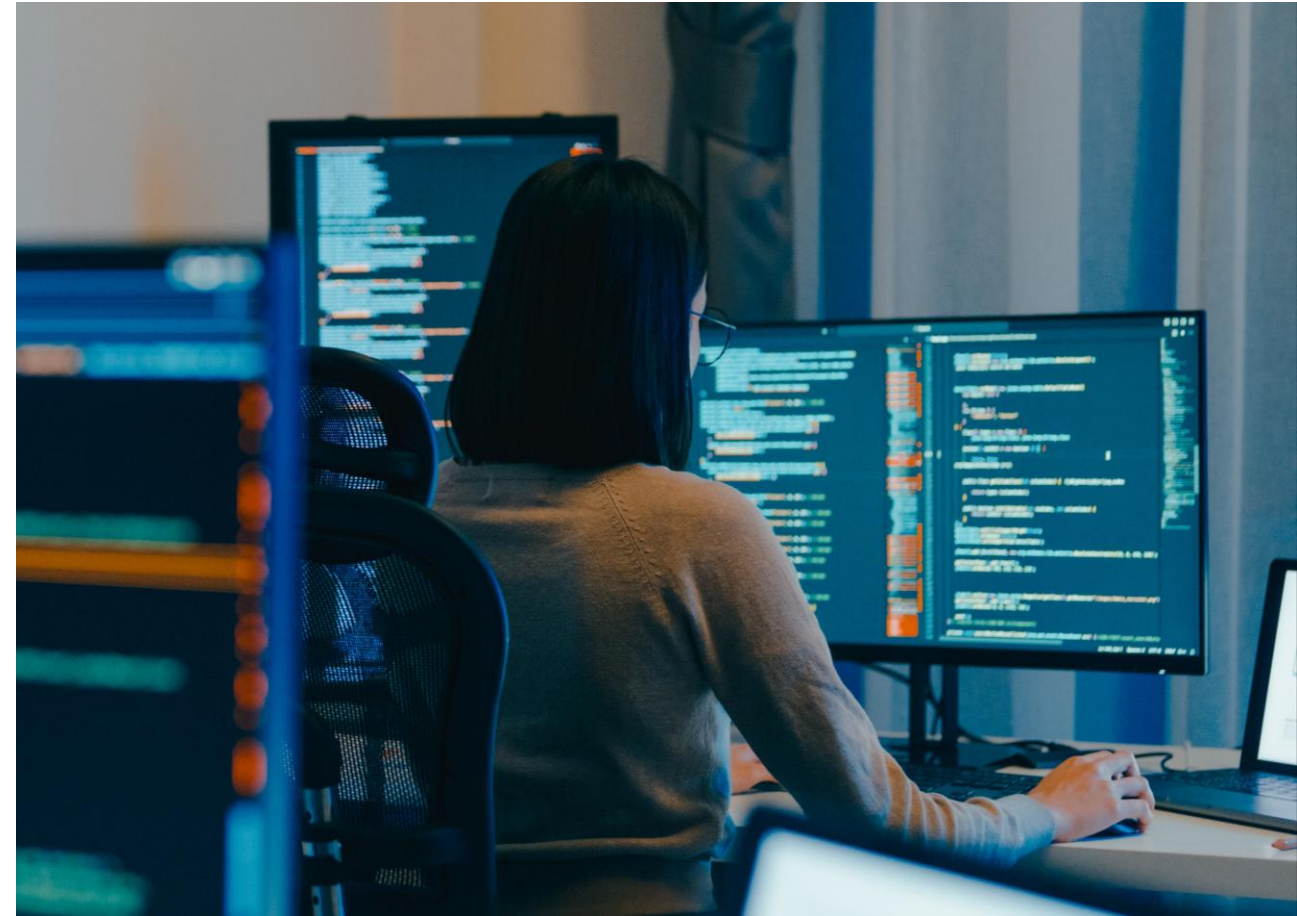
KPMG assesses and prioritises risks, designs governance and transformation roadmaps, and aligns them with Oracle's end-to-end security capabilities across OCI, Database, Fusion and AI.

Output

A phased roadmap showing which solution areas to prioritise first, supported by target controls, implementation priorities and continuous assurance.

Impact

An integrated path from board-level governance to technical controls and ongoing operations



Explore a secure digital transformation roadmap

Discover how KPMG and Oracle can address your most critical risk and transformation priorities across six connected solution areas.

Consider a discussion if your organisation is:

- Strengthening identity governance for human, machine and AI access
- Modernising data, ERP and regulatory control environments
- Scaling cloud adoption and security operations with confidence

Request a consultation to explore your path to resilient transformation.



Shailesh Namjoshi

**Associate Director,
Technology Enablement,
KPMG in Singapore**

shaileshnamjoshi@kpmg.com.sg

6 business conversations — Govern & scale

Each of the six topics is a business risk discussion for the board, not a technology project.

Govern

- **01 Zero Trust Transformation:** who can access what, and how do we know?
- **02 Data Security and Privacy:** where is our sensitive data, who touches it, and are we compliant?
- **03 Fusion ERP Security:** who can approve a payment, and does the CFO know?

Threats detected and contained early
Controls and obligations evidenced on request

Scale

- **04 Cloud Security Posture:** are our cloud environments secure by design or by assumption?
- **05 Sovereign Cloud and Compliance:** where exactly is our data, and who controls it?
- **06 SOC Modernisation:** how fast can we detect and contain a threat across the estate?

Cloud adoption without compliance delays

Cyber Week / SICW Singapore | September 2026 | Confidential

Govern: Zero Trust — identity and access governance

Most identity breaches result from excessive standing privilege rather than sophisticated attack techniques.

Business problem

- **Network trust no longer holds** — employees are remote and vendors are connected
- **Machine identities exceed human ones** in many financial institutions
- **AI agents run autonomously** with high, often unmonitored privileges
- **Continuous verification is required** for every user, API, workload and device

Reduced identity breach risk and audit findings

Oracle technology

- **OCI IAM** — SSO, MFA, risk-based authentication and federation
- **OCI Bastion** — privileged access without VPN exposure
- **OCI Vault** — centralised control of keys and secrets
- **Cloud Guard and Security Zones** — policy guardrails against misconfiguration

Faster onboarding and offboarding at lower cost

KPMG services

- **Zero Trust strategy and roadmap** — board-aligned, phased delivery
- **IGA and PAM** — governance over privileged identity
- **Access certification** — periodic review of excess privilege
- **Cyber operating model** — governance, RACI and board reporting

Stronger control over AI and non-human identities

Sources: KPMG Cyber Advisory Services; Oracle security documentation

Govern: Data security — regulatory obligations and AI

Data carries direct regulatory obligations, and AI adoption has widened the scope of data governance.

Regulatory and AI pressure

- **MAS TRM, PDPA, APRA and GDPR** apply simultaneously to ASEAN organisations
- **Different obligations** on breach notification timelines and penalties
- **AI governance** — which models access sensitive data, and does it cross borders?
- **Discovery and classification** are the prerequisite to any data security programme

Compliance across Singapore jurisdictions

Oracle technology

- **Oracle Data Safe** — discovery, classification and activity auditing
- **OCI Vault and key management** — control over encryption keys
- **Database encryption** across the estate
- **Data masking and subsetting** for non-production use

Reduced breach and penalty exposure

KPMG services

- **Data governance framework** — ownership and accountability
- **Privacy assessments** across business processes
- **Regulatory reviews** against MAS, PDPA, APRA and GDPR
- **AI data governance** for controlled adoption
- **Infrastructure-level controls** — data residency and security enforced by OCI by design

Trusted AI adoption with clear data ownership

Sources: KPMG Cyber Advisory Services; KPMG–Oracle joint cyber use cases

Govern: Fusion ERP security — A CFO problem

Where one person can create a vendor, approve an invoice and authorise the payment in Oracle Fusion, segregation of duties has already failed.

Business risk

- **Fusion holds critical financial data** — payroll, procurement and vendor payments
- **Segregation of duties conflicts** create direct financial crime exposure
- **Excessive privileges** inherited from ERP migrations compound the risk
- **Board question:** does Internal Audit have continuous visibility into who can do what?

Reduced fraud exposure through enforced SoD

Oracle technology

- **Fusion security roles** and role-based access controls
- **Risk Management Cloud** — SoD conflict detection
- **OCI IAM** — federated identity and privileged access
- **Data Safe** — database security controls

Audit-ready, continuously documented controls

KPMG services

- **ERP security reviews** and SoD assessments
- **SoD redesign** aligned to the control environment
- **Controls optimisation** and continuous controls monitoring
- **Internal Audit alignment** and assurance

Reduced regulatory exposure and penalty risk

Target stakeholders: CFO, CIO, CISO, Internal Audit | Confidential

Scale : Cloud security posture — prevention by design

Most cloud breaches result from misconfiguration rather than sophisticated attacks.

Business problem

- **Over-privileged IAM roles** and public storage buckets are the largest exposure categories
- **Unencrypted data at rest** and weak network ACLs accumulate faster than teams remediate
- **Deployment velocity** consistently outpaces security review cycles
- **On-premises controls** do not automatically carry over to cloud

Fewer misconfigurations reaching production

Oracle technology

- **Cloud Guard** — continuous detection and remediation
- **Security Zones** — preventative guardrails by design
- **Vulnerability scanning** across the cloud estate
- **Logging and monitoring** for audit-ready evidence

Faster cloud adoption with documented assurance

KPMG services

- **Cloud security assessment** — baseline the current exposure
- **Secure landing zone** — build the target securely from day one
- **Continuous compliance monitoring** against regulatory obligations
- **Governance framework** — ownership and accountability

Continuous compliance posture, lower breach risk

Sources: KPMG Cyber Advisory Services; KPMG–Oracle joint cyber use cases

Scale : Sovereign cloud — data residency and control

Regulators now require evidence of where data resides, who controls it and how that control is demonstrated.

Business problem

- **Proof is now required** of data residency and operational control
- **Regulators and agencies** across Singapore and the region demand auditable cloud environments
- **Traditional public cloud** cannot always answer these questions
- **Regulated industries** are left exposed to compliance failure

Auditable data residency and sovereign control

Oracle differentiator

- **Dedicated Region Cloud@Customer** — full estate in your own data centre
- **OCI Sovereign Cloud** — regional control over data and operations
- **Oracle Alloy** — operator-controlled deployment
- **Government Cloud** — control over infrastructure and encryption keys

Regulatory confidence in supervised sectors

KPMG services

- **Regulatory readiness assessment** against supervisory expectations
- **Sovereignty strategy** aligned to business footprint
- **Cloud risk assessment** across the migration path
- **Compliance by design** for banking, government, healthcare and CNI

Faster cloud adoption in regulated sectors

Singapore opportunity sectors: banking, government, healthcare, critical national infrastructure

Scale : SOC modernisation — from alerts to response

Disconnected alerts across Oracle Fusion, OCI, firewalls, identity and endpoints slow detection and raise operational cost.

Stage 01 — Reactive

- **Where many organisations are today.**
- **Incident response after the fact** with manual triage and limited visibility
- **Siloed logs** across Fusion, OCI, firewall, identity and endpoints
- **Alert fatigue** slows every investigation

Faster detection and lower analyst workload

Stage 02 — Proactive

- **The KPMG and Oracle target state.**
- **Continuous monitoring** with SIEM integration across Splunk, Sentinel and QRadar
- **Managed detection and response** across the hybrid estate
- **Threat hunting** as a standing capability

Single view across hybrid cloud and on-premises

Stage 03 — Predictive

- **The longer-term target.**
- **AI-driven detection** with automated response
- **Compressed MTTD and MTTR** against agreed board thresholds
- **Continuous intelligence** from Fusion, OCI Audit and Cloud Guard

Clear accountability during an incident

Cyber Week / SICW Singapore | September 2026 | Confidential

KPMG and Oracle — a combined proposition by phase

KPMG's regulatory depth and Oracle's integrated platform, delivered phase by phase — an outcome neither provides independently.

	Phase 1 — Assess · Weeks 1 to 4	Phase 2 — Design and transform · Months 2 to 6	Phase 3 — Operate and optimise · Ongoing
What KPMG brings Regulatory depth and assurance	<ul style="list-style-type: none">• Current-state assessment across identity, cloud, SOC, ERP and data• Regulatory gap analysis against MAS, PDPA, APRA and GDPR	<ul style="list-style-type: none">• Zero Trust architecture with IGA and PAM, plus the SOC target operating model• Data governance framework and privacy compliance programme	<ul style="list-style-type: none">• Managed detection and response as a continuous service• Continuous compliance monitoring and threat hunting
What Oracle brings Integrated, sovereign platform	<ul style="list-style-type: none">• Platform and estate discovery across Fusion, Database, OCI and AI services• Sovereign deployment options mapped — DRCC, OCI Sovereign Cloud and Alloy	<ul style="list-style-type: none">• Secure landing zone with Security Zones, IAM and CSPM tooling• Security built into the infrastructure — not bolted on	<ul style="list-style-type: none">• Cloud Guard for continuous preventative control• AI and data services hardened as the estate evolves
Together One accountable outcome	<ul style="list-style-type: none">• Risk-prioritised findings and an executive readout the board can act on	<ul style="list-style-type: none">• Measurable risk reduction — regulatory depth matched to platform capability	<ul style="list-style-type: none">• Governance through to continuous operations under one accountable partnership

Cyber Week / SICW Singapore | October 2026 | Confidential



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