IERP®
Institute of Enterprise Risk Practitioners

GLOBAL CONFERENCE 2026

FROM CHAOS TO COMMAND: RISK LEADERSHIP IN INDUSTRY 6.0

LOVE, TRUST & DATA : TURNING THIRD-PARTY PARTNERSHIPS INTO ADVANTAGE

Jacky AW
Head of Tech Risk & BCM / CISO,
Kenanga Investment Bank

SESSION OPENING

Every external data partnership is a vote of trust — long before it becomes a line in a contract.

Third-party data is now core infrastructure for growth — and the fastest-growing concentration of regulatory, reputational and operational risk.

THE ASSET

Shared data unlocks better decisions, faster products, and richer customer experiences across the ecosystem.

THE EXPOSURE

The same data, once shared, carries compliance, privacy and resilience risk that lives beyond your own walls.

IERP®
Institute of Enterprise Risk Practitioners

SESSION ROADMAP

What We'll Cover in this session

01 **The Paradox**

Third-party data as strategic asset and concentrated risk

02 **Malaysia's Regulatory Backdrop**

PDPA 2024 amendments, BNM MCIPD and the Outsourcing PD

03 **Why Frameworks Alone Aren't Enough**

The gap between policy and operating reality

04 **Embedding Governance into the Lifecycle**

From onboarding to exit — a life-cycle model

05 **Four Pillars in Practice**

Due diligence, contracting, monitoring, resilience

06 **Turning Governance into Advantage**

Trust, CX and resilience as commercial value

Malaysia's Data & Outsourcing Regulatory Backdrop

2010

PDPA Enacted

Personal Data Protection Act — 7 Data Protection Principles for commercial data processing

2019

BNM Outsourcing PD

Governance & risk management standards for outsourcing arrangements

2024–25

PDPA Amendment Act

Phased in Jan/Apr/Jun 2025 — DPO mandate, breach notification, higher penalties

Oct 2025

BNM MCIPD

Management of Customer Information & Permitted Disclosures — consent conditions for disclosure

Dec 2025

BCBS TPSP Principles

International benchmark for third-party risk life-cycle management

Sources: PDPA 2010 & Amendment Act 2024; BNM Policy Documents on Outsourcing and MCIPD; BCBS (Dec 2025).

PDPA 2024 Amendment: What Changed for Data Sharing

Data Controller, Not Data User

Terminology aligned to international norms; data processors — including vendors — now face direct statutory obligations.

Mandatory DPO

Both data controllers and data processors must appoint a Data Protection Officer accountable for compliance.

Mandatory Breach Notification

Controllers must notify the Commissioner and affected individuals of a personal data breach without undue delay.

Higher Penalties

Fines increased to up to RM1,000,000 and/or up to 3 years' imprisonment for breach of the data protection principles.

Data Portability

Individuals may request their data be transferred to another service provider in a usable format.

Cross-Border Transfer Reform

The old 'whitelist' regime is removed — replaced by a comparable/adequate-protection test for overseas transfers.

SECTOR-SPECIFIC EXPECTATIONS

BNM's Lens: Customer Information & Outsourcing

MCIPD (Oct 2025)

Management of Customer Information & Permitted Disclosures

- Board & senior management oversight of the customer-information lifecycle
- Controls over collection, use, storage and disclosure of customer data
- Conditions for consent: specific, voluntary, explicit & deliberate, revocable
- Requirements extend to outsourced service providers handling customer information

Outsourcing PD & RMiT

Outsourcing risk governance & technology risk management

- Board-approved outsourcing risk appetite and annual outsourcing plan submitted to BNM
- Due diligence, contractual safeguards, data confidentiality and BCP obligations
- Prior written BNM approval for new or materially modified material outsourcing
- RMiT-aligned technology and cyber controls extended over service providers

THE TRUST GAP

Why Frameworks Alone Aren't Enough

Patterns seen across the industry — a well-written policy is not the same as a well-run partnership.

- Checklist-based assessments confirm a document exists — not the real level of risk
- Due diligence treated as a one-time gate at onboarding, not a continuous discipline
- Strong contract clauses that are never operationalised into day-to-day monitoring
- No single, group-wide register — visibility on data-sharing stops at business-unit level
- Business continuity plans that quietly assume disruption is “the vendor's problem”
- Exit and substitution options are only worked out after something has already gone wrong

THE SHIFT REQUIRED **Connect Business, Procurement, Legal, Compliance, Data Governance, Privacy, Cybersecurity, Technology Risk and BCM through one common partnership lifecycle.**

Embedding Governance into the Partnership Lifecycle

1 — Classify & Assess
Data sensitivity, criticality, concentration

2 — Due Diligence
Security, privacy, resilience, financial soundness

3 — Contract
Data clauses, audit rights, breach notice, exit terms

4 — Onboard
Access controls, register & dependency mapping

5 — Monitor
KRIs/KPIs, incidents, continuous due diligence

6 — Exit / Renew
Data return & destruction, transition, lessons learned

The life cycle is iterative: monitoring outcomes and incidents feed back into re-assessment, re-contracting and renewed due diligence.

SHARED ACCOUNTABILITY

Business Owner | Data Owner | DPO / Privacy | Compliance | CISO / Technology Risk | Legal / Procurement | BCM

One lifecycle. Common evidence. Clear decision rights.

Pillar 1 — Due Diligence & Data Classification

1

PILLAR

- Classify data sensitivity: personal, sensitive personal, customer information
- Map data volume, cross-border flow and criticality of the underlying service
- Assess security, privacy controls and the vendor's own sub-processor chain
- Evaluate financial soundness, resilience posture and regulatory standing

Tiered, risk-based scrutiny

Not every vendor needs the same depth of review — but every vendor needs some. Calibrate effort to data sensitivity and service criticality.

Pillar 2 — Contracting for Trust

2

PILLAR

- Purpose limitation and need-to-know access to shared data
- Security, confidentiality and data-segregation obligations
- Breach-notification timelines and minimum information to be provided
- Audit and regulator access rights, extending to sub-contractors
- Cross-border transfer terms and, where required, data localisation
- Data return, deletion and certified destruction on exit

A contract is a starting point

Clauses only create trust when they are monitored and enforced — build the operational link before you need it.

KEEP WATCHING AFTER THE INK DRIES

Pillar 3 — Continuous Monitoring: KRIs & KPIs

3

PILLAR

- % of critical data vendors overdue for reassessment
- Number of unresolved high-risk findings, by age and severity
- Data-incident count and severity, tracked to root cause
- Concentration exposure to a single data vendor or platform
- % of vendors with tested BCP/DR aligned to RTO/RPO

Metrics, not just checklists

Move from “does the document exist” to “what is the vendor actually delivering” — feed monitoring outcomes back into re-assessment.

Pillar 4 — Resilience & Exit Readiness

4

PILLAR

- Build vendor data dependencies into BIA and recovery strategies
- Align vendor recovery commitments to your RTO, RPO and MTD
- Test, don't assume — joint walkthroughs and tabletop exercises
- Maintain a documented exit plan before it is needed

Exit-readiness is a KRI

Review data-return, transition assistance and alternative-provider options at every renewal — not only in a crisis.

FROM COST CENTRE TO COMPETITIVE EDGE

The Trust Dividend: Turning Governance into Business Value

1

Customer Experience

Seamless, privacy-respecting data journeys build lasting loyalty and reduce friction at every touchpoint.

2

Resilience

Fewer surprises, faster recovery and a lower cost of disruption when a partner's service is interrupted.

3

Speed to Market

Pre-vetted, well-governed partners let new data-driven products launch faster, with fewer late surprises.

4

Regulatory Confidence

A defensible, audit-ready evidence trail strengthens the licence to operate with regulators and boards.

MEASURE THE TRUST DIVIDEND

Partner onboarding time | Repeated evidence requests | Customer complaints | Partner incidents | Recovery time | Tested exit readiness

A PRACTICAL TOOL

Illustrative Data–Partner Risk Scorecard

Dimension	Indicative Weight	Illustrative Rating Scale
Data sensitivity & volume	High	Low → Moderate → High → Critical
Security & privacy controls	High	Immature → Developing → Leading practice
Regulatory & contractual compliance	High	Non-compliant → Partially aligned → Fully aligned
Resilience (BCP / DR)	Medium	Untested → Self-tested → Jointly assured
Concentration / substitutability	Medium	Sole-source → Limited options → Substitutable
Financial soundness	Low–Medium	Weak → Adequate → Strong

Illustrative only — weights and thresholds should be calibrated to each organisation's risk appetite and regulatory obligations.

MINI-CASE

BEFORE

Partner selected before data flows, consent, sub-processors and exit arrangements are fully mapped. Gaps emerge late and delay launch.

AFTER

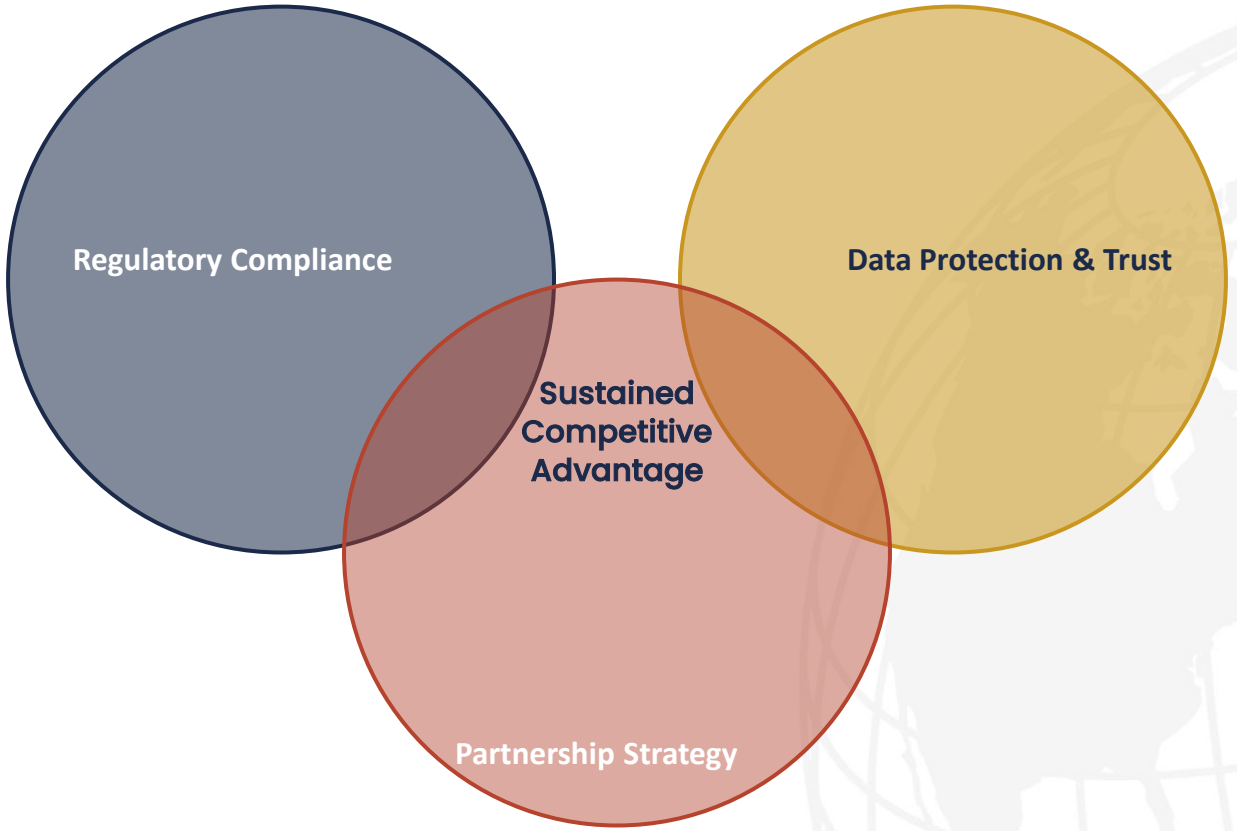
Purpose, data classification and partner risk tier are confirmed early. Standard clauses, controls, monitoring and exit evidence are agreed before signing.

OUTCOME

Faster onboarding, fewer late-stage issues and stronger customer and regulatory protection.

GOVERNANCE AS ENABLER, NOT BRAKE

Aligning Governance with Partnership Strategy



Where compliance, protection and strategy overlap, organisations unlock customer experience, resilience and speed — together.

BEFORE YOU GO

Key Takeaways

1. **Treat governance as a lifecycle, not a gate**

   Classification, due diligence, contracting, monitoring and exit are one continuous discipline.

2. **The regulatory bar has risen in Malaysia**

   PDPA 2024 and BNM's MCIPD 2025 mean compliance must be built in by design, not bolted on.

3. **Contracts are only as strong as the monitoring behind them**

   KRIs and KPIs turn clauses into evidence — and evidence into confidence.

4. **Resilience and exit readiness are trust signals**

   Tested recovery and a documented exit plan protect customers as much as they protect the balance sheet.

5. **Well-governed data partnerships are a competitive advantage**

   Not just a compliance cost — a source of customer experience, resilience and speed to market.

IERP®
Institute of Enterprise Risk Practitioners

GLOBAL CONFERENCE 2026

FROM CHAOS TO COMMAND:
RISK LEADERSHIP IN INDUSTRY 6.0

THANK YOU

SCAN THE QR CODE
TO KNOW MORE ABOUT US!

enquiry@insterp.com
www.insterp.com