Falconry360™

WHITEPAPER

GOVERNANCE / CYBER / PRIVACY

# Cyber risk and data privacy, converged.

Why leading organisations are governing security and privacy as one discipline — and how a connected operating model builds durable digital trust.

For CISOs, DPOs, risk leaders and boards · Global perspective, GCC lens

falconry360.com

# Contents

EXECUTIVE SUMMARY

# One discipline, one operating model

Cyber risk and data privacy grew up as separate functions — one owned by security engineering, the other by legal. Regulators, customers and boards no longer see that separation. A breach is simultaneously a security failure, a privacy violation, a disclosure event and a trust event.

This paper argues that the organisations best positioned for the next decade run cyber and privacy on a single governance, risk and compliance operating model: one risk register, one control library mapped to every applicable framework, one evidence base, and one executive view.

We examine the global and GCC regulatory landscape, the shift from heat maps to decision-grade risk quantification, and privacy's emergence as a competitive differentiator — then set out a maturity model and a 90-day plan for getting started.

FINDING 1

**Fragmented cyber and privacy programmes duplicate controls, evidence and reporting — and still leave gaps at the seams.**

FINDING 2

**Regulation is converging faster than organisations: security regimes now mandate privacy outcomes, and privacy laws mandate security controls.**

FINDING 3

**Boards act on quantified, business-framed risk. Converged data is the precondition for credible quantification.**

# 01

# The case for convergence

Cyber protects systems; privacy protects people. In practice they share the same data, the same controls and the same failure modes.

- **Convergence**
- Regulation
- Board reporting
- Digital trust
- Operating model

# The cost of running two programmes

When security and privacy operate as parallel functions, the same encryption control is assessed twice, the same vendor is reviewed twice, and the same incident triggers two uncoordinated response tracks — each with its own regulator clock.

1. **Duplicated control work**
   Access, encryption, retention and vendor controls tested separately by each team against overlapping frameworks.

2. **Conflicting risk pictures**
   Two registers, two scoring scales, two versions of "our top risk" — the board sees neither clearly.

3. **Gaps at the seams**
   Shadow data stores, unclassified personal data in security tooling, breach notifications that miss privacy deadlines.

4. **Slower transformation**
   Every new product or AI initiative waits on two separate assessments instead of one integrated review.

# What a converged model shares

### CYBER RISK BRINGS

- Threat and vulnerability intelligence
- Technical control depth — identity, network, endpoint
- Incident detection and response discipline

### PRIVACY BRINGS

- Data-centric view — what is held, why, and for whom
- Legal-basis and purpose discipline for every processing activity
- Rights of individuals as first-class obligations

### THE SHARED FOUNDATION

**One risk register**
Cyber, privacy and third-party risk on one scale, one taxonomy.

**One control library**
Each control mapped once to every applicable framework.

**One evidence base**
Collected once, reused for every audit and regulator.

**One executive view**
Board, executive and regulator reporting from the same data.

# 02

# The regulatory landscape

Security regimes now mandate privacy outcomes, and privacy laws mandate security controls — globally and across the GCC.

- Convergence
- **Regulation**
- Board reporting
- Digital trust
- Operating model

# The global baseline

Wherever your organisation operates, four regulatory families now shape both disciplines at once. Each one assumes the other exists.

### Comprehensive privacy law

GDPR MODEL

The EU General Data Protection Regulation (GDPR) set the template most jurisdictions now follow: legal basis, individual rights, 72-hour breach notification — and an explicit duty to secure personal data with "appropriate technical and organisational measures".

### Sector resilience regimes

NIS2 · DORA

Europe's NIS2 directive and the Digital Operational Resilience Act (DORA) hold management bodies personally accountable for cyber risk, extend obligations deep into the supply chain, and impose incident-reporting clocks measured in hours.

### Disclosure & governance rules

SEC MODEL

The US SEC requires listed companies to disclose material cyber incidents within four business days and describe board oversight of cyber risk — turning security posture into an investor-facing governance question.

### Certifiable standards

ISO 27001 · 27701

ISO/IEC 27001 (information security) and its privacy extension ISO/IEC 27701 are literally one management system — the standards bodies converged the disciplines before most organisations did.

# The GCC regulatory map

| JURISDICTION | KEY INSTRUMENTS | REGULATOR | BREACH NOTIFICATION |
|---|---|---|---|
| **Saudi Arabia** | Personal Data Protection Law (PDPL) · NCA Essential Cybersecurity Controls (ECC) · SAMA Cyber Security Framework | SDAIA · NCA · SAMA | 72 hours to SDAIA where harm is likely |
| **UAE — federal** | PDPL (Federal Decree-Law 45 of 2021) · UAE Information Assurance Regulation | UAE Data Office · CSC | Notify on breach likely to cause harm |
| **DIFC & ADGM** | DIFC Data Protection Law No. 5 of 2020 · ADGM Data Protection Regulations 2021 | DIFC & ADGM Commissioners | As soon as practicable; GDPR-style regimes |
| **Wider GCC** | Qatar PDPPL · Bahrain PDPL · Oman PDPL · Kuwait DPPR | NCSA · PDPA · MTCIT · CITRA | Varies; all trending toward GDPR-style duties |

Summary for orientation only — obligations depend on sector, licence and data flows. Take legal advice on applicability.

# A decade of accelerating obligation

**2017–18**

SAMA Cyber Security Framework · GDPR in force · Saudi NCA established

**2019–20**

NCA ECC controls adopted · DIFC DP Law No. 5 · ISO/IEC 27701 published

**2021**

Saudi PDPL enacted · UAE federal PDPL · ADGM DP Regulations

**2023**

Saudi PDPL amended · SEC cyber disclosure rules · Oman PDPL in force

**2024**

PDPL enforcement begins · NIS2 applies · EU AI Act adopted

**2025**

DORA applies to EU financial entities · AI-governance rules phase in

**2026 →**

Enforcement matures across the GCC · cross-border transfer rules tighten

**The direction is one-way: more regimes, shorter clocks, personal accountability. A framework-by-framework response cannot keep pace.**

# 03

# Cyber risk at board level

Boards do not act on heat maps. They act on quantified exposure, framed in the language of business decisions.

# From heat maps to decision-grade risk

### WHERE HEAT MAPS FALL SHORT

- "High" means different things to the CISO, the DPO and the CFO — ordinal scores cannot be compared or aggregated.
- A 5×5 grid cannot answer the board's real questions: how much should we spend, and on which risk first?
- Privacy exposure — regulatory fines, remediation, trust erosion — rarely appears on the cyber heat map at all.

### WHAT QUANTIFICATION ADDS

- Scenario-based estimation — for example Factor Analysis of Information Risk (FAIR) — expresses exposure as a range of loss, not a colour.
- Loss scenarios include privacy outcomes: notification costs, regulatory penalties, contractual claims, customer churn.
- Controls are prioritised by risk reduced per riyal or dollar spent — a language boards already speak.

**Quantification is only as credible as its inputs — and converged risk, control and incident data is what makes the inputs defensible.**

# Reporting the board can act on

**01** **Lead with exposure, not activity**

Top risks framed as business scenarios with estimated loss ranges and trend — not counts of patched systems or completed training.

**02** **Anchor to appetite**

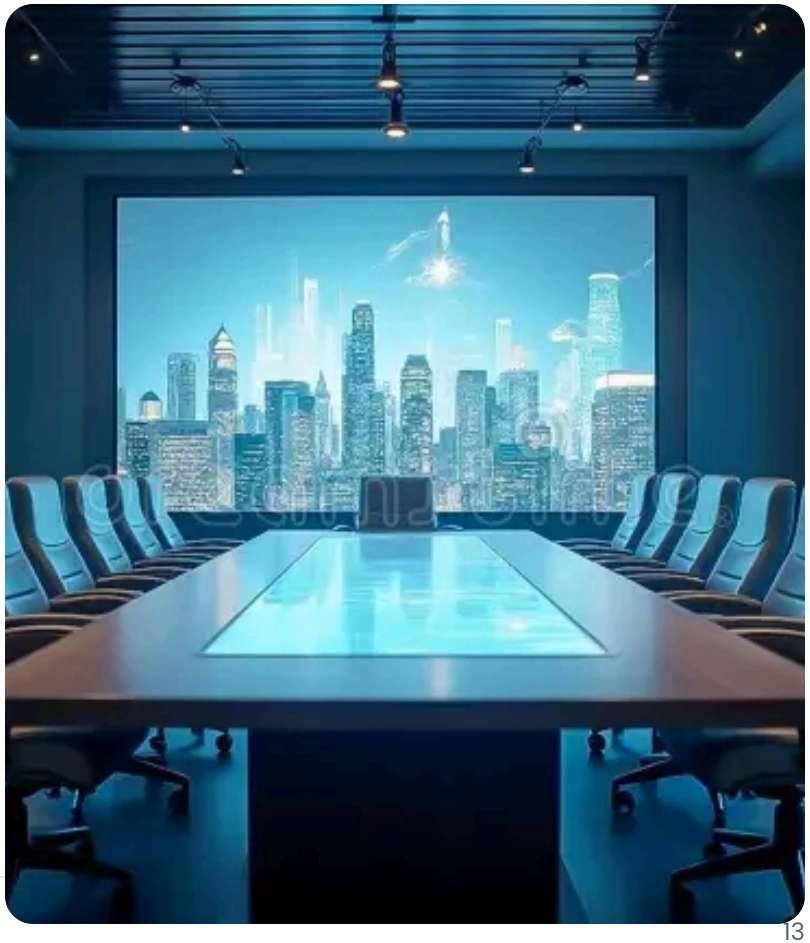
Every risk shown against a board-approved appetite statement, so "accept, treat or transfer" is a governed decision with an owner.

**03** **Report cyber and privacy together**

One view spanning security posture, privacy compliance, third-party risk and regulatory commitments — with drill-down to evidence.

**04** **Show the regulator clocks**

Open findings, notification deadlines and remediation commitments by regulator — visible before they become escalations.



# The question boards ask has changed — from "are we secure?" to "which risks are we carrying, what would they cost, and who is accountable for each one?"

The premise of converged cyber-privacy governance

# 04

# Privacy as digital trust

Handled as a legal chore, privacy is a cost. Handled as a promise kept at scale, it becomes a reason customers choose you.

- Convergence
- Regulation
- Board reporting
- **Digital trust**
- Operating model

# Trust compounds where compliance merely avoids

A compliance-only privacy programme aims at the floor: avoid fines, answer complaints, survive audits. A trust programme aims higher — it treats every data interaction as a moment where a promise is kept or broken.

### Sales enablement

Enterprise and government buyers now audit privacy posture before contracting. A demonstrable programme shortens procurement, not just audits.

### Data for growth

Clear lawful bases and clean data maps let analytics and AI initiatives proceed with confidence instead of stalling in review.

### Incident resilience

Organisations that notify clearly and quickly are treated differently — by regulators, by media, and by the customers affected.

### National-programme alignment

GCC digital agendas make trusted data handling a condition of participation in government platforms and smart-city ecosystems.

# Six practices of an operational privacy programme

## 01

### Records of processing (RoPA)

A living inventory of what personal data is processed, why, where, and with whom — the map everything else depends on.

## 02

### Impact assessments (DPIA)

Privacy and security review built into project intake — one integrated assessment, not two queues.

## 03

### Rights requests (DSR)

Access, correction and deletion handled inside statutory deadlines, with an auditable trail per request.

## 04

### Consent & notice

Consent captured where required, honoured everywhere, and reflected in downstream systems — not just the website banner.

## 05

### Cross-border transfers

Transfer mechanisms and localisation duties mapped per jurisdiction — critical where GCC regimes diverge on data residency.

## 06

### Breach response

One incident process that triggers security containment and privacy notification together, against every applicable clock.

# 05

# The target operating model

Where to aim, how mature you are today, and what to do in the first ninety days.

# Converged does not mean merged

The Chief Information Security Officer (CISO) and Data Protection Officer (DPO) keep distinct mandates — the DPO's independence is a legal requirement in most regimes. What converges is the machinery underneath them.

### CISO RETAINS

- Security architecture and control operation
- Threat management and incident command
- NCA, SAMA and sector security compliance

### DPO RETAINS

- Independent advice and regulator liaison
- DPIA opinions and lawful-basis decisions
- Rights-request oversight and privacy training

### SHARED MACHINERY

- One risk register, taxonomy and appetite
- One control library and evidence base
- One incident process and one executive report

**A joint risk committee — CISO, DPO, risk, audit and business owners — becomes the single forum where trade-offs are decided and recorded.**

# A four-stage convergence maturity model

Stage 1

## Fragmented

Cyber and privacy run separately. Spreadsheets and email. Duplicate assessments; incidents handled in parallel tracks; the board sees two stories.

Stage 2

## Coordinated

Teams share plans and meet regularly. A joint incident playbook exists. Registers and control libraries are still separate; mapping is manual.

Stage 3

## Integrated

One platform, one register, one control library mapped to every framework. Evidence collected once. Combined executive reporting is routine.

Stage 4

## Optimised

Quantified risk drives investment. Controls are monitored continuously; assessments are triggered by change, not by calendar. Trust is reported as a business metric.

Most organisations self-assess at stage 1–2. The step-change in value — and in audit efficiency — comes at stage 3.

# Scenario: a vendor breach on two operating models

An illustrative composite, not a client engagement. A regional financial group learns that a customer-communications vendor has been compromised; personal data of account holders is exposed.

### FRAGMENTED RESPONSE

| | |
|---|---|
| **Hour 0** | Security opens an incident; privacy hears about it two days later through a status email. |
| **Day 3** | No one can say which data sets the vendor held — the vendor file and the RoPA live in different tools. |
| **Day 5** | The 72-hour notification window has closed before legal review starts. Two regulators receive different accounts. |
| **After** | Findings, fines and a remediation programme — rebuilding the map that should have existed. |

### CONVERGED RESPONSE

| | |
|---|---|
| **Hour 0** | One incident record triggers both tracks: containment tasks for security, notification assessment for privacy. |
| **Hour 4** | The vendor record links to the data sets it processes, the affected population and the applicable regimes. |
| **Hour 48** | Regulators notified inside the window with one consistent account; customers informed with clear guidance. |
| **After** | Lessons feed the shared register and control library; the board sees one report with quantified residual exposure. |

# The first ninety days

DAYS 1–30

## See the whole picture

- [ ] Inventory both programmes: frameworks, registers, assessments, tooling, owners.
- [ ] Map applicable regimes and notification clocks per entity and jurisdiction.
- [ ] Self-assess against the four-stage maturity model; agree the gap honestly.

DAYS 31–60

## Unify the foundations

- [ ] Adopt one risk taxonomy and scoring scale covering cyber, privacy and third-party risk.
- [ ] Merge control libraries; map each control once to all applicable frameworks.
- [ ] Stand up the joint risk committee with a decision log and appetite statement.

DAYS 61–90

## Prove it works

- [ ] Run one integrated incident exercise — a breach with personal data — against real clocks.
- [ ] Quantify two or three priority scenarios end to end, privacy losses included.
- [ ] Deliver the first combined board report and agree the twelve-month roadmap.

REFERENCE

# Glossary

| | |
|---|---|
| **PDPL** | Personal Data Protection Law — the comprehensive privacy statutes of Saudi Arabia and the UAE. |
| **NCA ECC** | Essential Cybersecurity Controls issued by Saudi Arabia's National Cybersecurity Authority. |
| **GDPR** | EU General Data Protection Regulation — the template for most modern privacy law. |
| **RoPA** | Records of Processing Activities — the inventory of personal-data processing. |
| **DSR** | Data Subject Request — an individual exercising access, correction or deletion rights. |
| **TPRM** | Third-Party Risk Management — governance of vendor and supply-chain risk. |
| **SDAIA** | Saudi Data & AI Authority — competent authority for the Saudi PDPL. |
| **SAMA CSF** | Cyber Security Framework of the Saudi Central Bank, binding on regulated financial entities. |
| **NIS2 / DORA** | EU regimes for network security and financial-sector operational resilience. |
| **DPIA** | Data Protection Impact Assessment — structured review of high-risk processing. |
| **FAIR** | Factor Analysis of Information Risk — a model for quantifying risk in financial terms. |
| **ISO 27001 / 27701** | Certifiable standards for information-security and privacy-information management. |

Falconry360™

HOW FALCONRY360 SUPPORTS CONVERGENCE

# One platform to govern, manage, assure and improve

### Govern
One register, taxonomy and appetite across cyber and privacy.

### Anticipate
Risk assessment and third-party risk on shared data.

### Comply
Controls mapped once to PDPL, NCA, SAMA, ISO and more.

### Withstand
One incident process covering containment and notification.

### Assure
Evidence collected once, reported to board and regulator alike.

---

**Talk to us about converged cyber-privacy governance** falconry360.com