
Baker
McKenzie.
Annual Compliance Conference
16 - 18 June 2026

Cyber trends and risk mitigation

Thursday 18 June

Agenda

01 Geopolitics, AI-Enabled Threats & Critical Infrastructure

02 Global Cyber Laws: A Trip Around the World

- Asia Pacific
- European Union
- United Kingdom
- Middle East & North Africa
- Latin America
- North America

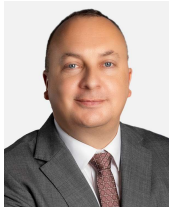
Speakers

Justine Phillips
(Chair) Partner
Los Angeles

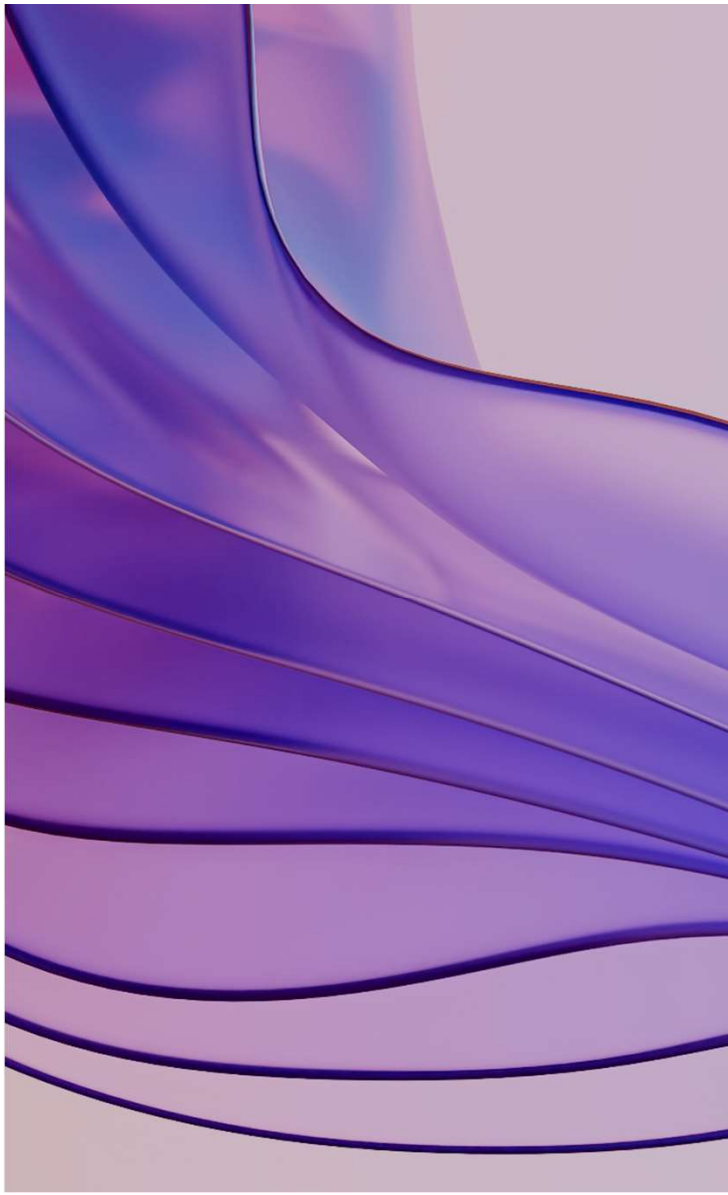
Carolina Pardo
Partner
Bogota

Michael Schmidl
Partner
Munich

Frankie Tam
Partner
Hong Kong



Dino Wilkinson
Partner
Abu Dhabi



01 Geopolitics, AI-Enabled Threats & Critical Infrastructure

Private Ownership of Critical Infrastructure Metrics

North America

85% - 86% of U.S. Critical Infrastructure

80% - 85% of Canada's Critical Infrastructure

Latin America

60% - 80% of Latin America Critical Infrastructure

Varies widely

- Higher Chile
- Lower Venezuela

EMEA

60% - 80% Western Europe

40% - 60 % Eastern Europe

- Middle East
- Africa

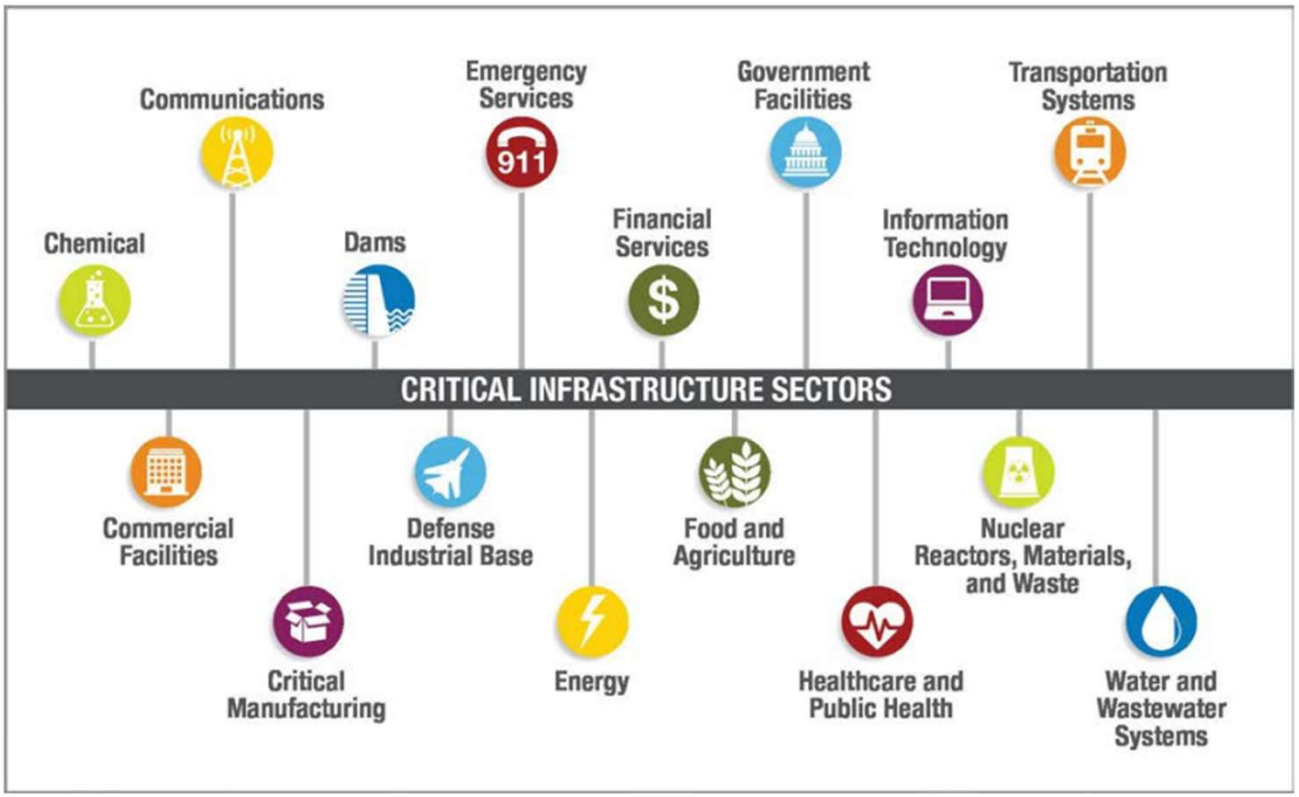
State/Public

Asia Pacific

90% Australia's critical Infrastructure

- Japan – mixed Public/Private
- China – State Owned
- India – mixed Public / Private

“Critical Infrastructure” & “Essential Entities”



National Policy on Critical Infrastructure

Figure 1: The 16 Critical Infrastructure Sectors

Geopolitically Motivated Actors Target Critical Infrastructure

- Cyber Espionage & Disruption
- Supply Chain Attacks
- Cyber warfare and financial gain

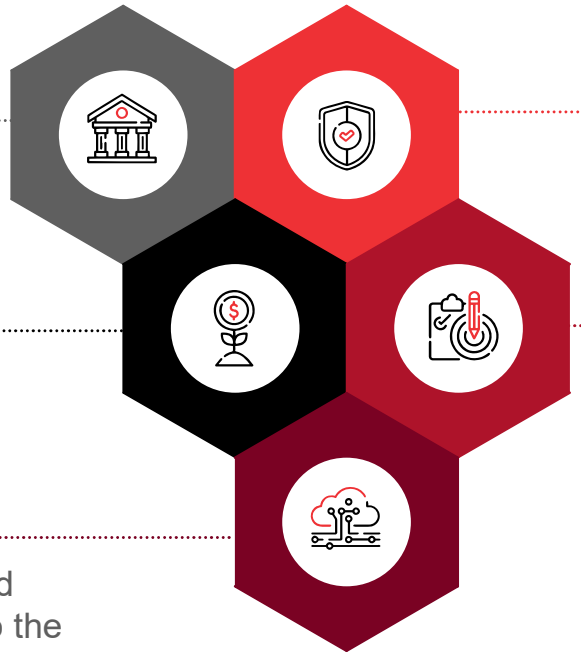
Multidimensional Cyber Laws Framework

Cyber laws encompass multiple regulatory domains, addressing different risk vectors and interests

Sector-specific regulation
tailoring cyber and data security requirements for industries characterised by systemic risk or ultra-sensitive data

Personal/Non personal data
addressessing access, sharing, and monetisation of industrial and machine-generated data

Critical infrastructure
ensuring operational continuity and protecting services that are vital to the functioning of the state and society



Cybercrime
addressing cybercrime, content, and individual liability.

National Security and defence
access controls, digital sovereignty, preventing espionage, cyber-warfare, sanctions, dual-use controls and secrecy laws.

Global Trends & Themes Emerge

Deglobalization

Data Localization & Digital Sovereignty

National Security & Transparency

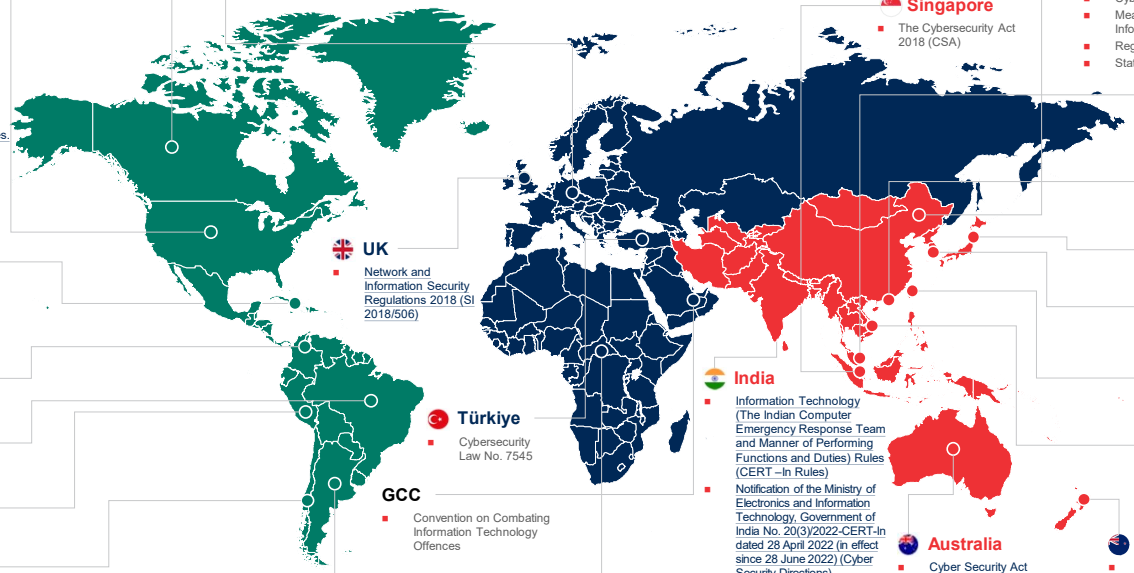
24 Hour Notice for Ransom Payments & 72 Hours for “Cyber Incident”

Technical & Organizational Controls

“Reasonable Security” & Owning Supply Chain Risk

02 Global Cyber Laws: A Trip Around the World

Evolving Cyber Laws Across the Globe



Canada

Federal

- PIPEDA – Personal Information Protection and Electronic Documents Act (Federal)

United States

Federal

- Federal Trade Commission Act – Section 5
- FTC Health Breach Notification Rule (HBNR)
- Gramm-Leach-Bliley Act (GLBA)
- Security Rule under the Health Insurance Portability and Accountability Act (HIPAA)
- FISMA – Federal Information Security Management Act
- Securities and Exchange Commission (SEC) Cybersecurity Rules.
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).
- Defense Federal Acquisition Regulation Supplement (DFARS) – Safeguarding Covered Defense Information and Cyber Incident Reporting
- Cybersecurity and Infrastructure Security Agency Act (CISAA)

LATAM & Caribbean

- Mexico - Federal Law on the Protection of Personal Data held by Private Parties (FDPL)
- Paraguay - Law No. 4.439/2011
- Venezuela - Law of Informatic Crimes published in the Official Gazette N° 37.313 dated 30 October 2001

Colombia

- Criminal System Code

Brazil

- Bill No. 4752 establishing the Cybersecurity Legal Framework

Peru

- Supreme Decree No. 016-2024-JUS

Chile

- Law No. 21.663 (Framework Law on Cybersecurity)

Argentina

- Law No. 26,388 – Cybercrime Law
- Resolution No. 829/2019 – National Cybersecurity Strategy
- Resolution No. 44/2023 – Second National Cybersecurity Strategy

EU

- Regulation (EU) 2019/881 (Cybersecurity Act)
- Regulation (EU) No 910/2014 (eIDAS Regulation)
- Directive (EU) 2022/2555 (NIS 2 Directive)
- Commission Implementing Regulation of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 (Commission NIS 2 Implementing Regulation")
- Regulation (EU) 2024/2847 (Cyber Resilience Act - CRA)
- Regulation (EU) 2022/2554 (Digital Operational Resilience Act – DORA)
- Directive (EU) 2022/2557 (Critical Entities Resilience Directive)
- Directive (EU) 2015/2366 (PSD2 Directive)

UK

- Network and Information Security Regulations 2018 (SI 2018/506)

Türkiye

- Cybersecurity Law No. 7545

GCC

- Convention on Combating Information Technology Offences

African Union

- Guideline for Model Cybersecurity Law to African Member state
- South Africa - Cybercrimes Act
- Congo - Law No. 27-2020
- African Union Convention on Cyber Security and Personal Data Protection

Singapore

- The Cybersecurity Act 2018 (CSA)

India

- Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules (CERT –In Rules)
- Notification of the Ministry of Electronics and Information Technology, Government of India No. 20(3)/2022-CERT-In dated 28 April 2022 (in effect since 28 June 2022) (Cyber Security Directions)

Australia

- Cyber Security Act 2024 (Cth) (Cyber Security Act)

China

- Cybersecurity Law (CSL)
- Cryptography Law
- Data Security Law (DSL)
- Regulations on Critical Information Infrastructure Security Protection
- Provisions on Administration of Security Vulnerabilities in Network Products
- Cybersecurity Review Measures
- Measures for Data Security Management in the Field of Industry and Information Technology (Trial Implementation)
- Regulations on the Administration of Network Data Security which
- State Measures for the Administration of Reporting of Cybersecurity Incidents

Malaysia

- Cyber Security Act 2024 (CSA)
- Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024

Hong Kong

- Protection of Critical Infrastructures (Computer Systems) Ordinance (Chapter 653 of Laws of Hong Kong)

Japan

- The Basic Act on Cybersecurity

South Korea

- Act on Promotion of Information and Communications Network Utilization and Information Protection

Taiwan

- Cyber Security Management Act (CSMA)

Vietnam

- Law No. 116/2025/QH15on Cybersecurity (2025 Cybersecurity Law)

New Zealand

- Privacy Act 2020 (IPP 5)

Cybersecurity & Digital Trust Standards Landscape (2026)

International Standards – the common language for multinationals

- ISO/IEC 27001:2022 (ISMS): the gold standard for Information Security Management; increasingly paired with ISO/IEC 27701 to evidence privacy accountability.
- NIST Cybersecurity Framework (CSF) 2.0: expanded to include "Govern"; widely used as a baseline across sectors.
- EU Cybersecurity Certification Framework (Cybersecurity Act / ENISA): EU-wide certification schemes (e.g., Cloud (EUCS), 5G) increasingly expected in public tenders.
- BSI IT-Grundschutz (Germany): highly detailed, prescriptive alternative often used alongside or instead of ISO 27001.

Emerging Guidance (2026 watchlist)

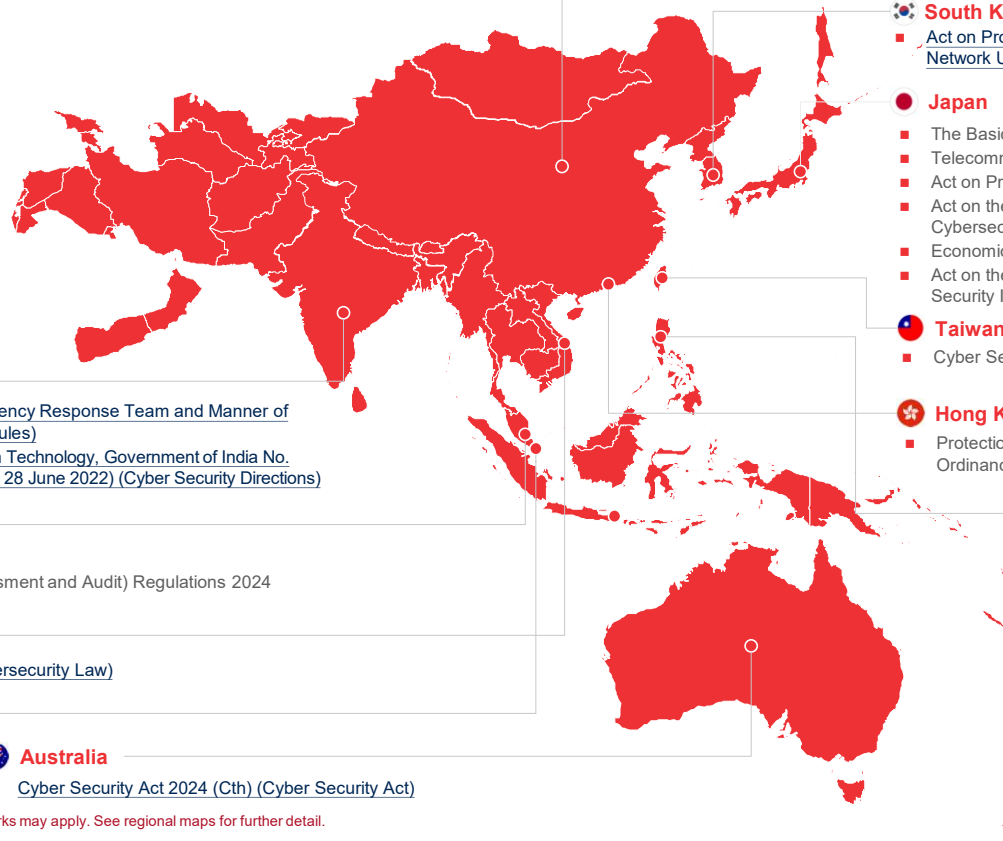
- NIST Post-Quantum Cryptography (PQC) Guidelines: migration guidance toward quantum-resistant algorithms—now a board-level priority.
- OWASP Top 10 for LLM Applications: benchmark guidance for securing LLM apps (e.g., prompt injection and related threats).
- ETSI EN 303 645 (Consumer IoT): EU-aligned baseline "security by design" requirements for consumer IoT manufacturers.

Illustrative only. Not exhaustive. Other legal and regulatory frameworks may apply. See regional maps for further detail.

Asia Pacific

Frankie Tam

APAC



China

- Cybersecurity Law (CSL)
- Cryptography Law
- Data Security Law (DSL)
- Regulations on Critical Information Infrastructure Security Protection
- Provisions on Administration of Security Vulnerabilities in Network Products
- Cybersecurity Review Measures
- Measures for Data Security Management in the Field of Industry and Information Technology (Trial Implementation)
- Regulations on the Administration of Network Data Security which
- State Measures for the Administration of Reporting of Cybersecurity Incidents

India

- Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules (CERT –In Rules)
- Notification of the Ministry of Electronics and Information Technology, Government of India No. 20(3)/2022-CERT-In dated 28 April 2022 (in effect since 28 June 2022) (Cyber Security Directions)

Malaysia

- Cyber Security Act 2024 (CSA)
- Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024

Vietnam

- Law No. 116/2025/QH15on Cybersecurity (2025 Cybersecurity Law)

Singapore

- The Cybersecurity Act 2018 (CSA)

Australia

- Cyber Security Act 2024 (Cth) (Cyber Security Act)

South Korea

- Act on Promotion of Information and Communications Network Utilization and Information Protection

Japan

- The Basic Act on Cybersecurity
- Telecommunications Business Act
- Act on Prohibition of Unauthorized Computer Access
- Act on the Development of Infrastructure for Ensuring Cybersecurity and Implementing Active Cyber Defense
- Economic Security Promotion Act
- Act on the Protection and Utilization of Critical Economic Security Information

Taiwan

- Cyber Security Management Act (CSMA)

Hong Kong

- Protection of Critical Infrastructures (Computer Systems) Ordinance (Chapter 653 of Laws of Hong Kong) (CI Ordinance)

Philippines

- Cybercrime Prevention Act
- Implementing Rules and Regulations of the Cybercrime Prevention Act
- Rule on Cybercrime Warrants

New Zealand

- Privacy Act 2020 (IPP 5)

Illustrative only. Not exhaustive. Other legal and regulatory frameworks may apply. See regional maps for further detail.

Regional Developments
Global Data & Cyber Handbook

Cybersecurity Law Across APAC

China

- Amended Cybersecurity Law took effect on 1 January 2026 – first major amendment since 2017
- Increased penalties; expanded extraterritorial scope; introduction of AI-related provisions

Hong Kong

- Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653) came into effect on 1 January 2026
- Three categories of obligations on critical infrastructure operators: (1) organisational, (2) preventive, (3) incident reporting and response

Singapore

- Cybersecurity (Amendment) Act 2024 passed in May 2024, regulating critical information infrastructure (CII)
- Expansion of CII definition to cover virtualization; expansion of incident reporting obligations

Korea

- PIPA amendment passed in February 2026 and promulgated on 10 March 2026, with most provisions taking effect in September 2026
- Amended Network Act passed the plenary session on 31 March 2026; enforcement from October 2026
- Expanded CISO roles; mandatory annual security reviews

India

- The Digital Personal Data Protection Act, 2023 became operationalized through the notification of the Digital Personal Data Protection Rules, 2025 on 13 November 2025

Malaysia

- Cyber Security Act 2024 came into force in August 2024
- Regulation of national critical information infrastructure

Australia

- Cyber Security Act 2024 (Cth)
- Mandatory reporting of ransom payments; limitations on cyber incident sharing; security standards for smart devices

Japan

- Active Cyber Defense Law passed in May 2025; enforcement from 2027
- Four pillars: (1) strengthened public-private collaboration, (2) use of communication data, (3) access and neutralisation, (4) organisational and structural readiness

Actions to Strengthen Regulatory Readiness

Proactive communication

- Map key regulators and establish a clear incident communication playbook to ensure timely and consistent notifications across jurisdictions
- Conduct regular internal simulations to align legal, technical, and communications teams on coordinated response strategies

Operational adjustments

- Carry out targeted gap assessments against relevant APAC cybersecurity frameworks and implement necessary enhancements to controls, monitoring, and response capabilities
- Regularly test and refine incident response plans to ensure readiness for evolving threat scenarios

Customer contracts

- Review and update customer agreements to reflect current cybersecurity obligations, breach notification timelines, and cooperation requirements
- Clearly allocate responsibility and liability for incidents to minimise disputes and regulatory exposure

Supply chain resilience

- Identify high-risk vendors and implement risk-based due diligence, supported by robust contractual safeguards and audit rights
- Establish ongoing monitoring mechanisms to detect and manage third-party cybersecurity risks over time

Multi-jurisdictional compliance

- Develop a harmonised regional compliance framework that aligns overlapping regulatory requirements across APAC jurisdictions
- Adopt a highest-common-denominator approach to ensure consistent compliance and reduce fragmentation in cross-border operations

European Union

Michael Schmidl

EMEA

EU

- Regulation (EU) 2019/881 (Cybersecurity Act)
- Regulation (EU) No 910/2014 (eIDAS Regulation)
- Directive (EU) 2022/2555 (NIS 2 Directive)
- Commission Implementing Regulation of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 (Commission NIS 2 Implementing Regulation")
- Regulation (EU) 2024/2847 (Cyber Resilience Act - CRA)
- Regulation (EU) 2022/2554 (Digital Operational Resilience Act – DORA)
- Directive (EU) 2022/2557 (Critical Entities Resilience Directive)
- Directive (EU) 2015/2366 (PSD2 Directive)

Italy

Hard Law – National Transposition & Primary Legislation

- Legislative Decree 138/2024 (NIS2): Core Italian cybersecurity law; classification of Essential and Important entities; mandatory risk management and incident reporting (24h/72h) to the Italian CSIRT.
- Legislative Decree 23/2025 (DORA): National implementation of EU digital operational resilience for the financial sector; supervisory powers vested in Bank of Italy, Consob and IVASS.
- Decree-Law 105/2019 (National Cybersecurity Perimeter): Strategic assets protection regime; enhanced ACN oversight and scrutiny of ICT procurement, including non-EU vendors.
- Law 132/2025 (National AI Law): Domestic AI governance framework; anticipates EU AI Act application and establishes the national supervisory authority.
- Legislative Decree 231/2001: Extends corporate administrative liability to cybercrimes; requires updates to organisational and compliance models (231 Models)

Soft Law – Technical Guidelines & Regulatory Practice

- ACN Determination No. 379907/2025: Definition of "significant incidents" and baseline cybersecurity measures for NIS2 entities.
- ACN Incident Reporting Guidelines (February 2026): Operational procedures and templates for notifications to the National CSIRT.
- National Cybersecurity & Data Protection Framework (v2.0): Best-practice maturity model aligned with ISO/NIST, tailored for Italian SMEs.
- Bank of Italy Circulars (2026): Supervisory guidance interpreting DORA for smaller financial intermediaries and payment institutions.
- ACN Cloud Marketplace Guidelines: Qualification rules for cloud services used by Public Administration (data sovereignty, encryption, security).

UK

- Network and Information Security Regulations 2018 (SI 2018/506)
- Product Security and Telecommunications Infrastructure Act 2022
- Communications Act 2003
- Computer Misuse Act 1990, which includes cybersecurity related criminal offences
- Financial Conduct Authority Handbook and Prudential Authority Rulebook

Türkiye

- Cybersecurity Law No. 7545

GCC

- Convention on Combating Information Technology Offences
- Cybersecurity Regulatory Framework for Service Providers in the ICT and Postal Sector (version 1.0)2020
- Regulations of Cybersecurity Operations in Communications, and Information Technology Sectors 2022
- Essential Cybersecurity Controls (ECC – 2: 2024)
- Cloud Cybersecurity Controls (CCC –1:2020)
- Saudi Arabia Cabinet Decision No. 79/1428 on the Approval of the Anti-Cyber Crime Law

African Union

- Guideline for Model Cybersecurity Law to African Member state
- South Africa - Cybercrimes Act
- Congo - Law No. 27-2020
- African Union Convention on Cyber Security and Personal Data Protection

Norway

- Health Registers Act (LOV-2014-06-20-43)
- Police Databases Act (LOV-2010-05-28-16)
- Debt Information Act (LOV-2017-06-16-47)
- Patient Journal Regulation (FOR-2019-03-01-168)
- Police Databases Regulation (FOR-2013-09-20-1097)
- E-health Services Regulation (FOR-2015-07-01-853)
- Personal Data Regulation (FOR-2018-06-15-876)
- CCTV Regulation (FOR-2018-07-02-1107)
- Employers Access Regulation (FOR-2018-07-02-1108)

Regional Developments

Global Data & Cyber Handbook

Illustrative only. Not exhaustive. Other legal and regulatory frameworks may apply. See regional maps for further detail.

Interplay of Key EU Cybersecurity Laws

NIS2 Directive Overview

NIS2 enhances cybersecurity governance by expanding regulated entities and strengthening organizational security obligations.

Digital Operational Resilience Act

DORA focuses on financial institutions' ability to resist and recover from ICT disruptions.

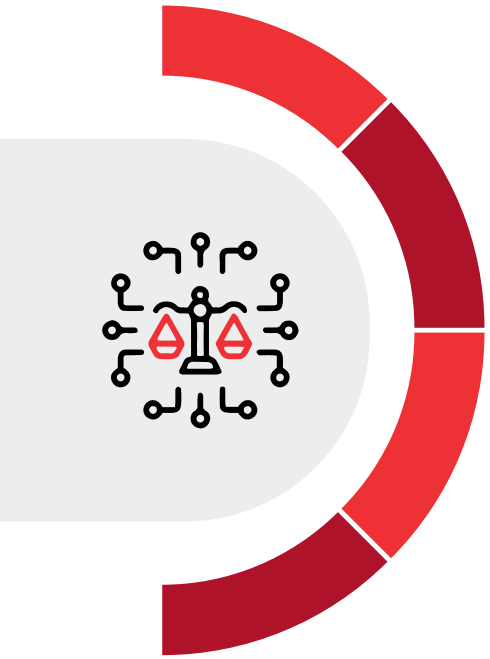
Cyber Resilience Act Focus

CRA mandates security by design for digital products to enhance overall cybersecurity of manufactured goods.

Critical Entities Resilience Directive

CER Directive and national laws ensure physical resilience and continuity of critical infrastructure and services.

Core Compliance Obligations Across NIS2, CRA, and DORA



Governance and Accountability

NIS2 requires strong governance with management accountability and oversight of cybersecurity measures.

Comprehensive Risk Management

Risk management includes supply chain security, assessing and mitigating third-party vendor risks.

Incident Reporting Timelines

Strict incident reporting with 24-hour early warning, 72-hour notification, and final report within one month.

Product Security and Resilience

CRA mandates secure-by-design products, ongoing vulnerability management, and conformity assessments.

Proactive vs Reactive Compliance Obligations

Proactive Compliance Measures

Proactive obligations focus on preventing incidents via risk assessments, security measures, and supply chain due diligence.

Reactive Compliance Measures

Reactive obligations involve incident reporting, regulatory engagement, remediation, and managing penalties after incidents.

Regulatory Expectations

Regulators emphasize both preparedness before incidents and rapid, transparent responses afterward as critical compliance aspects.

Practical Steps for Businesses to Achieve Compliance

Define Compliance Scope: Identify entities, products, and units under regulations like NIS2, CRA, and DORA to clarify compliance boundaries.

Conduct Gap Assessment: Benchmark current cybersecurity practices against ISO 27001, NIST, or BSI to find governance and technical gaps.

Strengthen Governance and Training: Assign management responsibility and implement training to improve cybersecurity awareness organization-wide.

Enhance Supply Chain Security: Update vendor contracts with cybersecurity clauses and monitor third-party risks continuously.

Develop Incident Response: Create playbooks and run simulations to prepare for managing cyber incidents effectively.

Integrate Security in Product Development: Embed security during design and implement vulnerability management under the Cyber Resilience Act.

United Kingdom

Dino Wilkinson

United Kingdom

Cyber Security and Resilience Bill

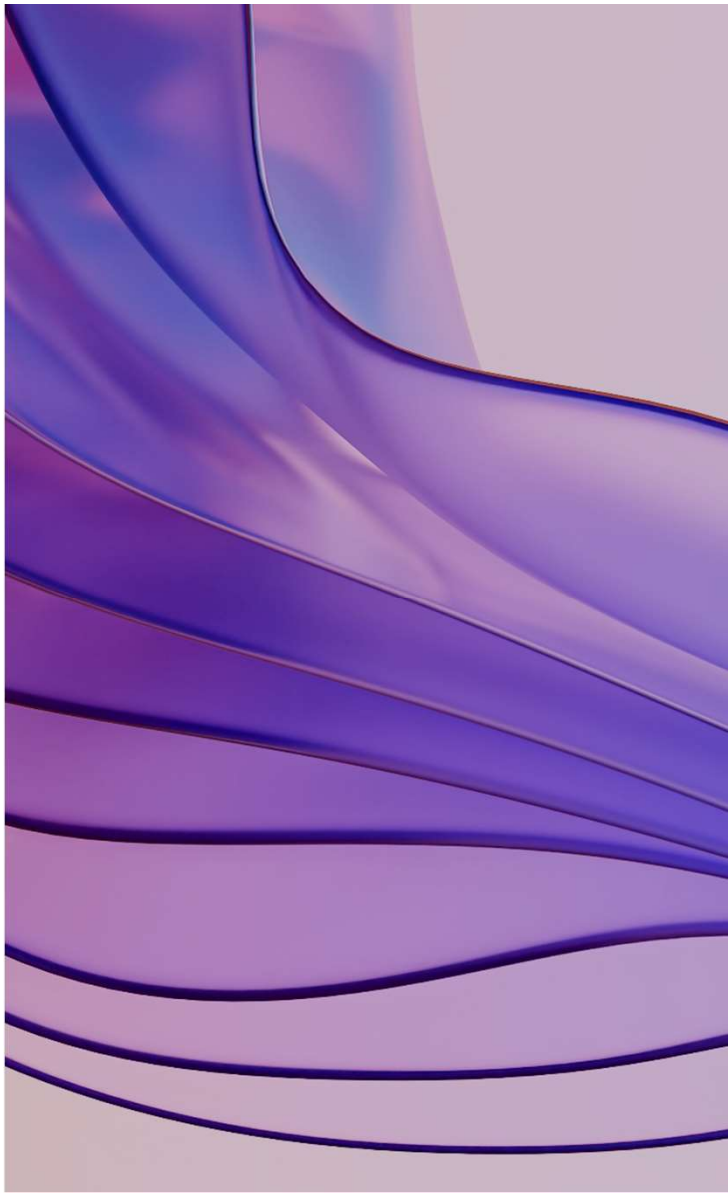
- Additional entities in scope
- More incidents in scope
- Burdensome incident reporting

Proposals for Ransomware Prohibition

- Targeted ban on ransomware payments
- Ransomware payment prevention regime
- Mandatory incident reporting

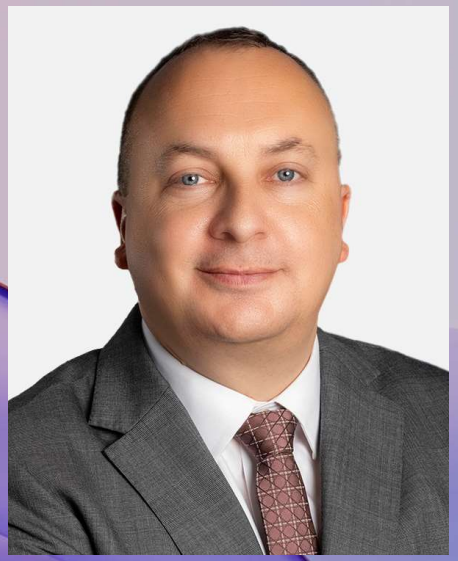
The ICO's Proceeds of Crime Orders

- Misuse and theft of data by employees
- Recent confiscation orders by the ICO against former employees



Middle East & North Africa

Dino Wilkinson



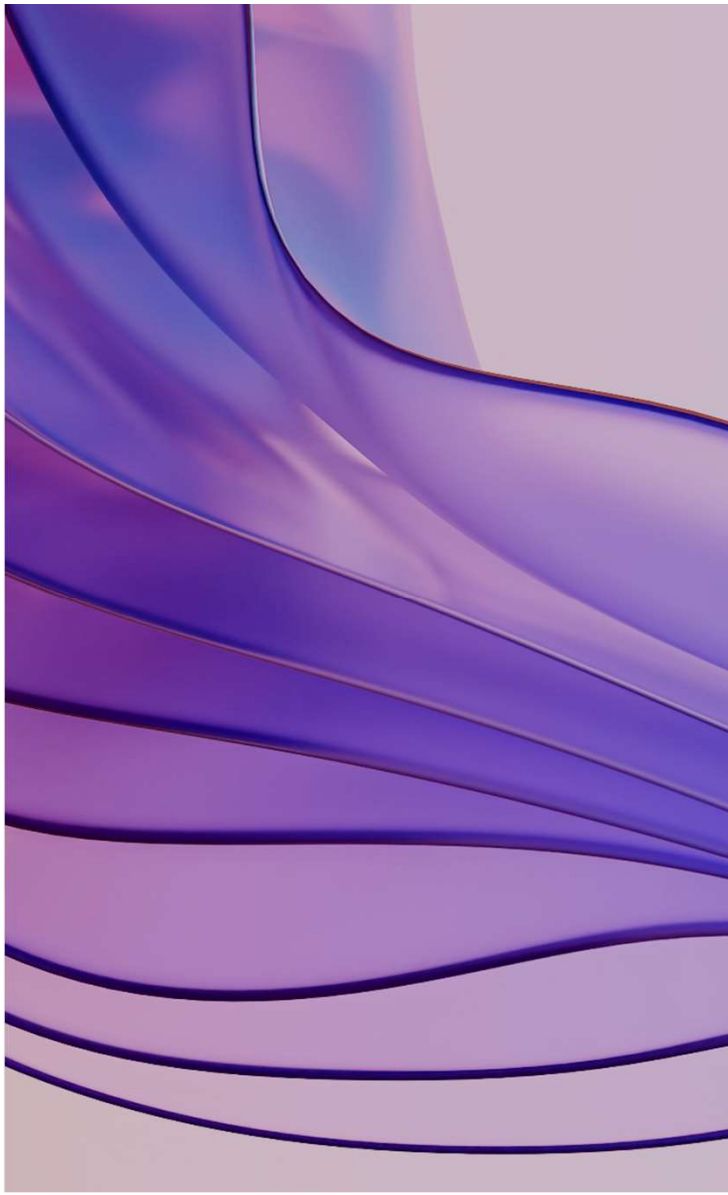
Middle East & North Africa

Regional measures

- Arab Convention on Combating Information Technology Offences

National developments

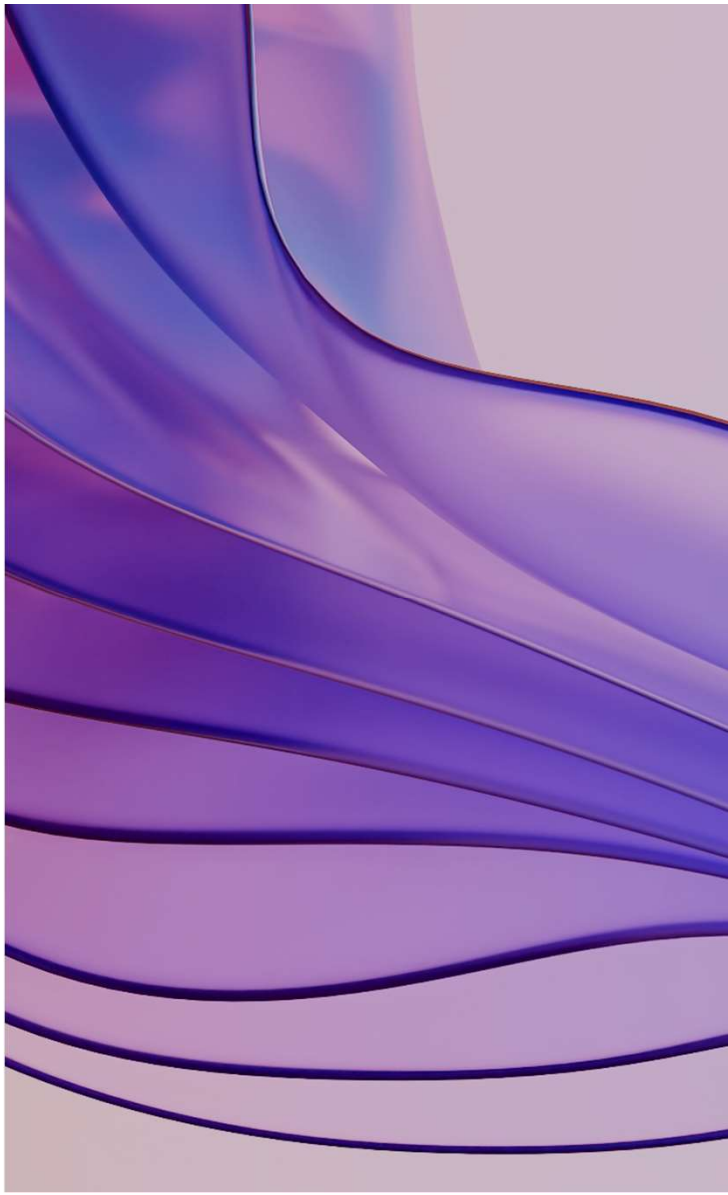
- Cybercrime laws adopted in most states
- Cybersecurity authorities and strategies
- Saudi Arabia NCA enforcement law



Current Issues and Trends

Rising geopolitical tensions leading to changing risk profile for cyber and infrastructure:

- Physical threats to data centres
- Enhanced cyber attack risks
- Data/tech as the new battleground
- Ancillary issues including content controls, hardware supply disruption



Latin America

Carolina Pardo

Americas

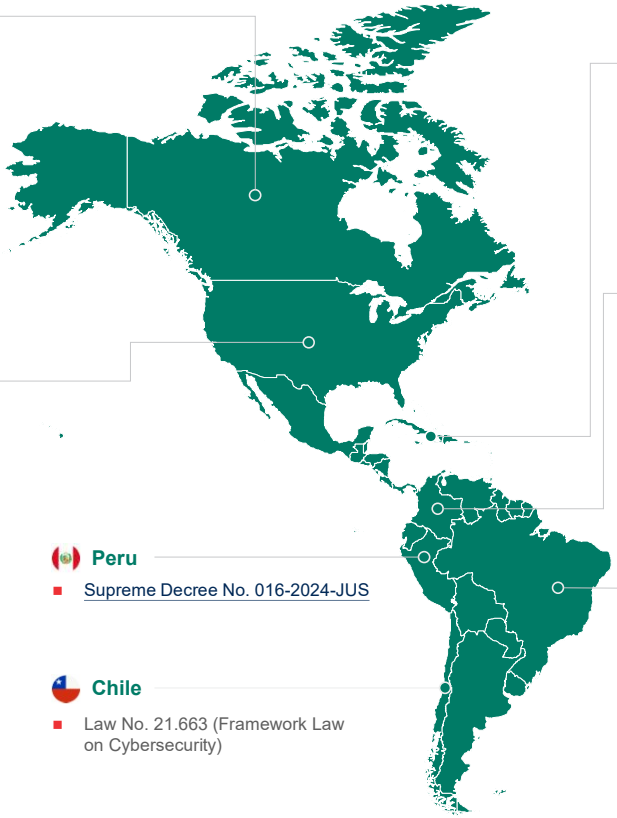
Canada

- Personal Information Protection and Electronic Documents Act, SC 2000, c 5 (PIPEDA) and regulations thereunder, including the Breach of Security Safeguards Regulations, SOR 2018-64 and the Regulations Specifying Publicly Available Information, SOR 2001-7
- **Alberta** - Personal Information Protection Act, SA 2003, c P-6.5 (Alberta PIPA) and the Personal Information Protection Act Regulations, 366/2003
- **British Columbia** - Personal Information Protection Act, SBC 2003, c 63 (BC PIPA) and the Personal Information Protection Act Regulations, B.C. Reg. 473/2003
- **Quebec** - Act respecting the protection of personal information in the private sector, CQLR c P-39.1 (Quebec Act), the Regulation respecting confidentiality incidents, CQLR c A-2.1, r 3.1, and the Regulation respecting the anonymization of personal information, CQLR c A-2.1, r 0.1

United States

Federal

- Securities and Exchange Commission (SEC) Cybersecurity Rules
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
- Executive Order 14117
- Defense Federal Acquisition Regulation Supplement (DFARS) - Safeguarding Covered Defense Information and Cyber Incident Reporting
- Cybersecurity and Infrastructure Security Agency Act (CISAA)
- New York State Department of Financial Services Cybersecurity Requirements (NYDFS) CR and New York SHIELD Act
- Payment Card Industry Data Security Standard (PCI DSS)
- Section 5 of the Federal Trade Commission Act (FTC Act)
- FTC Health Breach Notification Rule (HBNR)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- State data security and breach notification laws



Peru

- Supreme Decree No. 016-2024-JUS

Chile

- Law No. 21.663 (Framework Law on Cybersecurity)

LATAM & Caribbean

- Mexico - Federal Law on the Protection of Personal Data held by Private Parties (FDPL)
- Paraguay - Law No. 4.439/2011
- Venezuela - Law of Informatic Crimes published in the Official Gazette N° 37.313 dated 30 October 2001

Colombia

- Decree 338 of 2022 applicable to all public agencies as well as private companies and individuals who carry out administrative activities or administer critical cybernetic infrastructures or provide essential services.
- Guidelines of the Superintendence of Industry and Commerce (SIC) regarding security incidents and data breaches

Brazil

- Bill No. 4752 establishing the Cybersecurity Legal Framework

Regional Developments
Global Data & Cyber Handbook

Illustrative only. Not exhaustive. Other legal and regulatory frameworks may apply. See regional maps for further detail.

Regional Landscape

LATAM recorded the sharpest global rise in cyberattacks in 2025: 3,065 attacks/week per organization (+26% year over year), 450+ ransomware breaches (+78%), and ransomware variants nearly doubling (48 to 79). Ransomware remains the top concern, closely followed by cyber-enabled fraud (77% of organizations affected). Most impacted countries: Colombia, Ecuador, Chile, and Mexico, with Brazil accounting for approximately 30% of ransomware victims in the region.

85% of LATAM organizations report increased AI-related cybersecurity risks, yet 51% have no processes to assess the security of AI tools before deployment (vs. 29% globally). On the defense side, 74% have adopted AI-enabled cybersecurity tools. Attackers are leveraging AI for phishing, deepfake impersonation, and automated exploitation at growing scale.

65% of LATAM organizations report a lack of critical cybersecurity skills and personnel (vs. 50% globally). Most countries remain at or below the second maturity stage per the OAS (Organization of American States) cybersecurity assessment, with significant gaps in critical infrastructure protection and cyber insurance adoption.

Regulatory Developments

Brazil

Strengthened enforcement capacity by transforming the ANPD into an autonomous regulatory agency (Law No. 15,352/2026). Additional cybersecurity measures continue to be developed, including sector-specific requirements and a proposed national cybersecurity legal framework. Bill No. 4,752/2025 (Cybersecurity Legal Framework Bill) is pending in the Senate and would create a National Cybersecurity Authority (ANC). | Sector-Specific Cybersecurity Notification:

- Financial sector (BCB/CMN). Cybersecurity regulations require formal incident detection, response, and traceability mechanisms, with supervisory oversight and reporting expectations embedded in prudential regulation (CMN Res. 5,274/2025; BCB Res. 538/2025).
- Telecommunications (ANATEL). Mandatory notification of relevant cybersecurity incidents affecting networks or user data. Incidents triggering LGPD notification must also be reported to ANATEL (Res. 740/2020, as amended by Res. 767/2024).
- Energy (ANEEL). Critical infrastructure operators must report cybersecurity incidents to the regulator and share relevant information within the sector to ensure service continuity (Res. 964/2021).
- Healthcare. No unified sector-specific cybersecurity notification regime; obligations primarily derive from the LGPD and general regulatory duties.
- Cross-sector baseline. Under LGPD/ANPD rules, data breaches involving relevant risk or damages to data subjects must be notified within 3 business days, creating overlapping obligations with sector regulators.

Chile

Enacted the first comprehensive cybersecurity law in the region (Law 21,663), creating the Agencia Nacional de Ciberseguridad (ANCI), operational since January 2025. The law introduces minimum security standards, incident reporting obligations, and a sanctions regime for critical information infrastructure (in force since March 2025). Chile also approved a major reform of its data protection framework (December 2024), which will enter into force in December 2026 and create a new Data Protection Agency.

Key aspects of the regulation

- Creation of the ANCI: A technical institution with powers to issue regulations, oversee compliance, and coordinate incident response at the national level.
- Entities subject to the law: It applies both to public administration bodies and to private entities classified as Essential Services (e.g., energy, healthcare, finance, telecommunications) and Operators of Vital Importance (OIV), An Operator of Vital Importance is an organization—public or private—that sustains essential services for the continuity of the country. Its operations depend on infrastructures and technological systems that the new Chilean legislation identifies as critical assets for national security. If you are part of the board of directors or lead GRC, your regulatory and reputational exposure changes significantly once you fall within this category.
- Incident reporting: Critical organizations have a legal obligation to report significant cyberattacks or security breaches promptly (within timeframes that may be as short as a few hours) to the National CSIRT.
- Corporate responsibility: Cybersecurity is no longer solely an IT function; boards of directors and senior management are directly responsible for risk management.
- Severe penalties: Non-compliance with preventive regulations or failure to report incidents is subject to fines ranging from minor (up to c. USD 3,2 million at current rates.

Argentina

Approved a National Cybersecurity Strategy, ratified Convention 108+, reinforcing alignment with international data protection standards. A comprehensive reform of its data protection law is currently under discussion.

Colombia Cybersecurity Strategy

Colombia. Launched its National Digital Security Strategy 2025-2027, setting out a comprehensive roadmap focused on governance, cyber resilience, critical infrastructure protection, and talent development. Colombia has also enabled adoption of ISO/IEC 42001:2023, the first certifiable international standard for AI governance.

Why It Matters for Business

1 Strategic Objective

- Colombia is implementing a national shift toward stronger cybersecurity governance and resilience given increased number of attacks.
- Goal: enable secure digital growth while protecting critical services and data.

2 Business Relevance

- Cybersecurity is becoming a core operational priority across sectors.
- Government will continue to increase scrutiny on how companies manage cyber risks, data, and incidents.

3 Policy Direction

- Intention to move from fragmented regulatory efforts → centralized national coordination
- Shift from reactive → risk-based and preventive approach
- Integrate cybersecurity into economic development and digital strategy

Mexican Law - General Rules Governing Information Security

Legal framework

- No single cybersecurity law; framework derived from multiple statutes (privacy, criminal, telecom, financial).
- Cybercrime prosecuted mostly under Federal Criminal Code (e.g., unauthorized access, data manipulation).

IT security obligations

- Set up appropriate technical, administrative and physical measures.
- Legal standard: Measures should be consistent with risk assessment.
- Risk assessment should consider certain minimum aspects (threats to PII, state of the art tech, etc.).
- Security measures to protect third party data should be at least equivalent to those implemented to protect the organization's own data (e.g., crown jewels).
- Protect personal data from theft, loss, alteration, destruction or unauthorized use.
- Obligation to develop a data security managing program – Regulatory benefits, included reduced fines.

Data Breach Notification duties

- Duty to notify data subjects when a data breach has occurred and may significantly affect moral or patrimonial rights of the data subject.
- Notification must be done immediately after the breach is confirmed and corrective actions are taken.
- Content of the notice is regulated (nature, data affected, mitigation measures).

Mexican Law – Special Rules

Sector Specific Regulation

- Banking Sector
  - Financial sector subject to detailed cybersecurity and operational resilience rules.
  - Mandatory authentication controls and encryption requirements.
  - Obligation to implement business continuity plans and contingency management.
  - Obligation to notify clients of security incidents affecting their data.
  - Obligation to report operational contingencies to regulators (CNBV/Banxico).
- Public Procurement
  - Data Localization rules may apply for certain projects.
  - Specific cybersecurity rules applies to the data centers providing services to government.

New laws and bills

- The federal government presented a National Cybersecurity Plan (2025–2030) and a General Cybersecurity Policy for the federal administration.

Recent developments

- **Data Breaches:** Focus on breaches involving personal data (e.g., Telcel).
- **Real-Real-time government access to customer transaction data:** Mexican authorities require continuous, real-time access to customer transactions, creating significant cross-border compliance risks for global platforms (including potential conflicts with GDPR). The aggregation of highly structured, sensitive data also makes these systems a prime target for sophisticated cyberattacks.
- **Mandatory data interconnection increases cyber exposure:** Private companies must connect their databases to government platforms to support missing persons searches, sharing sensitive data through interoperable endpoints. Affected industries include telecom, financial services, healthcare, transportation, digital platforms, and any data-rich entities, including those with large employee databases all facing heightened cybersecurity and legal liability pressures.

North America

Justine Phillips

Canada Cyber Laws

Key Instruments –

What legal instruments create private sector cybersecurity obligations?

- **Federal**
  - Personal Information Protection and Electronic Document Act ("PIPEDA")
  - Breach of Security Safeguards Regulations (SOR/2018-64) under PIPEDA
  - Authoritative guidance issued by Canada's federal privacy regulator
  - Enforcement decisions by Canada's federal privacy regulator

Additional Resources

- **Canadian Cybersecurity Laws**
  - 2026 Guide: Cybersecurity Laws and Regulations in Canada
  - 2026 Guide: Global Data and Cyber Security Handbook - Canada

Core Requirements –

What are core cybersecurity requirements that need to be satisfied?

- **Federal and Provincial Private Sector Cybersecurity Laws**
  - Reporting incidents to applicable federal and/or provincial privacy regulators using prescribed breach reporting forms where an incident creates a "real risk of significant harm" (RROSH) "as soon as feasible"
  - Where an incident creates a RROSH, there may also be an obligation to notify data subjects who could have been impacted by the incident as soon as feasible and there are prescribed requirements for the notification;
  - Personal information must be protected using physical, technical, and administrative safeguards that are appropriate to the sensitivity of the information, and such safeguards must be contractually imposed on service providers and other third parties to whom personal information is sent.

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

Scope:

- Applies to entities that operate in one of 16 “critical infrastructure sectors” and meets “covered entity” criteria (which is met when entity exceeds small business size)
- Regulations being revised
- Town hall meetings this week

Key Requirements:

Report covered cyber incidents within 72 hours of the companies’ reasonable belief that a cyber incident has occurred

Report ransom payments within 24 hours after a payment is made

Executive Order 14117: Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Gov. Related Data by Countries of Concern

National security law that establishes a Data Security Program (DSP) administered by DOJ's National Security Division (NSD)

Prohibits and restricts access to certain data about the U.S. Government and U.S. Citizens by certain countries

Imposes new obligations on covered businesses for people, process and technology

Elements of US sanctions, criminal/civil liability, foreign investment review, and cybersecurity and data privacy regulations.

California Cyber Audits

Who?

Every business covered by California Consumer Privacy Act whose processing of consumer personal information presents a significant risk to consumers' security shall complete a cybersecurity audit.

When?

Starting April 1, 2028, a business must submit to California regulators a certification under penalty of perjury, signed by an executive that it has completed a cybersecurity audit. After this, an audit must be completed every calendar year.

By Whom?

The auditor can be internal or external. If internal, the auditor can't be involved in any business activities that the auditor may assess (e.g., implementing/maintaining a cybersecurity program).

CCPA Cyber Audit: What Must be Included?

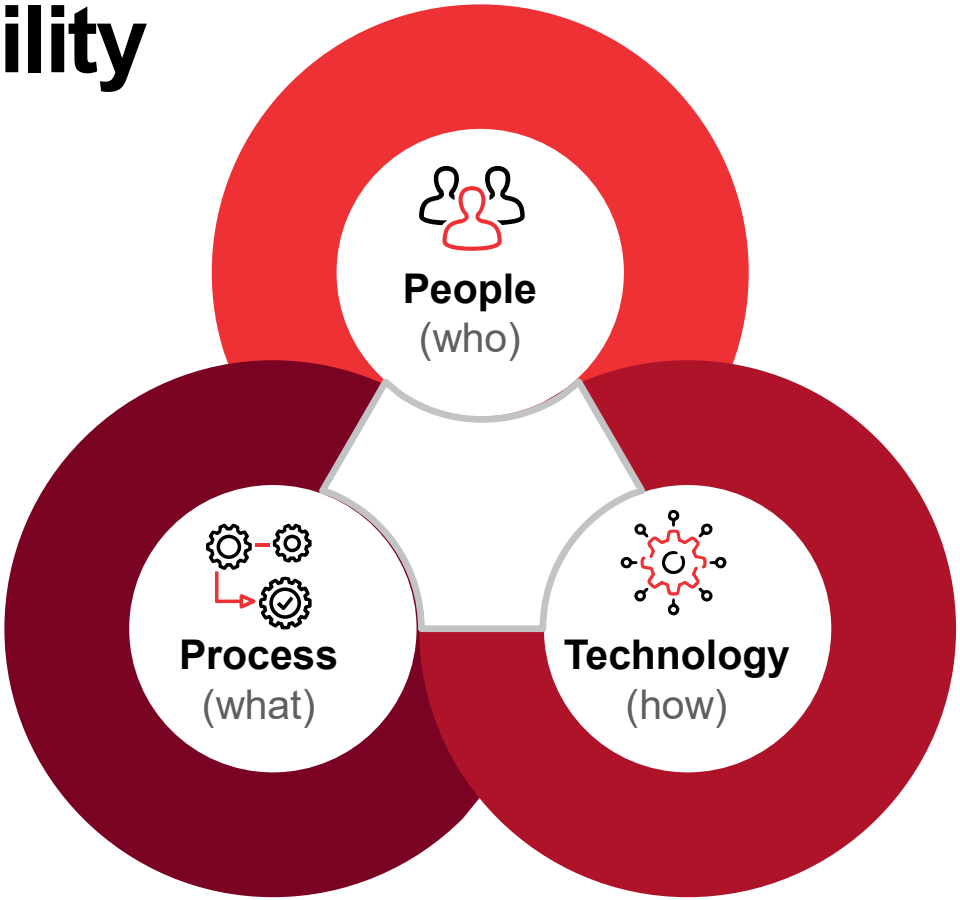
Identify and assess the business' establishment, implementation and maintenance of its cybersecurity program.

Provide any breach notifications made to impacted customers or agencies (in other states, territories, or countries).

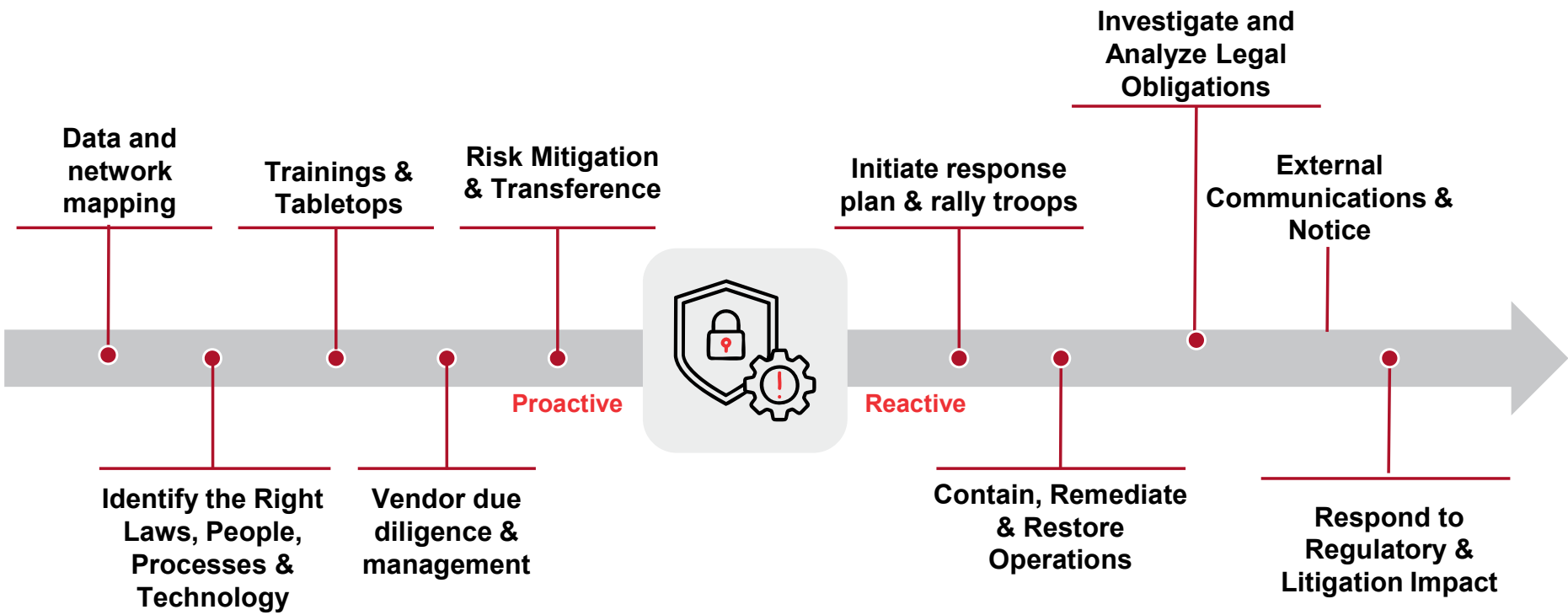
Identify compliance with each of the following if applicable. If not applicable, the business must explain why not compliant:

- MFA
- Cyber awareness/education/training
- Encryption of PI (at rest and in transit)
- Vendor management
- Data retention/destruction schedules
- Account Management and Access Controls
- Inventory and Management of PI
- Incident response management & tabletops

Defensible + Compliance = Shared Responsibility



Proactive & Reactive Cyber Compliance



Questions

Baker McKenzie empowers clients to compete in the global economy.

We provide comprehensive and practical legal advice that cuts through complexity with clear, actionable guidance. Our people represent diverse cultures and jurisdictions, combining local know-how with international expertise to ensure your business thrives across borders.

bakermckenzie.com