Acronym Overload!

CCPA, GDPR, HIPAA, GLBA, TCPA, CAN-SPAM

How Internal Audit can partner with the Privacy Office for operating and monitoring a sustainable internal audit program that minimizes risks to personal data holdings and drives accountability with global privacy and data protection laws and regulations.

January 14, 2020

pwc

The privacy landscape

Once the responsibility of a single department, cybersecurity and privacy now touch every part of the business on a global scale.

Health Insurance Portability and Accountability Act (HIPAA)

Mandates a myriad of privacy, security and breach notification requirements regarding protected health information (PHI)

California Consumer Privacy Act (CCPA)

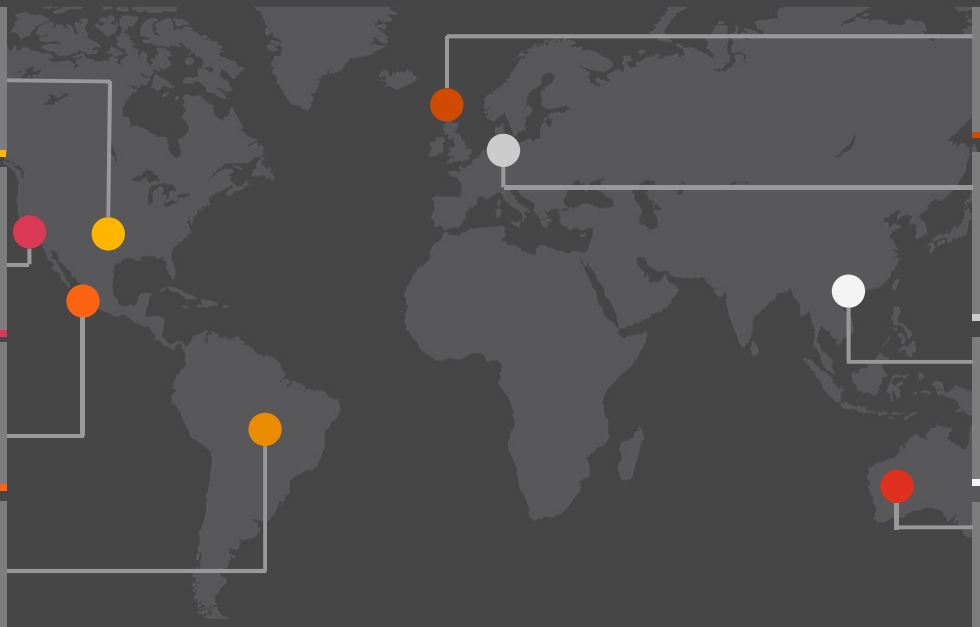
Designates an array of new rights regarding California residents' personal data, starting with the right to be informed about what kinds of personal data companies have collected

Mexico's Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Applies to private individuals or legal entities that process personal data for commercial use

Brazil Lei Geral de Proteção de Dados (LGPD)

Used Europe's General Data Protection Regulation (GDPR) as the blueprint for a national privacy framework for Brazil



UK Data Protection Act

Aims to modernize data protection laws to make sure they are effective in years to come

General Data Protection Regulation (GDPR)

Gives regulators unprecedented power to impose fines for privacy violations, requiring wide-scale privacy changes across organizations operating in the EU

China Cybersecurity Law

Establishes new requirements for user consent in China, as well as for personal data collection, storage, and sharing

Amendment to Australia Privacy Act

Introduces a mandatory notification procedure for data breaches as an amendment to the existing legislation from 1988

Note: this map is for illustrative purposes only and is not intended to be inclusive of all global privacy laws and regulations.

Privacy impacts across the organization

Privacy Office
- Enhancing consumer notice and transparency
- Enforcing privacy by design
- Conducting privacy impact assessments
- Honoring data subject rights

Legal
- Evaluating legal compliance gaps
- Advising on updates and changes to the law
- Managing contract process with third-party sellers, buyers, and processors
- Driving data breach notification
- Managing response to enforcement actions, private and state

Compliance
- Administering corporate policies and procedures, including records retention
- Enforcing privacy requirements across the organization

Internal Audit
- Monitoring and reporting privacy program and compliance
- Promoting continued accountability
- Performing independent assessments of administrative, technical, and physical controls

Information Security (IS)
- Promoting security throughout the data life cycle
- Assisting with data breach notification
- Driving incident response
- Involved in response to civil and state enforcement actions

Information Technology (IT)
- Enabling rights of access and deletion upon identity verification
- Enhancing data life-cycle management functions
- Managing consent indicators and logs
- Maintaining inventory of systems and processing activities

Marketing and Human Resources (HR)
- Limiting data collection and access as a leading practice
- Respecting opt-in and opt-out consent on a rolling basis
- Maintaining standards with third-party sellers, buyers, or processors
- Training employees on privacy compliance

Customer Service and Operations
- Enabling rights of access and deletion
- Fielding questions, inquiries, and concerns while maintaining brand reputation

PwC's ten privacy domains

Developing capabilities and mastering the ten privacy domains is the key to operating a successful and holistic privacy program.

Strategy and governance 	Define an overarching privacy program governance structure, with roles and responsibilities designed to coordinate and maintain the program on an ongoing basis.	• DPO strategy • Privacy program governance • Steering committee structure • Privacy program charter, KPIs • Privacy compliance controls framework	**Privacy by design** 	Develop a strategy and playbook for privacy by design (PbD) to incorporate privacy controls and impact assessments throughout the data life cycle for new and changing data use initiatives.	• PbD strategy and implementation playbook • PbD socialization workshop collateral • PIA tools, templates, and workflow • PIA risk rating engine
Policy management 	Privacy policies, notices, procedures, and guidelines are formally documented and consistent with applicable laws and regulations.	• Privacy policy • Notice inventory and analysis matrix • Policy gap analysis document • Change management strategy	**Information security** 	Identify existing security information protection controls and align security practices with legislative and regulatory considerations.	• Security strategy assessment • Risk analysis • User access management process • Defined backup, disaster recovery, and business continuity process • Encryption strategy • Security risk framework
Cross-border data strategy 	Determine go-forward cross-border data transfer strategy based on current and future planned data collection, use, and sharing.	• Cross-border mechanism assessment • Fitness assessment for alternative mechanisms (such as BCRs, binding corporate rules) • Updated vendor contract clauses and standard language (as needed)	**Incident management** 	Align incident response processes with legislative and regulatory specifications and reporting requirements. Establish a triage approach to evaluating potential privacy.	• Incident response and breach plan • Playbooks for business units • Triage frameworks for notifying supervisory authorities and individuals • Assessment mechanism to determine harm to the individual
Data life-cycle management 	Create ongoing mechanisms to identify new personal data processing and use activities, and apply appropriate checkpoints and controls.	• Data inventory and mapping • Personal data use governance mechanisms – legal basis analysis and documentation • Ongoing data inventory/mapping management and validation process	**Data processor accountability** 	Establish privacy requirements for third parties to mitigate risks associated with access to the organization's information assets.	• Inventory of third parties where personal data is transferred • Validation of data transfer mechanisms and associated contractual protections • Due diligence/assessment procedures • Risk ranking and ongoing monitoring plans for third parties
Individual rights processing 	Enable the effective processing of consent and data subject requests, such as data access, deletion, and portability.	• Data subject rights decision matrix, process flows, user experience guidance • Procedures and tools to receive, evaluate, and execute requests • Consent management framework	**Training and awareness** 	Define and execute a training and awareness strategy at the enterprise and role level.	• Data privacy training and awareness strategy • List of roles/functional areas for targeted training • Privacy training collateral

Internal Audit and the privacy journey

Internal Audit can achieve sustained accountability and influence positive risk management outcomes by establishing repeatable internal audit practices to continuously evaluate the compliance posture of privacy requirements helping to continuously improve and mature an organization's privacy program.

Operate & monitor key activities

Independently audit the organization's current privacy and data protection capabilities against a privacy controls framework. Identify capability gaps, capture management's response, and develop corrective action plans tailored to organizational goals, objectives, and risk profile.

Audit plan and design

- Perform discovery efforts to understand the organization's operational environment related to privacy
- Develop a privacy controls framework across the ten privacy domains, inclusive of test procedures and evidence request list, tailored to the organization's business model and personal data processing
- Identify internal audit respondents across the ten privacy domains to provide input into the privacy audit

Test

- Review existing documentation related to current state of privacy compliance
- Validate execution of control activities through sample testing, where appropriate
- Document audit results describing the current state of the organization's privacy compliance posture

Identify gaps

- Evaluate the organization's current state against the privacy controls framework, and document audit findings in an audit report, including capability gaps

Drive remediation activities

- Assist with capturing management's response to audit findings driving remediation accountability

Validate remediation

- Develop high level corrective action plans for capability gaps across the ten privacy domains tailored to the organization's goals, risk profile, and current and planned personal data processing
- Debrief leadership and other key stakeholders on outcomes of the privacy audit

The big picture: Effectively establish sustainable compliance and promote continued accountability.

An example of an internal audit workflow

- Hold initial scoping discussions and develop a planning memo based on the scope and purpose of the audit
- Develop an audit timeline and budget estimated hours
- Decide team structure for the audit and assign roles

- Develop an audit framework which aligns with the scope and purpose of the audit decided during the pre-engagement phase
- Send an audit announcement, which explains what the audit is assessing and its scope, to all personnel expected to be involved with the audit
- Following the announcement, hold audit kick off meetings with key stakeholders

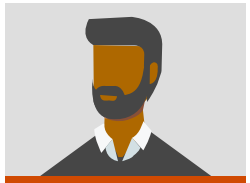
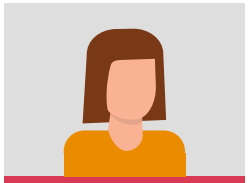
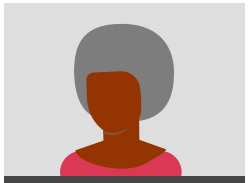
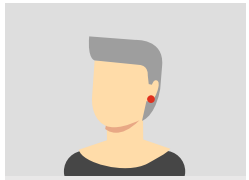
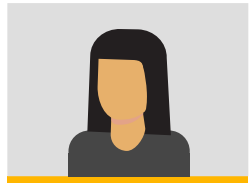
- Perform control testing against the finalized control framework
- Perform fieldwork which may consist of: stakeholder interviews to gain an understanding of business processes; observing processes taking place; or gathering evidence to test according to the control framework

- Validate observations with stakeholders who are knowledgeable over the processes being evaluated (they may have also been interviewed for fieldwork)
- Develop the audit report using a standard audit report template
- Ensure all changes to fieldwork and observations are reflected in the report and work papers

- Hold audit close-out meetings with senior leadership to ensure there is awareness over identified observations
- Assign management owners for each audit observation identified
- Meet with assigned observation owners to discuss submitting management responses which include planned remediation efforts for each observation

Key questions about cybersecurity and privacy

If leadership is not asking these questions, then perhaps you should...

CEO	CRO	CPO	CIO/CISO	Boardroom	CMO	CDO
						
Do we understand what the emerging risk landscape means for us?	Do we approach cybersecurity and privacy using a risk-based approach?	Is our organization respecting privacy while monetizing data?	Are we taking appropriate steps to protect our organization against cyber risk?	Do we have the information we need to oversee cybersecurity and privacy risks?	Are we gaining connectivity without losing consumer trust?	Do we have the personal data we need to achieve our business objectives?
Can we articulate our cybersecurity and privacy strategy across the organization?	Can we articulate our current cybersecurity and privacy risks?	Are we following applicable privacy laws and regulations?	Do we measure and demonstrate to stakeholders the effectiveness of our cybersecurity and privacy efforts?	Do we have a tested cyber incident response plan?	Does our program leverage strides in cybersecurity and privacy risk management to boost our economic performance?	Are we acquiring the personal data we need to achieve our business objectives in a compliant and ethical manner? How do we get the most value from our personal data?

Key takeaways

Internal Audit is key to supporting the Privacy Office in establishing and testing necessary data governance controls.

Agreement

Work in concert with the Privacy Office to design and develop the privacy controls for both implementation and then subsequent internal audits for sustainable compliance with privacy requirements.

Readiness

Perform readiness assessments to evaluate the design of privacy controls ensuring plans to meet privacy requirements are directionally correct and minimize risks to the company as a whole.

Partnership

Inform leadership and staff on privacy laws and regulations impacting their organization and partner with the Privacy Office for risk management purposes ensuring board and/or executive level visibility to critical issues.

Collaboration

Execute audits in a collaborative manner coupling the general privacy knowledge with specific internal audit know-how and resources in order to effectively and efficiently evaluate the controls design and/or operational effectiveness of privacy requirements.

Thank you

pwc.com