		Enterprise Risk Management Applying Enterprise Risk Management to Compliance Risks
		Example - General Privacy Risk in a Global Organization
ERM Component & Principle		**Characteristics of Effective Compliance Risk Management**
Governance and Culture		
1	Exercises board risk oversight	(a) Board is knowledgeable of assessment and response regarding privacy-related risks; (b) Board receives timely updates regarding the changing privacy legal, regulatory, professional practice and related risk environment and how the organization's operation has addressed related risks.
2	Establishes operating structures	(a) As part of the overall compliance infrastructure, a privacy function has been established (to include a sub-commitee or working group) to manage related risks. Management responsible for oversight of this function is properly situated at a senior level within the org structure, with unfettered access to the board of directors or a board-level committee tasked with compliance oversight; (b) the internal compliance committee consisting of representatives from across the organization is knowledgeable regarding privacy risks including related information security/IT risks impacting privacy; (c) an individual responsible for privacy-related risks, is assigned to oversee day-to-day operations of the organization's privacy function, to include but not be limited to, establishing and maintaining: A privacy operations team, sub-committee, or working group, privacy policies and procedures (*including Privacy Impact Assessment (PIA) protocols*), records of processing, privacy notices, privacy awareness efforts, privacy breach response protocols (*including root cause and remediation*), privacy risk assessment, third party supplier privacy due diligence and broader monitoring activities embedded within the lines of business.
3	Defines desired culture	(a) The Code of conduct, and associated policies/procedures, address compliance and related expectations with privacy standards and regulations globally, and are a response to the risks identified through privacy risk assessments; (b) The organization's privacy standards, appropriate practices and related expectations are clearly defined and stated in the organization's overall privacy policy, which is posted, distributed, and made readily available to all employees, customers and consumers, and applicable third-parties. For example, privacy policies address basic concepts and expectations such as standards related Notice, Choice, Collection, Access (*logical and technical*), Transfers to Third Parties, Transmission, Storage, Retention, Disposal, Security for Privacy and the inherent privacy rights within these principles where applicable; (c) The organization has defined and implemented measures which identify accountability for, and consequences for failure to adhere to privacy policies and protocols.
4	Demonstrates commitment to core values	(a) Leadership actively promotes and demonstrates a commitment to a culture that places value and importance on protecting the privacy and related personal information of its employees, customers and other stakeholders, and adhering to compliance with all applicable global or local standards and guidelines that set forth requirements and expectations; (b) compliance standards and expectations are consistently and regularly communicated throughout the organization; (c) Well-publicized and accepted reporting channels are in place and supported by leadership (*including a hotline mechanism for confidential and anonymous reporting*), where members of the organization can feel safe seeking help and reporting privacy concerns, without fear of retaliation; (d) Reporting channels are supported by leadership, to include a consistent policy and practices that protect reporters from retaliation; (e) These privacy related core values are periodically assessed as privacy related data use cases change such as with intelligent automation, monitoring at scale, etc.
5	Attracts, develops and retains capable individuals	(a) Hires qualified personnel who, through background checks, that exhibit no red flags of corrupt tendencies, or past history of compliance violations that would be inconsistent with an effective C&E Program; (b) Organization ensures personnel hired into the organization (*and contracted third-parties*) meet requisite requirements and expectations defined in defined job descriptions or statements of work, and are appropriate to the role (*e.g., education, experience*); (c) Risk based data privacy specific due diligence is performed on relevant third parties prior to entering into contracts and periodically thereafter, (d) Organization's performance goals are aligned with its policies so as to create incentive to comply with those privacy standards, (e) Training on privacy and management of privacy risks is provided to appropriate levels of employees and third parties, contextualized based on the privacy related activities they are responsible for. For example, related IT personnel responsible for system ownership would receive Privacy Impact Assessment (PIA) education; (f) Compliance with applicable privacy laws, policies, and other organizational compliance standards are incentivized through periodic performance evaluations, and other incentives.
Strategy and Objective Setting		
6	Analyzes business context	(a) Organization regularly evaluates the level, probability, and impact of privacy risks (i.e.,*the identification of reasonably foreseeable material risks, both internal and external, that could result in the organization's unauthorized collection, use, or disclosure of personal information and an assessment of the sufficiency of any safeguards in place to control these risks*). This includes evaluation of the organizations' business strategy and operation planning, and active monitoring of changes to applicable laws, regulations, professional practice, and industry trends through external benchmarking and other efforts; (b) Organization actively considers business operations with exposure to privacy-related risks and analyzes existing and future needs related to people, processes and technology. In particular, the organization examines how its information security program adequately addresses privacy risks such as through Privacy by Design mechanisms, and related controls (c) Privacy Impact Assessments (*PIA system and process*) are conducted that help identify potential risks to include data flow analysis activities that map how proposed and existing business processes manage personal information, and how this information flows through the organization as a result of business activities; (d) The organization specifically addresses privacy risks as a component of its third-party (supplier/vendor) due diligence program and the related information security considerations.
7	Defines Risk Appetite	(a) Privacy risks are included as part of the organization's risk profile in determining its risk appetite; (b) Management defines and regularly evaluates its risk appetite and tolerance for potential noncompliance with applicable global and local privacy standards, regulations, professional standards and other requirements; includes the impact of potential privacy breaches, when considering its business strategy and objective setting (*e.g., Privacy Impact Assessments*); (c) When determining risk appetite, the organization evaluates privacy risks generally across its operations, to include specific considerations of privacy risks by sub-categories (e.g., *type of risk, business unit or organizational function, and location or region*).
8	Evaluates alternative strategies	Privacy risk(s) and its corresponding risk appetite are specifically considered as the organization develops and evaluates alternative business strategies and objectives. For example, the organization specifically addresses privacy risks through its mergers, acquisitions and related transactions.
9	Formulates business objectives	(a) The organization considers the implications of its business objective setting related to privacy risks through Privacy Impact Assessments, and other risk management efforts, (b) Performance measures are established with consideration given to their potential effects on privacy risks, (c) Tolerance for risk is considered in connection with setting business objectives.

Performance		
10	Identifies risk	(a) Privacy risks are identified as relevant, top-tier risk to the organization, and it is priorized accordingly, (b) Specific Privacy risks are identified and analyzed through periodic risk identification and assessment activities that leverage internal/external inputs such as laws and regulations specific to privacy, industry trends and vulnerabilities, IT operations, business operations and inherent changes in data flows whether due to change in data type, data processing environment (*e.g. remote working location, cloud storage, cross border data flows, or other*), related information security controls, data incident response trends within the organization including root cause and remediation, management input, employee questionnaires, surveys, and other identification efforts and input; (c) The organization identifies and evaluates privacy risks and sub-categories of related-risks specific and unique to its operations, when determining likelihood, severity, prioritization, and risk responses (*e.g., risks related cyber attacks versus employee theft of data*). (d) Consideration is given to how the use of third parties affects privacy risk and the related trends in the third party privacy due diligence risk analysis.
11	Assesses severity of risk	(a) Determining the severity of privacy risks is assessed using a methodology that is consistent with the assessment of other compliance-related risks; (b) Specific privacy risks are reassessed on a regular basis or as circumstances indicate there has been a change in severity, through Privacy Impact Assessments or other methodologies for example that may be present within applicable laws; (c) Consideration is given to assessing privacy risks at multiple levels or at different regions or based on other factors that indicate privacy risk mitigation and compliance with standards may not be consistent across the organization.
12	Prioritizes risks	(a) Privacy risks are appropriately prioritized using criteria consistently applied to all compliance risks and considers the organization's risk appetite, along with the likelihood and impact of risk occurrence; (b) Consideration is given to prioritizing privacy risks differently by location, region or operating group based on unique characteristics associated with each.
13	Implements risk responses	(a) Organization implements risk management plans, controls, and other mitigation strategies to effectively address privacy risks (*e.g., enhance employee training related to privacy, improve IT controls for managing personal data, changing user rights to restrict data access*); (b) If privacy risks exceed the target risk level, the organization has designed and implemented controls, including new or modified policies and procedures and updated training and awareness efforts, designed to prevent or detect in a timely manner, violations and/or compliance failures related to global privacy laws and standards; (c) The organization takes timely remediation efforts following known instances of noncompliance in order to reduce risk of recurrence, to include notification and disclosures requirements as set forth by specific jurisdictions and laws where the organization operates; (d) Privacy risks identified through Privacy Impact Assessments, and other risk management efforts (*including data incident response*), are documented and risk management plans and controls are implemented to mitigate and manage the risks.
14	Develops portfolio view	Considers privacy-related risks as part of an overall portfolio of compliance risks, which in turn are viewed as part of a portfolio of all categories of risks facing the organization.
Review and Revision		
15	Assesses substantial change	Changes in the external and internal environment are considered in connection with assessing and updating efforts to manage and mitigate privacy risk throughout the organization and monitor related controls, to include leveraging findings to help improve the effectiveness of the C&E Program.
16	Reviews risk and performance	(a) Auditing and monitoring activities are in place for evaluating and monitoring privacy risk management and compliance; (b) Privacy Impact Assessments are conducted periodically to assess the mitigation and management of privacy-related risks throughout the organization; (c) Functional/operating units may incorporate additional contextualized privacy monitoring activities applicable to their profile; (d) The board and Leadership receives periodic updates on the status of privacy risk and performance review results; (e) Privacy risk management controls and other mitigations efforts periodically receive follow-up by internal audit.
17	Pursues improvement in ERM	The C&E program and risk management efforts related to privacy are periodically evaluated for completeness and effectiveness using one or more of the following methods: (a) internal audit, (b) independent third parties, or (c) self-assessment tools
Information, Communication, and Reporting		
18	Leverages information and technology	(a) The organization utilizes techology and available internal and external data (*including data obtained from third parties that are part of the organization's privacy risk universe*) to perform analytics aimed at identifying anomalies indicative of violations or break-downs in privacy-related internal controls (*e.g., continuous monitoring of data access and how/when customer personal information flows through systems*); (b) Technology is leveraged to deliver effective privacy training to employees and relevant third parties; (c) Ongoing Privacy Impact Assessments leverage technology and information to include data flow analysis activities that evaluate how and where personal/sensitive information flows through systems and databases; (d) the systems and processes covered by Privacy Impact Assessments are periodically evaluated for the effectiveness of measures/controls in place to protect data.
19	Communicates risk information	(a) Privacy risk assessment findings, prioritizations, and mitigation efforts/strategies are included in regular reports by a designated privacy leader, to the board/committee and organization leadership; (b) Leaders/managers in the organization who oversee the privacy risk management function are provided with relevant information and ongoing education to assist them in their compliance oversight roles.
20	Reports on risk, culture, and performance	(a) The organization identifies the appropriate audiences (*e.g., senior leadership, board, key internal stakeholders*), to receive periodic reporting on privacy risk management and mitigations efforts, and provides timely and relevant information regarding risk mitigation effectiveness (*e.g., Privacy Impact Assessment Report*); (b) the organization periodically reports on the assessment of culture, including the culture surrounding the importance of compliance with privacy standards, regulations, and related expectations; (c) The organization has implemented measures which identify accountability for, and consequences for failure to adhere to privacy policies and protocols. Privacy management reporting provides results and outcomes of these measures (*e.g. breaches by rank, etc.*).