IAPP Practical Privacy Series 2014

New York City

Privacy Governance and Controls: How Do You Know You Are Doing it Right?

#PracticalPrivacy
<table>
<thead>
<tr>
<th>Agenda</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Global Data Protection and Privacy (DPP) Organization Structure</td>
</tr>
<tr>
<td>▪ Privacy Compliance – The 3 Lines of Defense (LOD) Model: Overview</td>
</tr>
<tr>
<td>▪ Privacy Compliance – The 3 Lines of Defense Model: Detailed Responsibilities</td>
</tr>
<tr>
<td>▪ Privacy Compliance – LOB Responsibilities (1st Line of Defense) Across Information Life Cycle</td>
</tr>
</tbody>
</table>
Privacy Compliance - The 3 Lines of Defense (LOD) Model: Overview

JPMC’s Privacy Program establishes the firm-wide standards for maintaining the secure, confidential, fair and lawful treatment of information relating to our customers, clients, and employees. The Privacy Program covers all JPMC lines of business, corporate groups, and legal entities, and information collected, processed, stored, transmitted, and/or transported. (Privacy also includes data protection responsibilities handled by Privacy Compliance.)

1st LINE OF DEFENSE
Execution & Control
- Properly handle and safeguard information through the lifecycle of the relationship (clients, consumers, and employees), from prospecting through termination of the relationship
- Establish procedures that align to laws, regulations and Firm DPP Policies & Standards
- Own the control and risk environment; implement the control framework, including execution of process reviews, risk acceptances where necessary, and validation of issue closure
- Conduct Risk Control Self Assessments and quality review of control effectiveness
- Promote transparency and escalate to oversight forums such as Business Control Committees, Technology Councils etc.
- Manage applications and infrastructure, and protect the environment against security threats
- Administer training programs

2nd LINE OF DEFENSE
Oversight, Program Management & Policies
- Maintain Privacy program and/or Lead that includes the seven core practices for an effective compliance program. Develop governance, policies, oversight and accountability model to identify and track issues/trends and remediation activities
- Provide advice and interpretation regarding laws, regulations, and standards
- Provide SME expertise to provide effective tools and advice to support the control framework, including with regard to Privacy Controls and Standards
- Report and escalate to oversight forums such as Risk & Control Committee, Compliance Control Committee, IT Risk Committee, Data Protection & Privacy Forum
- Hold LOB accountable for execution; verify RCSA framework is in place and working effectively
- Identify and evaluate risks and effectiveness of action plans; perform periodic risk assessments; develop appropriate compliance coverage (monitoring, testing, and training for privacy risks based on inherent risk ratings)
- Develop training and monitor for completion

3rd LINE OF DEFENSE
Independent Assurance
- Independently evaluate and opine on the adequacy and effectiveness of the control environment
- Report to the Audit Committee of the Board and senior management on a periodic basis significant control issues and the overall adequacy of the control environment
- Perform Audit-focused root cause analysis and identify and determine severity of issues
### Privacy Compliance – The 3 Lines of Defense Model: Detailed Responsibilities

<table>
<thead>
<tr>
<th>1st Line</th>
<th>Primary Ownership and Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Council</td>
<td>Business Control</td>
</tr>
</tbody>
</table>

#### Governance
- LOBs: Establish procedures to align to policies, laws, and regulations; execute programs; manage ops infrastructure and risk environment
- Control Officers: Implement framework that includes process reviews, self assessments, quality checks, and escalation of risks/issues
- CIOs/Tech controls: Manage system infrastructure and controls per data classifications

**Prospecting, Sales & Marketing**
- LOBs: Protect data collected; honor opt-outs and Cross Marketing restrictions; Approve and implement privacy notices/disclosure

**On boarding and Off boarding**
- LOBs: Assist in account opening, honor privacy preferences; adhere to Cross Marketing restrictions; obtain client consents; and assist with vendor disengagement

**BAU/Relationship Management**
- LOBs: Protect data; manage/escalate incidents, ensure correct contracts terms

**Change Management**
- LOBs: Participate in key processes to ensure appropriate processes consider Privacy by design

<table>
<thead>
<tr>
<th>2nd Line</th>
<th>Functionally Independent Checks and Balances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>Legal</td>
</tr>
</tbody>
</table>

- **Compliance**
  - Maintain a Privacy Program Lead for oversight and accountability
  - Develop appropriate framework via Policy, Standards, Notices and training
  - Address and escalate significant matters
  - Integrate effectively into Firm processes
  - Participate in relevant committees
  - Create visibility into issues and trends via appropriate reports, metrics, and analysis

- **Legal**
  - Provide strategic legal services across the organization in support of business areas and Corporate Center
  - Provide legal analysis for new products services, activities, engagements
  - Advise and counsel on other legal questions on privacy, confidentiality, information security and banking secrecy

- **IT Security and Risk Leadership**
  - Establish appropriate administrative, technical and physical safeguards to control JPMC information through its life cycle
  - Adopt a model for Technology Risk Governance that considers Tech Compliance in design
  - Manage IT Policy & Standards
  - Implement Data Protection programs, application security, cyber security, and insider threat modeling
  - Conduct investigations, including forensic investigations of breaches, suspected fraud, employee wrongdoing & identify control gaps

<table>
<thead>
<tr>
<th>3rd Line</th>
<th>Independent Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Audit</td>
<td></td>
</tr>
</tbody>
</table>

- **Independent Audit**
  - Independently evaluate and opine on the adequacy and effectiveness of the control environment
  - Report to the Audit Committee of the Board and senior management on a periodic basis significant control issues and the overall adequacy of the control environment
  - Perform Audit-focused root cause analysis and identify and determine severity of issues
Privacy Compliance – LOB Responsibilities (1st Line of Defense) Across Information Life Cycle

Privacy risks are based on the nature of the information processed from collection through destruction by the JPMC, its business partners and service providers. Each LOB is responsible for adhering to the Policies & Procedures to ensure: 1) the proper handling and safeguarding of information 2) the appropriate stewardship & ownership of data and 3) proper alignment to the control framework.

<table>
<thead>
<tr>
<th>Life Cycle</th>
<th>Responsibilities</th>
<th>Considerations</th>
</tr>
</thead>
</table>
| Prospecting, Sales & Marketing  | • Market to approved prospects  
                                       • Protect data gathered during prospecting activities | • Client consent management  
                                       • Data use and protection requirements  
                                       • Rules for internal sharing/cross-marketing  
                                       • Data retention and destruction |
| On Boarding                     | • Create and/or collect only appropriate data required to offer the product/service  
                                       • Protect data gathered during onboarding process  
                                       • Identify information owners and categorize data elements  
                                       • Accurately & securely set up accounts; provide privacy notices/disclosures  
                                       • Manage contracts/SLAs, eg for appropriate clauses and execution  
                                       • Conduct appropriate due diligence on new hires, consultants and contractors | All of the above in addition to:  
                                       • Proper account setup  
                                       • Proper transmissions of data  
                                       • Booking location rules |
| Relationship Management         | • Handle information properly from data collection to destruction  
                                       • Secure data properly, eg controlling access to need-to-know; document risk acceptances  
                                       • Comply with consumer opt-outs, sharing restrictions, and contract requirements  
                                       • Provide annual and regulatory notices, obtain and manage consents, handle complaints  
                                       • Manage and verify effective infrastructure/controls for customer authentication, technology security, and physical access  
                                       • Perform monitoring and surveillance in accordance with Policies & Procedures  
                                       • Manage potential breaches; remediate risks  
                                       • Manage suppliers adequately and for adherence to MSA/contract and/or SLA  
                                       • Appropriately assign record retention codes & adhere to legal holds requirements  
                                       • Administer and track training | All of the above in addition to:  
                                       • Privacy Preferences  
                                       • Internal/Affiliate sharing restrictions  
                                       • Adherence to contract provisions  
                                       • Regulatory notice & registration  
                                       • Information processing restrictions  
                                       • Technological, Administrative & Physical Safeguards  
                                       • Monitoring/Surveillance Restrictions  
                                       • Red Flags Program  
                                       • Record Retention/Legal Hold requirement  
                                       • Training/Messaging |
| Off Boarding                    | • Close accounts in accordance with policies and procedures  
                                       • Return and/or destroy data properly; adhere to JPMCs record retention requirements  
                                       • Oversee employee exits, timely terminate access and obtain JPMC assets | • Account Closure/Status Changes  
                                       • Dormancy  
                                       • Record Retention  
                                       • Access Control |
| Change Management               | • Engage in Outsourcing, Off-shoring/On-shoring, & Technology Change projects  
                                       • Ensure Cross Border Data Transfers are reviewed and approved, or escalated as needed  
                                       • Assess regulatory changes to understand impact; adapt systems/processes to address reqs.  
                                       • Appropriately retire databases, systems, applications | • New Business Initiative  
                                       • Outsourcing  
                                       • Off-shoring  
                                       • Technology Changes |
Q & A