FPF Privacy Metrics: Summary

Uses

Purposes

Privacy program leaders use metrics for various purposes. These include:

- Operational. Measuring and ensuring compliance with policies, laws and regulations (E.g., DSARs and incident reporting) as well as internal goals and objectives (E.g. training, awareness, SLAs).
- Business imperatives. Facilitating market access for products and services (e.g., PbD, DPIAs, answering RFI/RFP, and customer questions).
- External. Supporting brand reputation and differentiating from competition (e.g., thought leadership, advocacy, transparency, best practices, special projects).

Audiences

Privacy program leaders use metrics to communicate with various stakeholders. One of the challenges the Working Group discussed involves fashioning a set of metrics into a narrative, that is, telling a story, to different stakeholders, ranging from the CEO to consumers and regulators. Audiences for privacy metrics include:

Stakeholders	Purpose of reporting metrics
Executives (CEO/ Board of Directors)	- Ensure buy in/support - Proper allocation of staff/resources to risks - Report on risk/impact on bottom line - Report on program maturity/status/progress
Senior Leadership	- Ensure buy in/support - Triage priorities - Control effectiveness - Ensure support in gathering data
Privacy Team	- Issue spotting: control program effectiveness / remediate problems - Information / dashboards - Getting team aligned on most important goals - Internal allocation of resources - Performance reviews
External	-- Customers: transparency and trust, differentiate brand Regulators: compliance, demonstrating accountability - Investors and shareholders: demonstrating effectiveness
Internal Audit	- Monitoring compliance, risks, costs, and remediation
Employees	- Ease of engaging with privacy team - Training and awareness - For sales employees, ability to share privacy practices and protections with customers for differentiation

Metrics

While different organizations measure different activities and trends, the inventory of metrics is generally standard. Most organizations measure daily privacy program activities such as

responding to individual complaints and requests, responding to incidents or breaches, offering training to team members and employees, conducting data mapping and privacy impact assessments, negotiating and signing data processing agreements, and so forth. The challenge is weaving these numbers into a narrative in order to achieve program goals such as increasing resources, ensuring organizational support and enhancing trust. These are some of the metrics we have identified:

Category	**Item**	**Metrics**
Individual rights	DSARs	Received Closed In progress Duration % satisfied Requests by type, region, SLA times
	Incidents/ breaches	# of incidents by type/severity % of incidents by type, closed with SLA commitments % of incidents where root cause has been identified and corrective action taken
	Complaints	Similar
	Queries	Similar
Training and awareness	Trainings	Offered Employees trained Attendees (in person) % of employees passing privacy challenge
	Privacy FAQs	Offered Engagement
Commercial	DPAs	Negotiated customer Closed customer Negotiated vendor Closed vendor
	RFI/RFP	Privacy compliance

		attestation requests
	M&As/ Divestitures/ TSA/ Joint Ventures	Negotiated/closed
Accountability	DPIAs	# of DPIAs completed
	Data Mapping	# of applications data mapped # of applications that require data mapping # of completed ROPs
	Projects / products advised on	# of marketing activities advised on # of HR activities advised on # of new business/models/ technology solutions advised on (e.g., cloud as a service) # of cross-functional projects
Privacy Stewards (hub & spoke)	Privacy projects in product teams	# of PIMs remediated # of DPIAs supported # of ROPs supported # of department personal data use reviews for data extraction # of cross-functional privacy projects # of DSARs supported # of department specific data privacy trainings offered # of data privacy FAQs and awareness communications (department/role-specific)

Strategies on how to use

Privacy program leaders deploy a toolkit that includes strategies to deliver a coherent story to various stakeholder groups.

- Simplify
  - Use metrics to tell a story, offer takeaways
  - Make insights obvious including to those without privacy expertise
  - Use metrics to highlight specific needs for investment/resources
  - Show how you execute your strategy
  - Help organization make smart business decisions

- Program Maturity (source: MITRE Privacy Maturity Model)
  - Ad Hoc. The program requirement is new, not yet reliably implemented, or undocumented.
  - Defined. The program requirement is documented but may not be implemented consistently.
  - Consistently Implemented. The program requirement is established as a standard business practice and its use is enforced by the organization.
  - Managed & Measurable. The program requirement is quantitatively managed with agreed upon metrics; the effectiveness of the process used to meet program requirements is monitored.
  - Optimized. Program requirement management includes deliberate and continuous process improvement; automation is used to continuously monitor and improve effectiveness.

- Progress from Activities to Trends to Outcomes (See Anna Zeiter presentation for examples)
  - Activities (e.g., # of DSARs, incidents)
  - Trends (e.g., % of DSARs closed satisfactorily over time)
  - Outcomes (e.g., customer trust for how their data is used)

- Link to business strategy
  - Tie metrics to the strategic goals of the organization
  - Prove delivery on team/organization's commitments

- Using template to show board of directors a standard set of core metrics
  - Demonstrate current status as well as changes over time (trends)

    - Highlight any new developments with additional metrics
    - Best practice in communicating to Board includes using a standard set of metrics (for consistency) but with drill down on key issues for decisions (e.g., need for resources, root cause analysis for incidents, response to changing regulatory landscape) and additions for new developments

- Public policy metrics
    - New developments watchlist (e.g., CPRA ballot initiative)
    - Will affect the business or not (e.g., opt in requirements affect business model)
    - We can impact or not (e.g., text still not finalized)

- Enable decision making
    - Provide transparency into current risks and enable management decisions (e.g., volume of open DSARs rising in a jurisdiction => channel additional resources to that jurisdiction).

- Benchmark across industries and jurisdictions
    - Use standards such as:
        - AICPA GAPP
        - NIST Privacy Framework v2
        - ISO (27001, 27018, 27701, 29100, ISO/PC317)
        - Ethics and Compliance Initiative
        - Consulting firm frameworks
    - Use industry benchmarks such as:
        - IAPP Governance Report
        - IAPP DPO Report template

- Documentation / recording
    - GRC tools
    - Ticketing systems
    - Privacy contract mailbox
    - ServiceNow (FAQs)

Additional resources

- NIST Privacy Framework
- MITRE Privacy Maturity Model
- World Economic Forum, Toward Common Metrics and Consistent Reporting of Sustainable Value Creation

- IAPP/Trustarc Measuring Privacy Operations
- IAPP-EY Annual Governance Report 2019
- IAPP Template DPO Report to Management