Components of a Comprehensive Program

Scott Taylor
HP Privacy Office
February, 2014

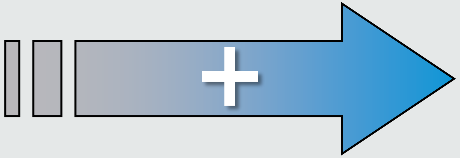
Accountability

Demonstrating Capacity

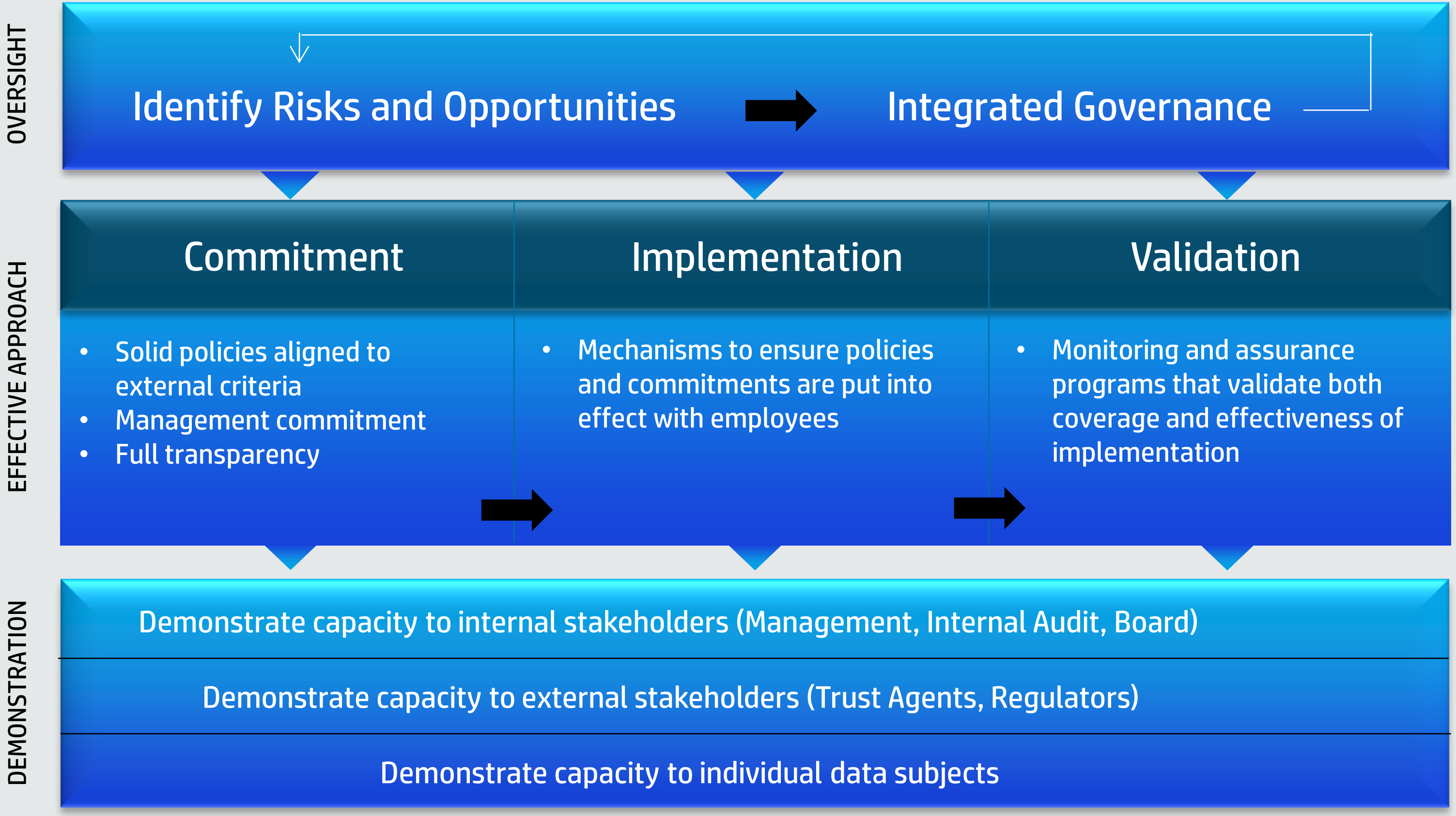
- Accountable organizations have comprehensive programs to assess risks, mitigate risks, implement compliant programs, and continually evaluate the effectiveness of implementation.
- In addition, these organizations should stand ready to demonstrate their programs and processes when appropriate.

A Fundamental Shift to Accountability

LIABILITY	ACCOUNTABILITY
Decisions are made based on technical compliance with local laws and regulations • Focuses on the minimum standard • What is legally defensible	Decisions are additionally made based on considering concurrent risks and a set of ethics- & value-based criteria beyond liability • Tie to social and/or company values • All employees accountable for stewardship of data under their charge • Effective & based on expectations



Accountability Ecosystem



OVERSIGHT

Identify Risks and Opportunities → Integrated Governance

EFFECTIVE APPROACH

Commitment

- Solid policies aligned to external criteria
- Management commitment
- Full transparency

Implementation

- Mechanisms to ensure policies and commitments are put into effect with employees

Validation

- Monitoring and assurance programs that validate both coverage and effectiveness of implementation

DEMONSTRATION

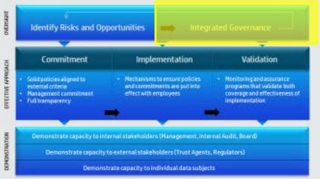
Demonstrate capacity to internal stakeholders (Management, Internal Audit, Board)

Demonstrate capacity to external stakeholders (Trust Agents, Regulators)

Demonstrate capacity to individual data subjects

Governance

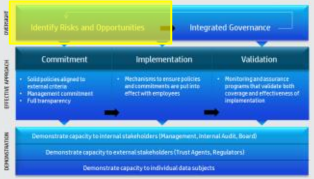
Expectations


OVERSIGHT
Identify Risks and Opportunities
Integrated Governance
EFFECTIVE APPROACH
Commitment
Implementation
Validation
• Solid policies aligned to external criteria
• Management commitment
• Full transparency
• Mechanisms to ensure policies and commitments are put into effect with employees
• Monitoring and assurance programs that validate both coverage and effectiveness of implementation
DEMONSTRATION
Demonstrate capacity to internal stakeholders (Management, Internal Audit, Board)
Demonstrate capacity to external stakeholders (Trust Agents, Regulators)
Demonstrate capacity to individual data subjects

- All groups within the organization that may create risks in the collection, use or maintenance of personal information are identified
- An ongoing engagement and dialog occurs
- An overall, collective strategy exists for Privacy and Data Protection, it is understood by all groups, and gets integrated into appropriate programs

Risk Assessment

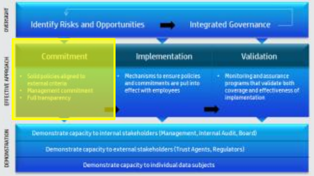
Expectations


OVERSIGHT
Identify Risks and Opportunities
Integrated Governance
EFFECTIVE APPROACH
Commitment
Implementation
Validation
Solid policies aligned to external criteria
Management commitment
Full transparency
Mechanisms to ensure policies and commitments are put into effect with employees
Monitoring and assurance programs that validate both coverage and effectiveness of implementation
DEMONSTRATION
Demonstrate capacity to internal stakeholders (Management, Internal Audit, Board)
Demonstrate capacity to external stakeholders (Trust Agents, Regulators)
Demonstrate capacity to individual data subjects

- The Governance group discusses the potential risks associated with Privacy and Data Protection – considering all concurrent risks to the company and individuals
- Risks are documented with descriptions, tolerances, and impacts
- The Governance group makes collective decisions about the need for mitigation and where appropriate, ownership is assigned and progress is reported regularly

Policies

Expectations

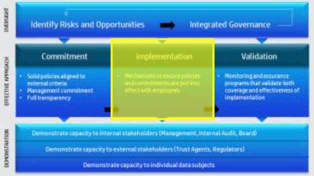


OVERSIGHT
Identify Risks and Opportunities
Integrated Governance
EFFECTIVE APPROACH
Commitment
Solid policies aligned to external criteria
Management commitment
Full transparency
Implementation
Mechanisms to ensure policies and commitments are put into effect with employees
Validation
Monitoring and assurance programs that validate both coverage and effectiveness of implementation
DEMONSTRATION
Demonstrate capacity to internal stakeholders (Management, Internal Audit, Board)
Demonstrate capacity to external stakeholders (Trust Agents, Regulators)
Demonstrate capacity to individual data subjects

- The organization establishes and maintains policies that are aligned to external criteria and internal company values, including standards that help the organization interpret the policies
- Senior management understands, accepts and supports the policies
- Data subjects are informed about the organization’s commitments/ practices through clear and conspicuous transparency

Implementation

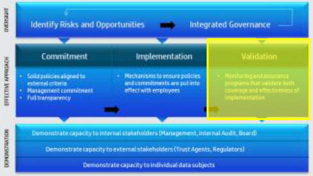
Expectations


OVERSIGHT
Identify Risks and Opportunities
Integrated Governance
EFFECTIVE APPROACH
Commitment
Implementation
Validation
• Solid policies aligned to external criteria
• Management commitment
• Full transparency
• Mechanisms to ensure policies and commitments are put into effect with employees
• Monitoring and assurance programs that validate both coverage and effectiveness of implementation
DEMONSTRATION
Demonstrate capacity to internal stakeholders (Management, Internal Audit, Board)
Demonstrate capacity to external stakeholders (Trust Agents, Regulators)
Demonstrate capacity to individual data subjects

- The team responsible for Privacy and Data Protection should identify and communicate with the groups that collect, use and maintain personal data
- Based on clear Policies and Standards, the organization should have ongoing mechanisms and processes to educate and guide employees in implementation
- It should be easy for employees to get answers to questions about implementation
- In HP's case, we have invested in a sophisticated tool that guides employees, connects them to the Privacy Office for consultation/approvals, and tracks history and trends for collection and use of data

Validation

Expectations



OVERSIGHT

Identify Risks and Opportunities → Integrated Governance

EFFECTIVE APPROACH

Commitment
- Solid policies aligned to external criteria
- Management commitment
- Full transparency

Implementation
- Mechanisms to ensure policies and commitments are put into effect with employees

Validation
- Monitoring and assurance programs that validate both coverage and effectiveness of implementation

DEMONSTRATION

Demonstrate capacity to internal stakeholders (Management, Internal Audit, Board)

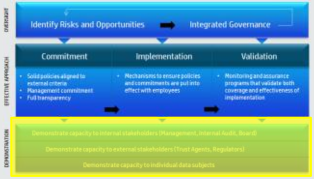
Demonstrate capacity to external stakeholders (Trust Agents, Regulators)

Demonstrate capacity to individual data subjects

- The team responsible for Privacy and Data Protection should establish and oversee processes to validate programs are being implemented in a manner consistent with the Policies and Standards
- When issues are identified, processes should exist to clarify/ modify Policies, Standards, Education, or Guidance
- Results should be reported to the Governance group and considered in risks

Demonstration

Expectations


OVERSIGHT
Identify Risks and Opportunities
Integrated Governance
EFFECTIVE APPROACH
Commitment
Implementation
Validation
• Solid policies aligned to external criteria
• Management commitment
• Full transparency
• Mechanisms to ensure policies and commitments are put into effect with employees
• Monitoring and assurance programs that validate both coverage and effectiveness of implementation
DEMONSTRATION
Demonstrate capacity to internal stakeholders (Management, Internal Audit, Board)
Demonstrate capacity to external stakeholders (Trust Agents, Regulators)
Demonstrate capacity to individual data subjects

- The team responsible for Privacy and Data Protection should stand ready to explain, discuss and defend the components of their program
- Internally, reporting should be provided to senior management regularly
- Externally, reporting may be done as part of communications to data subjects and if requested, made available to regulators and other interested parties
- Such demonstration can also form the basis for certification or approval in binding co-regulatory programs like BCRs and CBPRs

Conclusion

Rationale for establishing a Comprehensive Program

- Any organization can meet the basic criteria for a comprehensive program because the expectations (“what”) do not prescribe specific means to achieve the results (“how”)
- For large, complex enterprises, the solutions may be sophisticated and costly (based on the nature of the organization and their business models)
- For small organizations, the solutions may be very simple and inexpensive
- The most important factor is that the organization considers the risks they may create and has the appropriate components to manage and demonstrate capacity proportional to their business environment

End