Embed Privacy and Security Culture Within Your Organization

Drive employee engagement with privacy and security via governance and process integration.

INFO~TECH RESEARCH GROUP

Table of Contents

Embed Privacy and Security Culture Within Your Organization

Drive employee engagement with privacy and security via governance and process integration.

EXECUTIVE BRIEF

Analyst Perspective

Engagement means more than just completed training modules.

Privacy and security are two heavy-hitting items that all organizations, regardless of size, location, or industry, are considering with extreme care. The media is regularly peppered with stories of large-scale breaches, ransomware attacks, and incidences of insider threats that wreak havoc on organizations' internal operations, external perspectives and customer bases, and overall brand reputations.

And while a robust information security program and controls, coupled with a strong privacy program and framework, are of significant value, ultimately an organization must shift to take a proactive stance on both privacy and security. This requires that principles and behaviors that promote privacy and security are embedded in the operational seams of how the organization runs on a daily basis and are supported from both the top down and bottom up. A culture of privacy and security starts with employees and members of the organization being fully engaged with how these two disciplines promote their own success and the overall performance of the organization.

Logan Rohde
Research Analyst, Security, Privacy, Risk & Compliance
Info-Tech Research Group

Alan Tang
Principal Research Director, Security, Privacy, Risk & Compliance
Info-Tech Research Group

Executive Summary

Your Challenge

Engagement with privacy and security within organizations has not kept pace with the increasing demands from regulations. As a result, organizations often find themselves saying they support privacy and security engagement but struggling to create behavioral changes in their staff.

However, with new privacy and security requirements proliferating globally, we can't help but wonder how much longer we can carry on with this approach.

Common Obstacles

Driving engagement with privacy and security within organizations is a challenge because:

- Organizations struggle to differentiate between security and privacy.
- Leadership teams see privacy and security as something that's handled elsewhere.
- Organizations don't know how to measure engagement with security and privacy.

Privacy and security are often viewed as costs and inhibitors of innovation as opposed to competitive advantages.

Info-Tech's Approach

Follow Info-Tech's approach to ensure privacy and security are part of your organization's process governance and are accounted for at all relevant points. Specifically, this blueprint will help you to:

- Develop a defined structure for privacy and security in the context of your organization.
- Align your business goals and your security and privacy strategy to obtain support from your senior leadership team.
- Measure adherence to requirements using metrics.

Info-Tech Insight

To truly take hold, privacy and security engagement must be supported by senior leadership, aligned with business objectives, and embedded within each of the organization's operating groups and teams.

Your challenge

This research is designed to help organizations who are looking to:

- Build a culture of security and privacy within the organization.
- Leverage their privacy program as a competitive advantage.
- Ensure that their security standards go above and beyond what's expected for the industry.
- Obtain support from executives and senior leadership to change employee behaviours to create a more privacy-informed and security-aware organization.

Privacy and security, while two separate functions, are inextricably linked. An organization that puts privacy first must also employ the necessary security controls and processes to protect the organization, its assets, and the information it processes.

"I want to see comprehensive data program[s] as the norm, organizations better protecting the data of citizens and consumers and a change of culture that makes broader and deeper data protection accountability a focus for organizations..."

– Elizabeth Denham, UK's Information Commissioner

Source: ICO

$1.00 Company's spend on privacy

=

$2.70 Company's average return on privacy

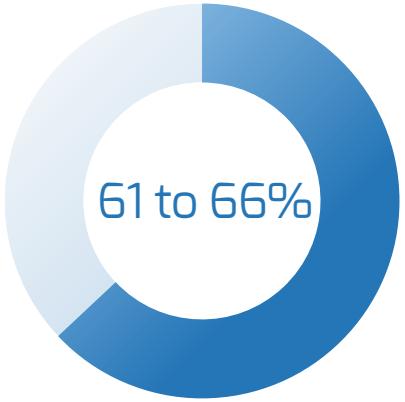
Source: CPO Magazine

Common obstacles

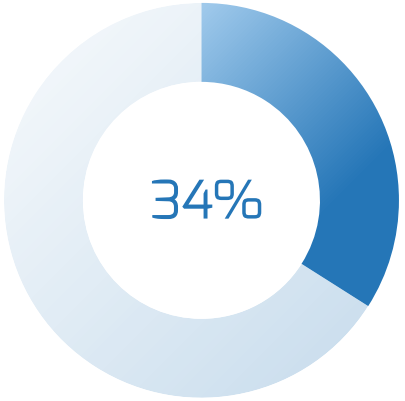
These barriers make this challenge difficult to address for many organizations:

- While business and IT leaders alike understand the importance of a robust cybersecurity program, the significance of a separate but related privacy program is not as readily recognized.
- Privacy is often viewed as an inhibitor of innovation and a compliance obligation box to be ticked as opposed to a competitive advantage and differentiator.
- Training modules, tests, and continuous learning are integral parts of ensuring that privacy and security are embedded in the organization, but they are just the beginning. Unfortunately, IT and business leaders consider them to be the core of a privacy- and security-centric culture.
- Identifying indicators by which to measure an organization's employee engagement with privacy and security is challenging at the best of times.

Employees aren't fully engaged with how privacy and security impact them



of surveyed employees are unsure of whether or not the GDPR, CCPA, PCI DSS, and FERPA apply to their organization.

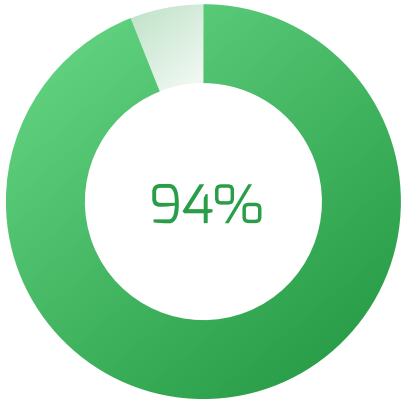


of employees that are considered **privileged users** do not believe that it is part of their duty to take additional security safeguards around corporate systems.

Source: MediaPRO

A custom culture of privacy and security is worth the investment

Right-size privacy and security engagement to meet the needs of your organization and drive business growth.

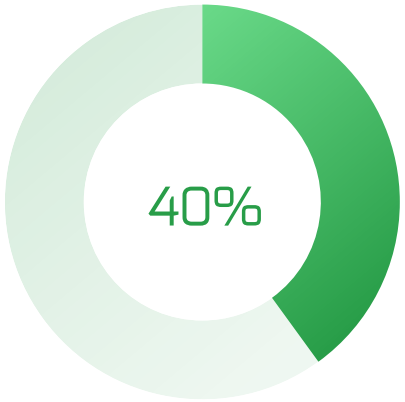


of organizations believe that security culture is integral, yet there is little agreement on what defines a security culture.

Source: KnowBe4

of companies that have invested time, effort, and money in privacy have experienced benefits of at least double the initiative investment.

Source: "From Privacy to Profit," Cisco, 2019



"At Uber, we are trying to change our employees' security stories. By creating programs catered to region, department, and role, our people understand that security is part of their story and our culture."

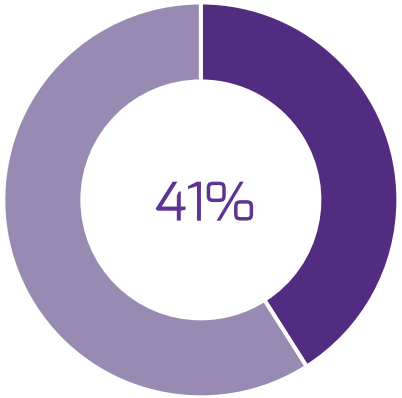
– Samantha Davison, Uber Security Program Manager (in TechBeacon)

Info-Tech Insight

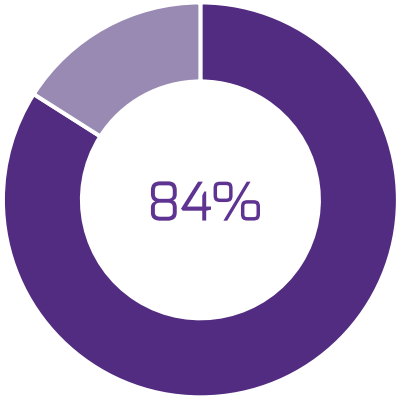
A privacy- and security-centric culture relies on employees understanding and engaging with these disciplines. They must be able to contextualize how privacy and security apply to their roles and responsibilities.

Information security: An overview

A perspective on the global information security landscape



of individuals do not believe that companies care about or take measures toward securing their personal data.[1]



of these same individuals say that they are more likely to remain loyal to companies with strong security controls in place.[1]

207 days

is the average time it took to identify a data breach in 2020, and 73 days is the average time to contain the breach.[2]

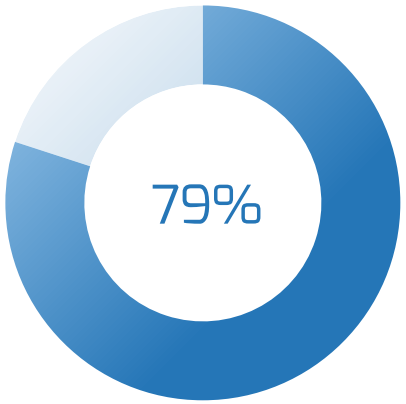
39 seconds

On average, a hacker attack occurs every 39 seconds.

Sources:
[1] Salesforce
[2] IBM and Ponemon Institute
[3] A. James Clark School of Engineering, University of Maryland

Privacy compliance: An overview

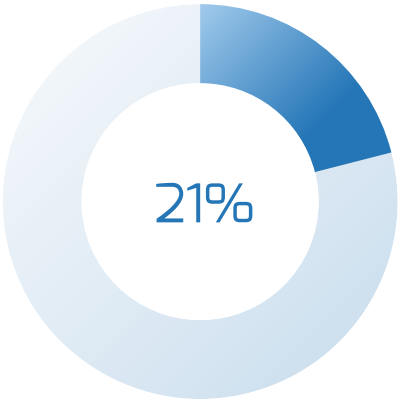
A perspective on the global privacy and compliance landscape



of individuals state that they are very or somewhat concerned about how companies are using the data they collect about them.[1]

128 countries

have established data protection or data privacy laws. Only 19% of countries have no data protection laws in place.[2]



of individuals believe that companies, not governments or users, are responsible for maintaining data privacy.[3]

Info-Tech Insight

Effective privacy and compliance help drive consumer confidence. Good data privacy practices can give you a competitive advantage through transparency.

Sources:
[1] Pew Research Center
[2] United Nations Conference on Trade and Development
[3] "Consumer Privacy Survey 2019," Cisco, 2019

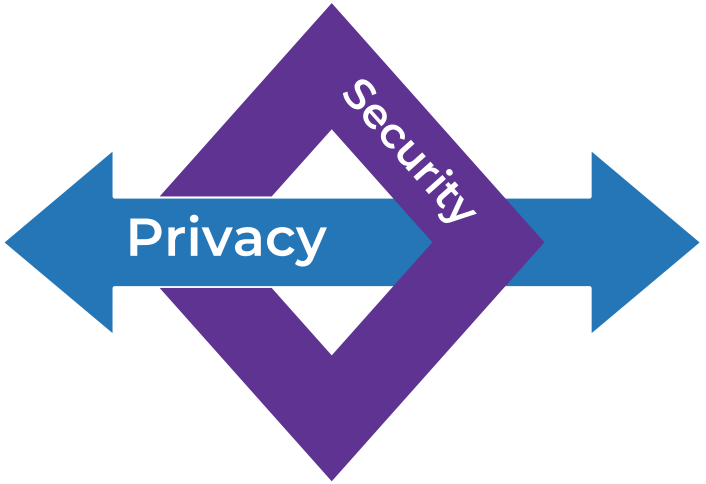
Delineating privacy vs. security

A common assumption is that security and privacy are one and the same.

Security's role is to protect and secure assets, of which confidential data – especially personal data – is a large focus. The consequences of a personal data breach can be severe, including potential regulatory consequences and the loss of customer trust. As a result, we often think of how we use security to protect data.

But security is not equivalent to privacy.

Privacy must be thought of as a separate function. While privacy will always have ties to security in the ways security protects data, privacy starts and ends with the focus on **personal data**. Beyond protection, privacy extends to understanding why personal data is being collected, what the lawful uses are, how long it can be retained, and who has access to it.



Evaluate the intersection of data privacy and information security

Security

Information security aims to ensure **confidentiality, availability, and integrity** of information throughout the data's lifecycle.[1] Common functions of information security include:

- Risk management
- Vulnerability management
- Identity and access management
- Strategy and governance
- Data protection
- Incident response

Privacy

Data privacy ensures that the rights of individuals are upheld with respect to **control over how their information is collected, used, and processed**. Data privacy emphasizes the following principles:

- Lawfulness, fairness, and transparency
- Integrity and confidentiality
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Accountability

Source: "Privacy Program Management," IAPP, 2019

Building a privacy culture

Ancestry aimed its privacy culture at helping its employees to better serve customers

SOURCE
Case Study Interview

Challenge

Given that Ancestry relies on collecting, processing, and analyzing sensitive personal data to provide its services to customers, Ancestry's privacy office sought to ensure that privacy was embedded within the organization's operations.

The chief privacy officer (CPO) and his team were tasked with ensuring that the company's employees understood the intricacies of privacy laws and had the tools to rely on to guide their daily tasks and responsibilities.

Solution

The privacy office developed a layered training program with training modules and vendor-supported testing, including mini-courses focused on important compliance topics.

To support this, they created a privacy dashboard to track specific metrics (e.g. privacy video views, number of cookie opt-outs by users), and they monitored proposed changes to privacy legislation to ensure staff were up to date.

The company also created a Privacy Champions council that included three tiers (Bronze, Silver, Gold), and to earn membership employees had to complete extra tasks based on the tier level, such as courses, assessments, and writing and presenting an essay on a specific privacy topic.

Results

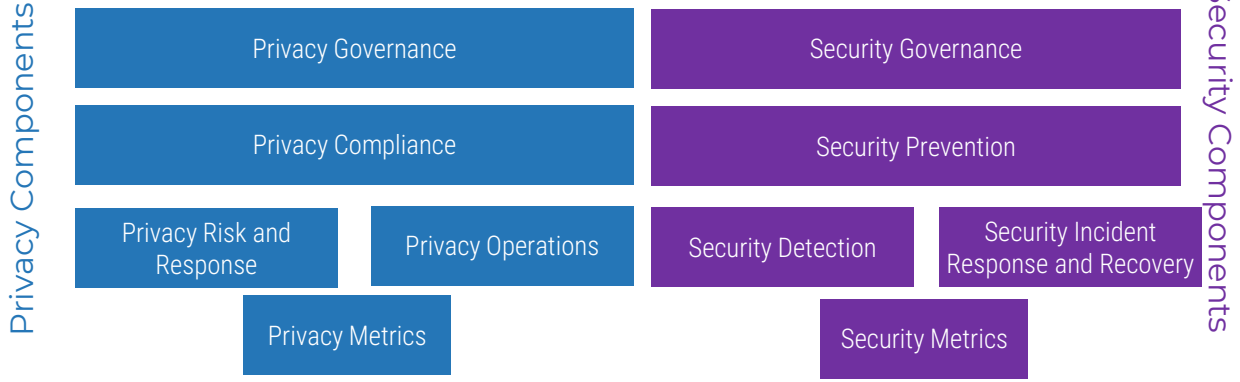
The end objective for Ancestry's privacy office was to foster a culture of privacy to further business processes rather than oppose them, which was accomplished by integrating privacy into Ancestry's value proposition, making it an integral part of customer relations.

Encouraging employees to see the role they play in protecting customer privacy has helped the privacy office to develop and maintain Ancestry's privacy culture, using the privacy dashboard to track progress and monitor any regression.

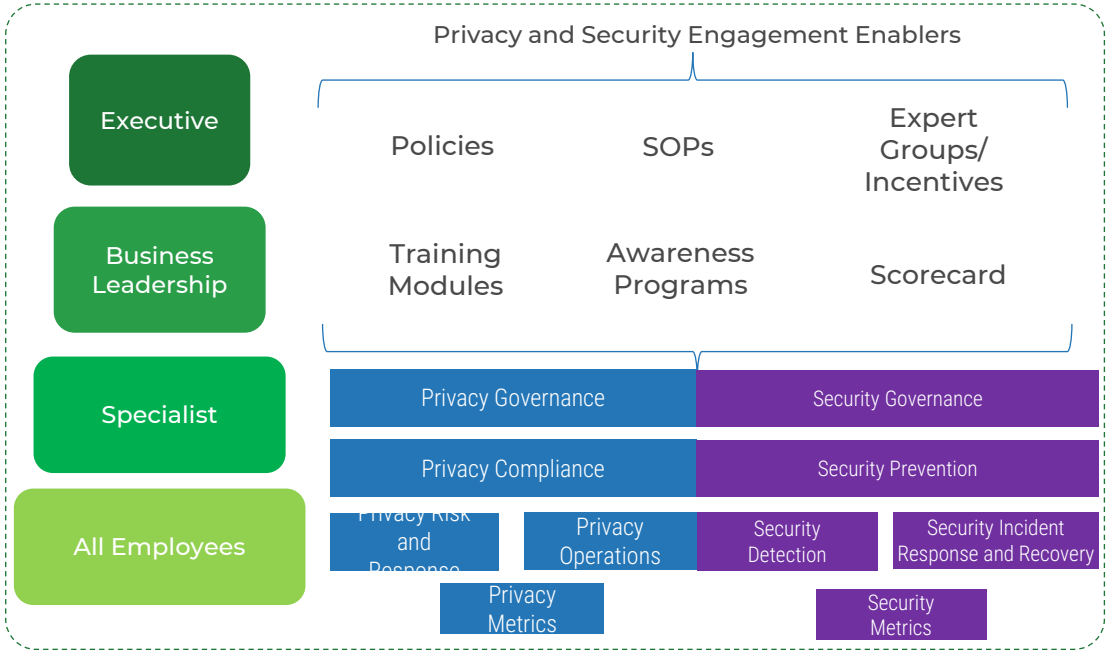
Info-Tech's approach

1 Identify Drivers for Your Organization's Operating Environment

2 Map to Info-Tech's Ten Pillars of Privacy and Security



3 Identify Enablers That Support Your Privacy and Security Program and Align to Your Org Structure



4 Customize Your Privacy and Security Organizational Engagement Model

	Policies	SOPs	Expert Groups/ Incentives	Training Modules	Awareness Programs	Scorecard
Executive	Enterprise-wide policies		Owner/ sponsor		Executive awareness	Executive scorecard
Business Leadership	Business-related policies	Business-related SOPs	Champions	Business-related training	Business awareness	Business leadership scorecard
Specialist	Security and privacy mgmt. policies	Security and privacy mgmt. SOPs	Core team	Profession-related training		
All Employees	Daily job-related policy		Incentive program		Employee awareness	

Info-Tech's methodology to Embed Privacy and Security Culture Within Your Organization

	1. Define Privacy and Security in the Context of the Organization	2. Map Your Privacy and Security Enablers	3. Identify and Track Your Engagement Indicators
Phase Steps	1. Identify privacy and compliance objectives. 2. Identify security objectives.	1. Align your organizational structure. 2. Review privacy and security enablers. 3. Match employee attributes and behaviors.	1. Develop process for monitoring and continuous improvement.
Phase Outcomes	• Understanding of the distinct characteristics of privacy and security practices as well as the linked dependencies. • Customized perspective on what privacy and security mean in the context of the organization's operating environment and strategy.	• Mapping between privacy and security objectives and business objectives/strategy. • Employee behavioral attributes that support a culture of privacy and security • Executive team support for privacy and security engagement program.	• Key performance indicators and metrics that help measure ongoing levels of employees' privacy and security engagement.

Culture develops via business engagement

Engagement starts at the top

Privacy and security engagement must be supported by senior leadership, aligned with your business objectives, and applied within each of the operating groups and teams in the organization.

Different but linked

Privacy and security are two separate disciplines, today's organizations must address them as such. They are, however, inextricably linked: An effective privacy program will need to be supported by strong cybersecurity governance.

Engage the business, engage the staff

Buy-in from the top for both privacy and security is a lot easier if you can directly link the impact of employees' privacy and security engagement to business objectives. A business-aligned privacy and security program ensures executive and employee support.

Measure your progress

Once you've identified how privacy and security support the business and which attributes your employees will take up, develop metrics based on your initiatives to promote continuous improvement.

Do not disregard risk

You must consider risk when determining which privacy and security objectives to focus on. In particular, assess risk associated with employee behaviors as you build your engagement plan.

Customize to optimize

A one-size-fits-all approach to privacy and security won't work: Engagement requires relevant training and awareness for each department or business group within the organization.

Key deliverable:

Privacy and Security Engagement Playbook

This document maps out the organization's continued efforts to ensure employees are engaged with privacy and security principles and to promote a strong culture of privacy and security.

Blueprint deliverables

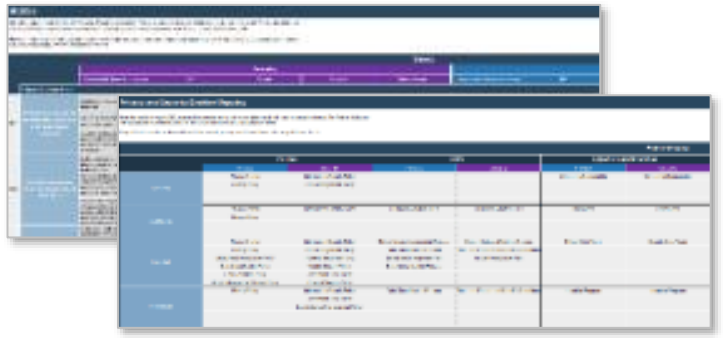
Each step of this blueprint is accompanied by supporting deliverables to help you accomplish your goals:

Privacy and Security Engagement Charter

Use this charter template to document the primary outcomes and objectives for the privacy and security engagement program within the organization.

Privacy and Security Business Alignment Tool

This tool maps business objectives and key strategic goals to privacy and security objectives and attributes identified as a part of the overall engagement program.



Blueprint benefits

IT Benefits

- Executive buy-in for the importance of privacy awareness among employees.
- Executive support for security and privacy as the default setting for business operations.
- A privacy and security employee engagement roadmap that aligns core privacy requirements and security targets and objectives with the organization's business objectives and strategy.
- Privacy and security indicators to help track overall employee engagement.

Business Benefits

- An organization that applies privacy and security as the default setting in how it operates.
- A privacy and security employee engagement roadmap that aligns with the organization's business objectives and strategy and supports each business group or division within the organization.
- Metrics and indicators to help determine whether or not employees are engaged with and embodying privacy and security attributes in their daily roles.

Measure the value of this blueprint

While it's not easy to put a dollar value on culture, understanding the impact of poor privacy and security practices is plain and simple.

- The ultimate objective of your privacy and security programs is to mitigate risk and avoid exposing the organization to damaging incidents, breaches, attacks, or violations and fines.
- In engaging your employees with the pillars of privacy and security, you foster an environment that sets both privacy and security as the default, not as an afterthought that may be forgotten.

In phase two of this blueprint, we will help you select privacy and security enablers to drive engagement.

In phase three, we will help you select a set of specific metrics catered to understanding the privacy and security performance of the organization.

3.1.1 Select privacy and security engagement metrics

1-2 hours

For each of the identified Primary Business Goals, Secondary Business Goals, and supporting Privacy and Security Initiatives, there should be a corresponding metric or set of metrics to demonstrate the overall progress of the Engagement program.

1. Document each of your goals on the whiteboard and discuss as a group what would indicate that progress is being made towards those goals (i.e. completing the initiatives that support them).
   - In many cases, your initiatives will focus on implementing something presently absent. In these cases, using a % complete metric is perfectly acceptable. (see examples on slides 72-73.
   - As you mature, however, initiatives will likely focus on improvement by setting targets that you want to meet. In these cases, % of cases within/outside target often work well.
   - Try to frame all of your metrics in terms of %, which helps to give context when reporting. In order to calculate these, you will likely need to draw from a few technical measures of some kind (e.g. number of incidents, mean time to respond).
2. Review the metrics assigned to each Goal. Select a maximum of 2-3 metrics per Business Goal, and document in slides 15-19 of the *Privacy and Security Engagement Playbook*, as well as tab 5 of the *Privacy and Security Business Alignment Tool*.

Input	Output
• Outputs from Phase 2 • Privacy and Security Engagement Charter • Completed Privacy and Security Business Alignment tool	• Privacy and security engagement metrics mapped to business goals
Materials	**Participants**
• Laptop • Markers • Whiteboard • Privacy and Security Engagement Playbook	• CISO/InfoSec lead • InfoSec managers and team • Privacy Officer/Privacy Program Manager • Compliance Manager/lead

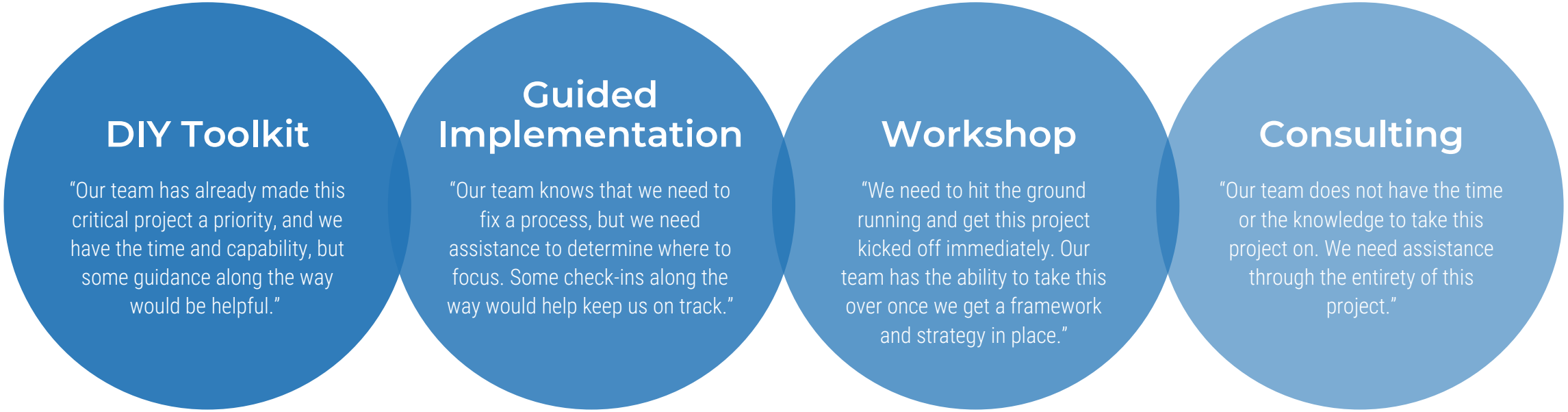
Download Info-Tech's *Privacy and Security Engagement Playbook*

Info-Tech Project Value

$165,000[1]	Average annual salary of a Principal Management Consultant
150 hours (initial)	Average total time/cost to complete all activities and deliverables in Phases 1 to 3 of this research product
=	
$ 11,900	Internal project cost
$3.36[3] million	Average total cost of a data breach, including compliance fines
27.7%[3] chance of a data breach	Likelihood of a data breach occurring
=	
$ 942,620	Total dollars saved

Sources: PayScale, IBM and Ponemon Institute

Info-Tech offers various levels of support to best suit your needs



Diagnostics and consistent frameworks are used throughout all four options.

Guided Implementation

What does a typical GI on this topic look like?

Call #1: Scope requirements, objectives, and your specific challenges.

Call #2: Align business goals and strategic objectives with privacy and security.

Call #3: Align business goals and strategic objectives with privacy and security, continued.

Call #4: Identify privacy and security behaviors for each business group.

Call #5: Identify and select your privacy and security engagement metrics and reporting structure.

Call #6: Establish your metric owners, reporting procedures, and cadence.

A Guided Implementation (GI) is a series of calls with an Info-Tech analyst to help implement our best practices in your organization.

A typical GI is between 4 to 6 calls over the course of 3 to 6 months.

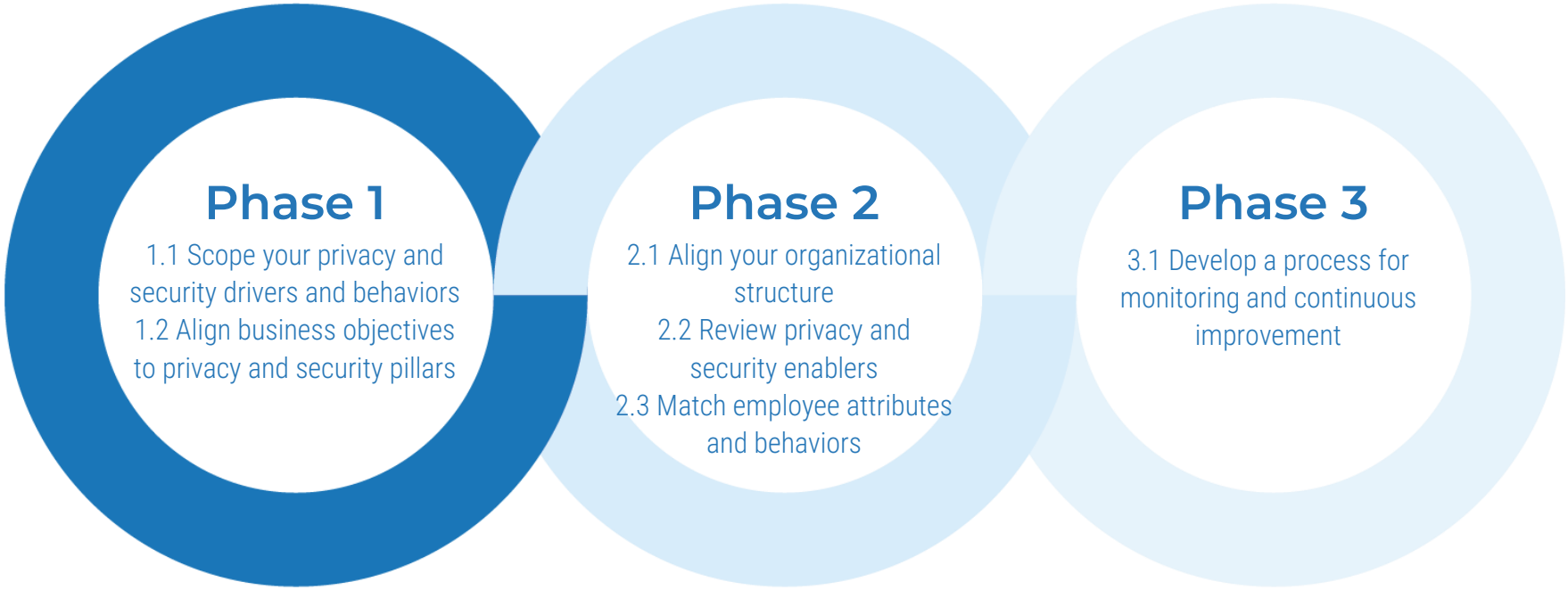
Workshop Overview

Contact your account representative for more information.
workshops@infotech.com 1-888-670-8889

	Day 1	Day 2	Day 3	Day 4	Day 5
Activities	**Determine drivers and engagement objectives** 1.1 Discuss key drivers for a privacy and security engagement program. 1.2 Identify privacy requirements and objectives. 1.3. Identify security requirements and objectives. 1.4 Review the business context.	**Align privacy and security with the business** 2.1 Review the IT/InfoSec strategy with IT and the InfoSec team and map to business objectives. 2.2 Review the privacy program and privacy strategic direction with the Privacy/Legal/Compliance team and map to business objectives. 2.3 Define the four organizational groupings and map to the organization's structure.	**Map privacy and security enablers to organizational groups** 3.1 Define the privacy enablers. 3.2 Define the security enablers. 3.3 Map the privacy and security enablers to organizational structure. 3.4 Revise and complete *Privacy and Security Alignment Tool* inputs.	**Develop privacy and security engagement metrics** 4.1 Segment KPIs and metrics based on categories or business, technical, and behavioral. 4.2 Select KPIs and metrics for tracking privacy and security engagement. 4.3 Assign ownership over KPI and metric tracking and monitoring. 4.4 Determine reporting cadence and monitoring.	**Next Steps and Wrap-Up (offsite)** 5.1 Complete in-progress deliverables from previous four days. 5.2 Set up review time for workshop deliverables and to discuss next steps.
Deliverables	1. Privacy and compliance drivers and obligations 2. Security drivers and obligations 3. Privacy and security engagement program objectives	1. Privacy and security objectives mapped to business strategic goals 2. Framework for privacy and security engagement program 3. Initial mapping assessment within the *Privacy and Security Alignment Tool*	1. Completed *Privacy and Security Alignment Tool* 2. Completed *Privacy and Security Engagement Charter*	1. Metrics identified at a business, technical, and behavioral level for employees for continued growth 2. Completed *Privacy and Security Engagement Playbook*	1. Recommendations for future growth of privacy and security engagement plan.

Phase 1

Define Privacy and Security in the Context of the Organization



Embed Privacy and Security Culture Within Your Organization

This phase will walk you through the following activities:

- Scope your privacy and security drivers and behaviors.
- Align business objectives to privacy and security pillars.

This phase involves the following participants:

- Executive team/senior leadership team
- CIO
- Chief information security officer (CISO)
- HR lead/VP of HR
- InfoSec lead
- IT lead
- InfoSec team
- IT team
- Privacy and Compliance team
- Internal Audit

Step 1.1

Scope Your Privacy and Security Drivers and Behaviors

Activities

1.1.1 Identify Privacy and Compliance Drivers and Behaviors

1.1.2 Identify Security Drivers

Define Privacy and Security in the Context of the Organization

This step involves the following participants:

- CISO/InfoSec lead
- InfoSec managers and team
- IT team
- Privacy officer/privacy program manager
- Compliance manager/lead
- Internal Audit

Outcomes of this step

Determine program needs.

Put data privacy principles into action

1 Lawfulness, Fairness, and Transparency

Do our employees understand the regulations that we are subject to and the reasons we process data?

2 Purpose Limitation

Is our team fully aware of the purposes for which data is processed and the importance of using the data only for these purposes?

3 Data Minimization

Is it a reflex for employees collecting and processing data to only collect and process what is necessary and nothing more?

4 Accuracy

Do we have the right controls around entering and rectifying data to ensure accuracy?

5 Storage Limitation

Do we promote retaining data for only as long as necessary and ensuring the processes are in place to validate this?

6 Integrity and Confidentiality

Do we promote a working environment where employees understand the importance of keeping data protected and private and of processing it with care?

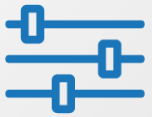
7 Accountability

Do we implement a holistic risk-based privacy program? Are we able to demonstrate compliance with relevant privacy laws and regulations?

Steps to build privacy engagement

Understand the privacy requirements and objectives of your privacy program.

Align these requirements and objectives with your core business goals and obtain senior leadership's support.



Identify your privacy enablers and map them to the privacy pillars and the different roles in the organization.

Pilot the privacy engagement program.

Privacy by design is no longer a nice-to-have

Apply the key principles behind privacy by design to embed privacy in the operations of the organization, creating a culture of *privacy first*.

Get a head start on integrating data protection into the foundations of your projects and processes with Info-Tech's *Demonstrate Data Protection by Design for IT Systems* research.

Download *Demonstrate Data Protection by Design for IT Systems*

1. **Proactive, not reactive; preventative, not remedial.**
2. **Privacy as the default setting.**
3. **Privacy embedded into design.**
4. **Full functionality; positive-sum, not zero-sum.**
5. **End-to-end security; full lifecycle protection.**
6. **Visibility and transparency; keep it open.**
7. **Respect for user privacy; keep it user-centric.**

Source: Privacy by Design, The 7 Foundational Principles, IPC

Review data privacy and protection regulations

The proliferation of data privacy laws globally creates more complexity for organizations looking to establish data security best practices.

GDPR

General Data Protection Regulation – 2018. European data protection regulation that includes specific provisions about how the personal data of EU citizens must be handled and protected.

PIPEDA (CPPA)

Personal Information Protection and Electronic Documents Act – 2004. Canadian private sector regulation that outlines the protection and safe handling standards for electronic documents. This will likely be replaced soon by the newly introduced Consumer Privacy Protection Act.

CPRA (CCPA)

California Privacy Rights Act – 2020. A recently modified privacy act (November 2020) that adds measures and definitions around sensitive data, new requirements for data processing, and the establishment of the California Privacy Protection Agency.

LGPD

Lei Geral de Proteção de Dados Pessoais – 2020. Brazil's personal data protection regulation that attempts to unify the nation's 40 additional statutes that outline personal data protection standards.

Review industry-specific regulations and standards for data privacy and security

Beyond national or federal governing privacy regulations, many organizations will also be subject to industry standards or laws that dictate minimum data security obligations.

PCI DSS

Payment Card Industry Data Security Standard – 2004. Industry standard, grouped into six control objective groups, that ensures safeguarding of cardholder data through stringent information security controls.

HIPAA

Health Insurance Portability and Accountability Act – 1996. American legislation that outlines a set of five main privacy and security provisions for healthcare organizations in an effort to protect medical information.

FISMA

Federal Information Security Management Act – 2002. Government-mandated framework that aims to protect the integrity of government information, data, and assets and that requires an annual review to maintain compliance.

GLBA

Gramm-Leach-Bliley Act – 1999. Information privacy act applied to the US financial services sector. The Act's three sections outline requirements for safeguarding collection and disclosure of consumer financial information.

Review industry-specific regulations and standards for data privacy and security

Business-to-business organizations: When reviewing the list of industry standards and frameworks, compare the controls listed by your organization's industry and the industries of your clients.

FERPA

Family Educational Rights and Privacy Act – 1994. American federal law that governs the protection and access of student education records. The law applies to any educational institution that benefits from funding through the US Department of Education.

23 NYCRR 500

New York State Department of Financial Services – 2017. Governing law applicable to financial institutions within the state of New York that outlines the implementation of a consumer data privacy framework.

CJIS

Criminal Justice Information Services – 1992. Division of the FBI with established policies and controls for wireless networking, remote access, data encryption, and MFA. CJIS' objective is to ensure safeguarding of confidential data around criminal justice information.

NERC-CIP

North American Electric Reliability Corporation Critical Infrastructure Protection – 2008. A guiding set of nine standards and 45 requirements that aim to ensure security and physical protection of North American electric operations.

1.1.1 Identify privacy and compliance drivers and behaviors

45 minutes

1. Bring together relevant stakeholders in the organization with significant knowledge of compliance and other regulatory obligations.
2. Using sticky notes, have each stakeholder write one key concern or question about compliance. The idea here is to start the conversation so that the group can begin to grasp how these various drivers interact, which will help you to strategize solutions later.
3. Group all sticky notes that address similar themes to create categories of drivers and behaviors, such as:
    - Access control and management
    - Data lifecycle (deletion, archiving, retention periods)
    - Disclosure and open access of data

    Be sure to discuss with the group what is being put on the list and clarify any unusual or unclear obligations.

↓ Download Info-Tech's *Privacy and Security Engagement Charter*

Input

- (Optional) Stakeholders involved can prepare a list of current compliance obligations
- Printed or digital document of all relevant compliance and industry standards or frameworks

Output

- Collective understanding of key compliance concerns and drivers within the organization
- Employee behaviors mapped to privacy concerns and drivers

Materials

- Laptop
- Sticky notes
- Markers
- *Privacy and Security Engagement Charter*

Participants

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead
- Internal Audit
- IT team (optional)

1.1.1 Identify privacy and compliance drivers and behaviors (cont'd)

4. Once you have grouped all your notes into representative categories, document them in the *Organizational Privacy Drivers* section in Info-Tech's *Privacy and Security Engagement Charter* template.
5. For each sticky note, name two or three employee behaviors that support efforts toward addressing the privacy/compliance concern in question. These can be behaviors that are currently exhibited or hypothetical. Document and keep for future activities.
6. Repeat step 5, but this time focus on employee behaviors that detract from efforts to address the privacy/compliance concern.

E.g. *Concern 1: Data retention requirements for employee records.*

+ Positive behaviors: HR staff use the Records Retention Schedule and Data Retention Policy and classify/store records accordingly, including classification label.

- Negative behaviors: Staff do not differentiate between documents and records in terms of storage location and neglect to include classification label.

Input

- (Optional) Stakeholders involved can prepare a list of current compliance obligations
- Printed or digital document of all relevant compliance and industry standards or frameworks

Output

- Collective understanding of key compliance concerns and drivers within the organization
- Employee behaviors mapped to privacy concerns and drivers

Materials

- Laptop
- Sticky notes
- Markers
- *Privacy and Security Engagement Charter*

Participants

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead
- Internal Audit
- IT team (optional)

The importance of security engagement

The role of security awareness and training in protecting an organization's operations has become increasingly important with the exponential growth in malicious attack vectors as well as the growing complexity of the technological environment.

Defining a security culture

The CIA triad is a staple of information security.

Confidentiality: "The prevention of unauthorized disclosure of information."

Integrity: "Ensures that information, systems, applications, and resources are protected from unauthorized or unintentional alternation, modification, or deletion."

Availability: "Information, systems, applications, and resources are accessible and experience minimal downtime."

Source: "Privacy Program Management," IAPP, 2019

Put information principles into action

1 Confidentiality

While this information security principal is similar to one of the data privacy principles, it should be applied beyond personal data or personally identifiable information (PII) to all the organization's proprietary data (intellectual property, trade secrets, etc.). Are our employees equipped with the knowledge and skills to maintain confidentiality to protect business operations?

2 Integrity

Does our organization educate employees on the importance of keeping our information systems, assets, and overall operating environment safe from external malicious attacks as well as intentional or unintentional inside threats? Is this integrity of operations a core pillar of how our employees do their daily jobs?

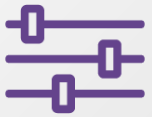
3 Availability

Is the reliability and availability of the IT infrastructure a key concern for our team and staff? Are they provided with the tools they need to ensure information systems, assets, and any other core pillars experience minimal disruption and downtime?

Steps to build security engagement

Understand both the technical and process-based requirements and objectives of your information security program.

Align these requirements and objectives with your core business goals and obtain senior leadership's support.



Identify your security enablers and map them to the security pillars and the different roles in the organization.

Pilot the security engagement program.

Align with information security frameworks

Know the role of best-practice frameworks and compliance frameworks in data security best practices.

NIST Cybersecurity Framework

The National Institute of Standards and Technology's framework with five key sections, each of which contains supporting controls that assist organizations in managing cyber risk.

NIST SP 800-53

Special Publication edition that details a set of security and privacy controls mapped to the NIST framework over 19 different control families.

CIS CSC

Center for Information Security's publication that provides a set of 20 top actionable controls for cybersecurity, which are leveraged globally as safeguards against cyberattacks.

ISO/IEC 27001:2013

Updated version of ISO/IEC 27001, which outlines the specific actions and steps for implementation and maintenance of an information security management system.

COBIT-5

ISACA's Control Objectives for Information and Related Technology, a framework that is based on five key principles and consists of four key domains and processes.

1.1.2 Identify security drivers and behaviors

45 minutes

1. Bring together the same group of stakeholders from Activity 1.1.1 and include any additional members from your InfoSec and IT teams.
2. Using sticky notes, have each stakeholder write one key concern or question about current security practices in the organization. These can be informed by past events, industry-specific concerns, or anticipated changes in the infrastructure or operating environment.
3. Collect these and group together similar themes as they arise. Themes may include:
    - Phishing attempts/malware
    - Network safety best practices
    - Responding to incidents
4. Discuss with the group what is being put on the list and clarify any unusual or unclear security concerns.
5. Review and document in the *Organizational Security Drivers* section of the *Privacy and Security Engagement Charter* template.

↓ Download Info-Tech's *Privacy and Security Engagement Charter*

Input

- (Optional) Printed or digital document of all relevant security frameworks and/or industry standards or frameworks

Output

- Collective understanding of key security program concerns and drivers within the organization
- Employee behaviors mapped to security concerns and drivers

Materials

- Laptop
- Sticky notes
- Markers
- *Privacy and Security Engagement Charter*

Participants

- CISO/InfoSec lead
- InfoSec managers and team
- IT team
- Privacy officer/privacy program manager
- Compliance manager/lead
- Internal Audit

1.1.2 Identify security drivers and behaviors (cont'd)

6. For each sticky note, name two or three employee behaviors that support efforts toward addressing the security concern. These can be employee behaviors that are currently exhibited or hypothetical. Document and keep for future activities.
7. Repeat step 6, but this time focus on employee behaviors that detract from efforts to address the security concern

E.g. *Concern 1: Malware injected into operating environment due to employee error.*

+ Positive Behaviors: Non-IT and IT staff are frequently marking and reporting suspicious emails to Service Desk using appropriate protocol (screenshot vs. forwarding onward).

- Negative Behaviors: Staff do not inform Service Desk of suspicious email attempts even if they do not click through. They simply move them to another folder and ignore.

Input

- (Optional) Printed or digital document of all relevant security frameworks and/or industry standards or frameworks

Output

- Collective understanding of key security program concerns and drivers within the organization
- Employee behaviors mapped to security concerns and drivers

Materials

- Laptop
- Sticky notes
- Markers
- *Privacy and Security Engagement Charter*

Participants

- CISO/InfoSec lead
- InfoSec managers and team
- IT team
- Privacy officer/privacy program manager
- Compliance manager/lead
- Internal Audit

Step 1.2

Align Business Objectives to Privacy and Security Pillars

Activities

1.2.1 Align Business Objectives to Privacy Program

1.2.2 Finalize the Privacy and Security Engagement Charter

Define Privacy and Security in the Context of the Organization

This step involves the following participants:

- CISO/InfoSec lead
- InfoSec managers and team
- IT team
- Privacy officer/privacy program manager
- Compliance manager/lead
- Internal Audit

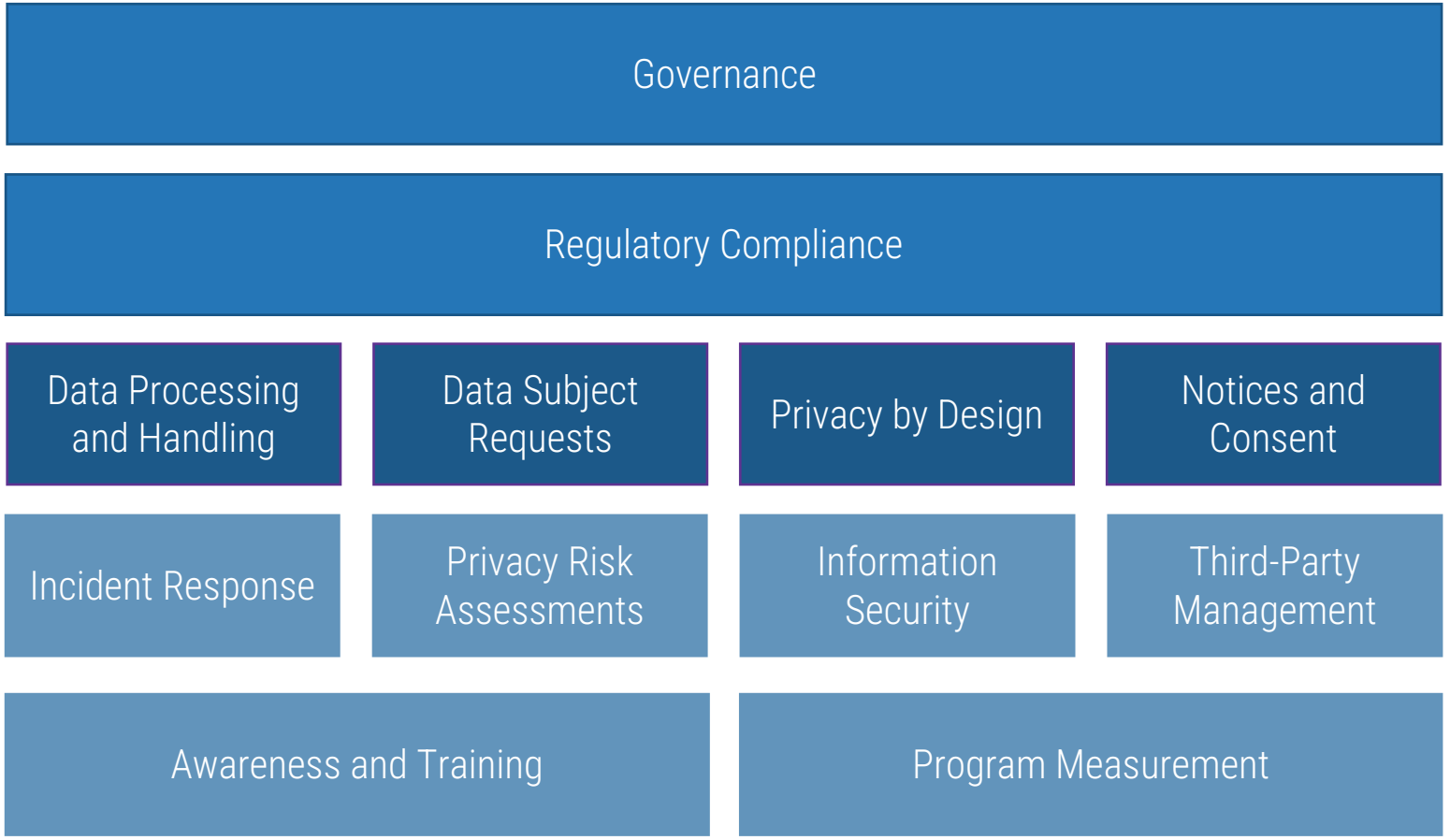
Outcomes of this step

Set of privacy and security objectives mapped to Info-Tech's Ten Pillars of Privacy and Security.

Alignment between business objectives and privacy and security objectives.

Info-Tech's Privacy Framework

Below is a visual representation of Info-Tech's Privacy Framework. This includes high-level governance items as well as more tactically defined areas.



These will be the tenets and foundations of the larger privacy program and represent the pillars of **Privacy Governance** and **Privacy Compliance.**

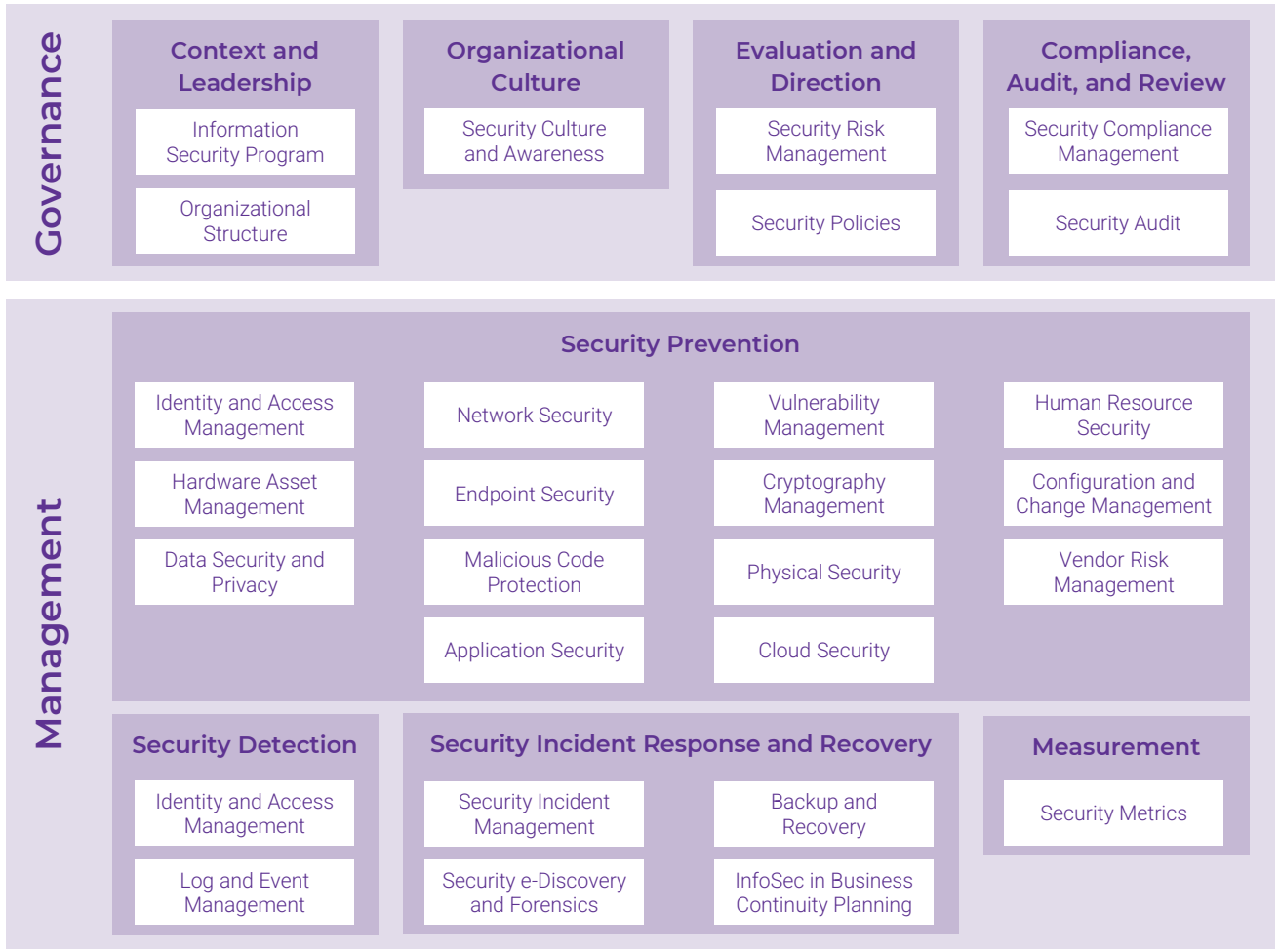
These are very tactical, operational areas and can be evaluated for the organization as a whole, or even by business unit as a part of the **Privacy Operations** pillar.

These four domains correspond to controls of **Privacy Risk Reduction** (performance of privacy impact assessments [PIAs], breach response, vendor privacy assessments, etc.).

These areas align with the **Privacy Metrics** pillar and relate to overall privacy program development.

Info-Tech's Security Framework

Below is a visual representation of Info-Tech's Security Framework. This includes high-level governance items as well as more tactically defined areas.



These domains focus on the strategic elements of building a security strategy as well as **Security Governance**.

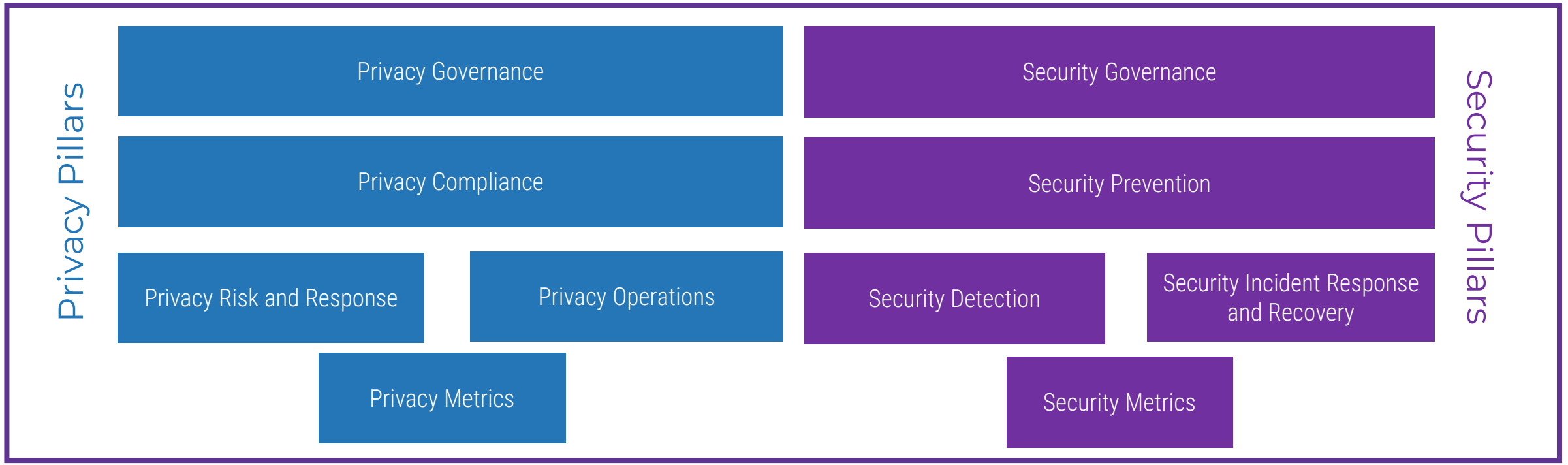
Security Prevention domains focus on each of the tactical, supporting components of an effective security program.

Security Detection and **Security Incident Response and Recovery** emphasize proactive approaches to threats and risks while Measurement/**Security Metrics** applies security metrics for continuous improvement.

Info-Tech's Ten Privacy and Security Pillars

Info-Tech's privacy and security frameworks are each composed of five pillars, which reflect their matching frameworks at a high level and will be used to help group planned or future initiatives.

Some areas may be more developed than others. As part of the next activity, we will look to discover any gaps, leaving us with a roadmap to arrive at a fully functional privacy and security engagement program.

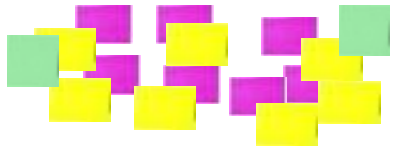


1.2.1 Align business objectives to privacy and security initiatives

45 minutes

Primary Business Objectives

Secondary Business Objectives



1. Create a list of the business objectives that intersect with security and privacy engagement and divide them into two categories: primary business objectives (blue notes) and secondary business objectives (purple notes)
2. Using yellow notes, document the organization's privacy initiatives. If no formal privacy initiatives exist, work as a team to map relevant privacy initiatives and place them within Info-Tech's five privacy pillars.
3. Map all yellow sticky notes to the blue and purple sticky notes with which they intersect. Some privacy initiatives may support multiple business objectives, so duplicate as necessary. Be as specific as possible (see examples in charter template).
    - Note: A well-developed program should have an initiative tied to each of the privacy pillars. If gaps exist, determine why and discuss possible initiatives that could be used to close them. Once complete, add these gap-closing initiatives to the charter.
4. Repeat the above steps for your security initiatives using green sticky notes to keep privacy and security initiatives separate.

Input

- Completed privacy framework or strategy

Output

- Strategic mapping of the organization's current privacy strategy/framework to the business strategy and objectives

Materials

- Laptop
- Sticky notes
- Markers/pen
- Notebook
- *Privacy and Security Engagement Charter*

Participants

- CISO/InfoSec lead
- InfoSec managers and team
- IT team
- Privacy officer/privacy program manager
- Compliance manager/lead
- Internal Audit

1.2.2 Draft the Privacy and Security Engagement Charter

45 minutes

1. Take the output from Activity 1.2.1, including alignment and mapping of both privacy and security initiatives to business objectives. For each of the primary business objectives, review all the aligned privacy and security initiatives and objectives. As a team, identify crossover or similar initiatives. Discuss whether it is possible to combine initiatives.
2. When combining initiatives, do not forget to map them to ensure each initiative can be placed within one of the security or privacy pillars.
3. Make any necessary updates to your charter.

Download Info-Tech's *Privacy and Security Engagement Charter*

Download Info-Tech's *Privacy and Security Business Alignment Tool*

Input

- Outputs from Activity 1.2.1

Output

- Completed *Privacy and Security Engagement Charter*
- Initial inputs to *Privacy and Security Business Alignment Tool*

Materials

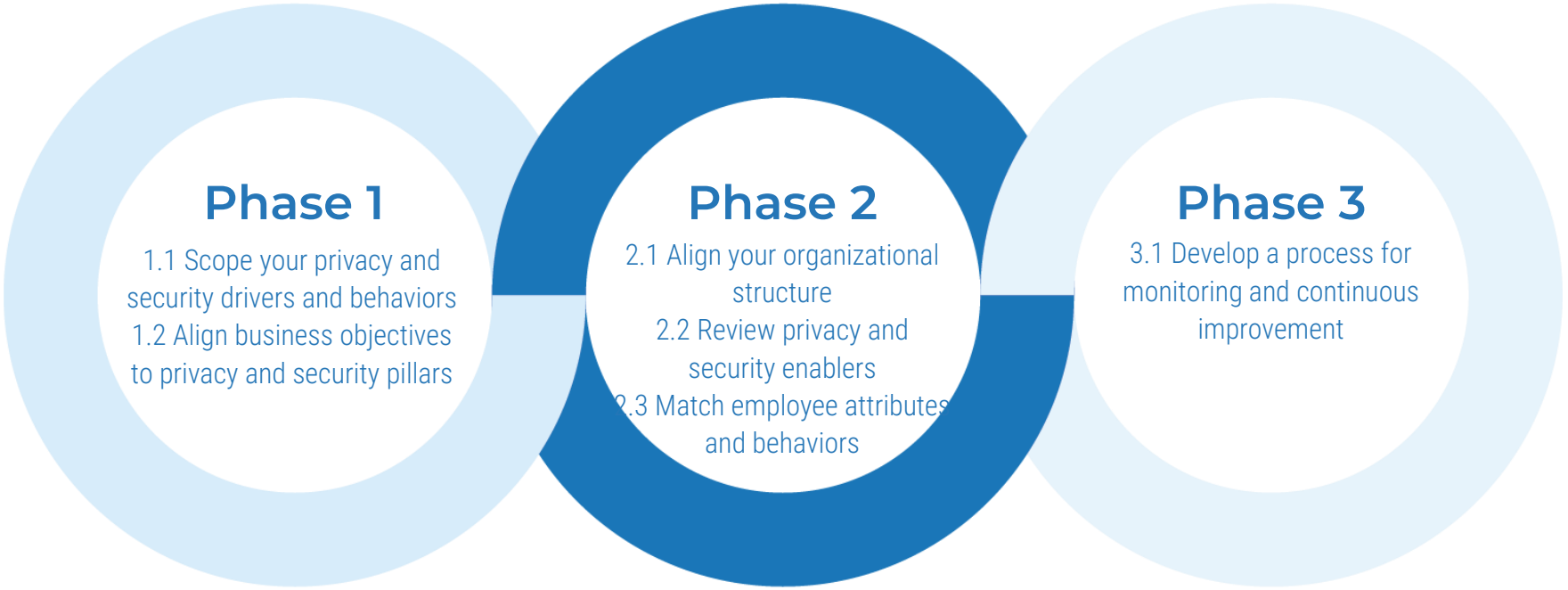
- Laptop
- Markers/pen
- Sticky notes
- Notebook
- *Privacy and Security Engagement Charter*
- *Privacy and Security Business Alignment Tool*

Participants

- CISO/InfoSec lead
- InfoSec managers and team
- IT team
- Privacy officer/privacy program manager
- Compliance manager/lead
- Internal Audit

Phase 2

Map Your Privacy and Security Enablers



Embed Privacy and Security Culture Within Your Organization

This phase will walk you through the following activities:

- Align your organizational structure.
- Review privacy and security enablers.
- Match employee attributes and behaviors.

This phase involves the following participants:

- Executive team/senior leadership team
- CIO
- CISO
- HR lead/VP of HR
- InfoSec lead
- Privacy and Compliance team

Step 2.1

Align the Organizational Structure

Activities

2.1 Align the Organizational Structure

Map Your Privacy and Security Enablers

This step involves the following participants:

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead

Outcomes of this step

Alignment between the current roles, responsibilities, and departments of your organization and Info-Tech's four-tiered organizational structure.

The role of organizational structure in privacy and security engagement

Gauging effective privacy and security will look different at each level of the organization's structure.

Your executive team will take accountability and ownership for both the positive and less-than-positive outcomes of your privacy and security performance.

This level of **accountability** will not be shared evenly across all employees of the organization, but **responsibility** still exist across all levels; it is, in fact, the key requirement for privacy and security engagement to succeed organizationally.

Executive Engagement

WHO

The Executive team contributes to discussions of risk tolerance and privacy and compliance requirements. The team also communicates business needs to the privacy, security, and IT leaders.

The Executive team should include all members of the senior leadership or C-suite within an organization and may also extend to VPs of functional groups.

WHAT

- Convey business needs to Leadership and Specialist groups.
- Work with the privacy and security teams to align business goals with privacy and security objectives.
- Maintain a functional understanding of possible security threats to make informed decisions about the organization's overall security program.
- Hold accountability through executive scorecards for the level of privacy and security engagement in the organization.
- Approve privacy and security policies.
- Communicate business obligations and goals.
- Hold the Leadership team accountable for putting the policies in place to support privacy and security engagement.

WHY

It is imperative that this team owns the privacy and security engagement program and promotes it through all supporting levels of the organization. If Executives don't buy in, the rest of the organization won't either.

Leadership Engagement

WHO

The Leadership team is the first level of translation between the executive leadership's understanding of privacy and security and how it is interpreted and upheld by the rest of the organization.

The Leadership team members span from VP to director/department-head level at an organization.

WHAT

- Review and advise on privacy and security policies prior to approval.
- Identify metrics for privacy and security operations and engagement at the department/business-group level.
- Train Specialists on privacy and security operating procedures.
- Develop the privacy roadmap and governance framework and the security strategy and governance framework.
- Write high-level summaries for Executive review describing actual or potential attacks against the organization.
- Document and present privacy and compliance obligations and reports.
- Provide summary documents of privacy and other compliance laws and regulatory changes that may impact the organization.

WHY

This is the first layer between the Executive team and the rest of the organization. This group leads efforts to ensure that the privacy and security programs and initiatives are functional and right-sized to the structure of the organization and business groups.

Specialist Engagement

WHO

The Specialist team functions as the operational tier within the organization's privacy and security engagement model.

The Specialist team members include those at a manager or senior manager level through to employees or contractors that hold specialized skilled roles in the organization.

WHAT

- Maintain and ensure execution of security operational standards and privacy and compliance standards at the respective department/business-group level.
- Assist in integrating privacy and security requirements into their respective department's/business group's operations.
- Operationalize, implement, and adapt initiatives related to privacy and security awareness and training at the department or business-group level.
- Ensure privacy and security key performance indicators (KPIs) and metrics are met within their respective team or business group.

WHY

The Specialist team is vital in adapting and implementing the initiatives, policies, and procedures at a department or business-group level. They make actionable what the Leadership and Executive groups define as strategy.

Foundations Engagement

WHO

The Foundations group is made up of everyone else. This includes all end users (employees/contractors) that provide business or support functions to the organization. Generally these are individuals without managerial duties or with limited management responsibility (no more than one or two direct reports).

WHAT

- Acknowledge yearly/semiannually/monthly changes in privacy and security policies.
- Comply with information security policies and privacy/data protection policies.
- Report known or suspected issues that may affect organizational security and infringe on privacy practices.
- Participate in training modules and awareness activities/initiatives.
- Attend training sessions, complete assignments, and participate in testing exercises designed by the CISO and data protection officer/privacy officer.

WHY

This is likely the largest part of your organization's employees and poses significant risk as an entry point for malicious attacks or user error. Promoting privacy and security awareness in this group relies on education and instilled attachment to the organization.

2.1 Assign responsibilities to organizational groups

30-45 minutes

1. Bring together key stakeholders in the privacy and security engagement program (see suggested list of participants in the table to the right).
2. List the four groupings on the whiteboard (i.e. Executive, Leadership, Specialist, Foundations). Form four small teams and assign one of these groupings to each.
3. Each team is responsible for identifying the employee groups and roles within the organization that would fall into the grouping they've been assigned. Reference slides 45 to 49 and the example text in the charter template to assist with this process.
4. Have each team present their findings and discuss them as a group. Make any necessary changes and validate each list using current job or role descriptions, if available.
5. Document in the *Roles and Responsibilities for Developing the Privacy and Security Engagement Program* section within Info-Tech's *Privacy and Security Engagement Charter* template. Complete a final review to finalize the charter.

↓ Download Info-Tech's *Privacy and Security Engagement Charter*

Input

- Understanding of the organization's structure
- (Optional) Job or role descriptions for employee groups

Output

- Organizational structure that aligns with the four tiers of Info-Tech's privacy and security engagement model
- Accountability across roles for the privacy and security engagement program

Materials

- Laptop
- Sticky notes
- Markers
- *Privacy and Security Engagement Charter*

Participants

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead

Step 2.2

Review Privacy and Security Enablers

Activities

2.2.1 Identify and Align Privacy and Security Enablers (Optional)

2.2.2 Assign Enablers to Organizational Groups

Map Your Privacy and Security Enablers

This step involves the following participants:

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead

Outcomes of this step

Alignment between the current roles, responsibilities, and departments of your organization and Info-Tech's four-tiered organizational structure.

Define and align engagement enablers

Privacy and security engagement enablers are the final missing piece in the development of the overarching program.

Policies

- Create and enforce policies around privacy (data classification, retention, protection) and security (incident response, physical security, acceptable use) to set expectations for privacy and security behaviors in the organization.

SOPs

- Operationalize policies through standard operating procedures (SOPs).
- Effective SOPs will be applicable across the organization's structure and employee groups and will have privacy and security layered in.

Expert Groups/ Incentives

- Engage employees by creating expert or Privacy or Security Champion teams.
- Incentivize employees with an opportunity to further their professional expertise and become privacy delegates for their department.

Training Modules

- Use effective, scalable privacy and security training modules to encourage policy and SOP adherence through customized educational efforts.

Awareness Programs

- Create campaigns and initiatives across employee groups to reinforce principles learned in training and supported by policies and SOPs.

Executive/Leadership Scorecard

- Assign accountability to the Executive and Leadership groups using executive scorecards, which are the performance evaluation component of privacy and security engagement.

Leverage privacy and security policies

Develop new policies and leverage existing policies to reinforce key principles and requirements of your privacy and security programs.

- Policies are the foundation of governance and operations of a solid privacy and security program.
- Policies must be reasonable, auditable, enforceable, and measurable, and they do not function in isolation. Policies should be supported by a set of tactical procedural documents and workflows.
- Effective policies should be easily understood across all groups within the organization but specific and directive enough to provide your IT, InfoSec, and Privacy teams with the operational guidance they require.

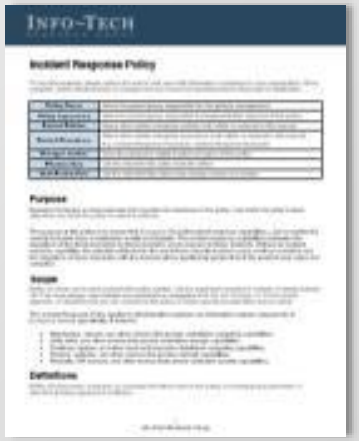
Policies

Data Protection Policy

Data Retention Policy

General Security – User Acceptable Use Policy

Security Incident Management Policy



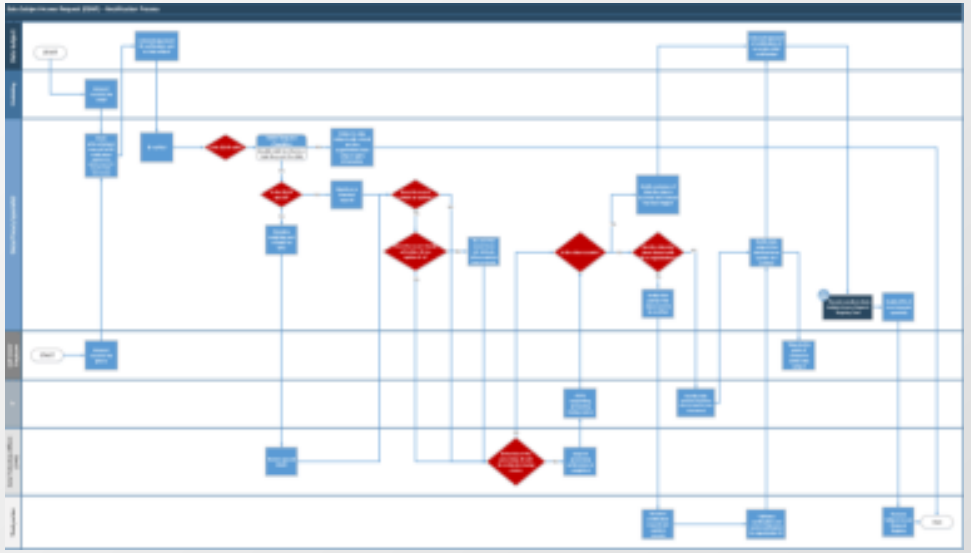
Leverage privacy and security SOPs

SOPs

Standard operating procedures (SOPs) provide a tactical set of steps that address the "how to" of high-level privacy and security policies.

- Integrating privacy and security principles into your organization's operations is challenging, but it's a key component in ensuring your employees can apply these important principles in their daily tasks and responsibilities.
- SOPs can be standalone documents or can be included within existing policy or crossover policy/procedural documents.
- Use the privacy and security policies as a baseline, and for policy statements that directly impact employees or staff, ensure that a corresponding procedure or set of procedures is built out in detail.
- Workflow SOPs help contextualize the step-by-step nature of the procedure and provide an easy-to-digest visual representation of what is often a complex set of tasks and steps.

Subject Access Request (SAR) – Rectification



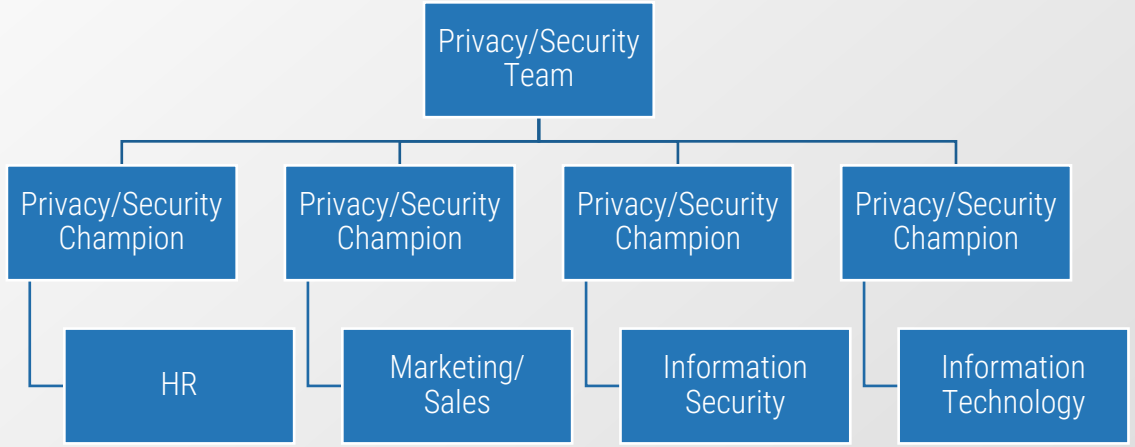
This data subject access request (DSAR) workflow is an example of a procedural document that helps employees understand the steps in, as well as the owners of, the process of responding to a request for information from a customer or client.

Leverage privacy and security expert groups and incentives

Expert Groups/ Incentives

Create ownership and develop in-house expertise in privacy and security by encouraging employees to join expert groups and share knowledge.

- Developing a team of Privacy Champions and Security Champions from different departments or business groups helps ensure that privacy and security initiatives are not only pushed from the top down but also supported from the bottom up.
- To determine who will act as your champions, consider the example on the right. Notice that the champion is a key point of contact between the Privacy and Security team and the respective business unit. Department heads may be the most logical choice, but remember to account for any special training (e.g. privacy certification) that might make another person more appropriate.
- Be aware that your proposed champions may not be fully ready for the job on day one. Consider how the organization might support their development (e.g. certifications, courses, professional memberships, job shadow). These perks may motivate people to join, but other incentives (e.g. earned day off) may also be appropriate in some cases.



Privacy Team Membership Perks

- Opportunities to assist with initial planning and final implementation of changes in privacy and security procedures within business unit.
- Paid/subsidized training courses or professional designation certification fee/professional association membership fee.
- Additional performance recognition as a part of yearly performance review.
- Cross-functional job shadowing opportunities.

Leverage privacy and security training modules

Create role-specific training that gives employees additional context for privacy procedures and security best practices.

- Effective privacy and security training is a core component of a strong privacy and security culture. Without training, your employees may not understand how their roles intersect with the pillars of security and privacy.
- Therefore, training should be role specific, and its scope should correspond to the level of interaction the role has with the pillars of security and privacy (e.g. your CEO will likely require different training than your HR department). When your staff feel the training is related to their role, they will be able to learn and apply the training more effectively.
- Info-Tech's security awareness and training research can assist with this effort.

↓ Download *Develop a Security Awareness and Training Program That Empowers End Users*

Training Modules

Security Training Campaign Development Tool

1. Privacy and security training content (videos, instructional e-cards/pamphlets, online learning sessions, visual slide deck presentations)
2. Policy and procedural reinforcement
3. Module-specific tests/quizzes, practical tests (phishing, social engineering, etc.)

Leverage privacy and security awareness programs

Like training modules, awareness programs must be designed to capture role-specific intersections with privacy and security. Generic programs that treat every role the same lack relevance and are easy to ignore and forget about.

- Awareness programs for privacy and security should directly align with the training modules that have been developed and deployed.
- Their primary purpose is to reinforce the key messages of the training modules through a variety of mediums and methods.
- Effective awareness programs should be personal and applicable: Highlight instances and examples that directly relate to the role of the employees in question.
- Focus on promoting a more proactive approach to privacy and security through behavior changes. Use the behaviors identified in Activities 1.1.1 and 1.1.2 to guide the development of your organization's custom awareness program.

Awareness Programs

Security Awareness and Training Module Builder

1. **Privacy and security awareness collateral (posters, emails, desk cards, calendar reminders)**
2. **Reinforcement of key principles from training modules**
3. **Policy and SOP acknowledgement**

Leverage privacy and security executive scorecards

Executive/Leadership Scorecard

Give your Executive and Leadership groups performance objectives that are based on the overall privacy and security culture of their teams.

- Quantifying culture and engagement is a complex task that ultimately relies on assessing the parties based on the selected thresholds, targets, metrics, or KPIs.
- Within the four primary organizational groupings you explored in Step 2.1, your top two groups – Executive and Leadership – should have performance assessment criteria directly linked to the organization's overall engagement in privacy and security.
- These can be included as a part of Executive Scorecards, which motivate these top-tier groups to embed privacy and security practices and principles within the organization's operations.
- Use the set of metrics you'll identify in Phase 3 of this research to develop your Executive Scorecards, customizing based on the role of the individual in question, as well as other relevant performance assessment objectives for their role.

Executive Privacy and Security Scorecard

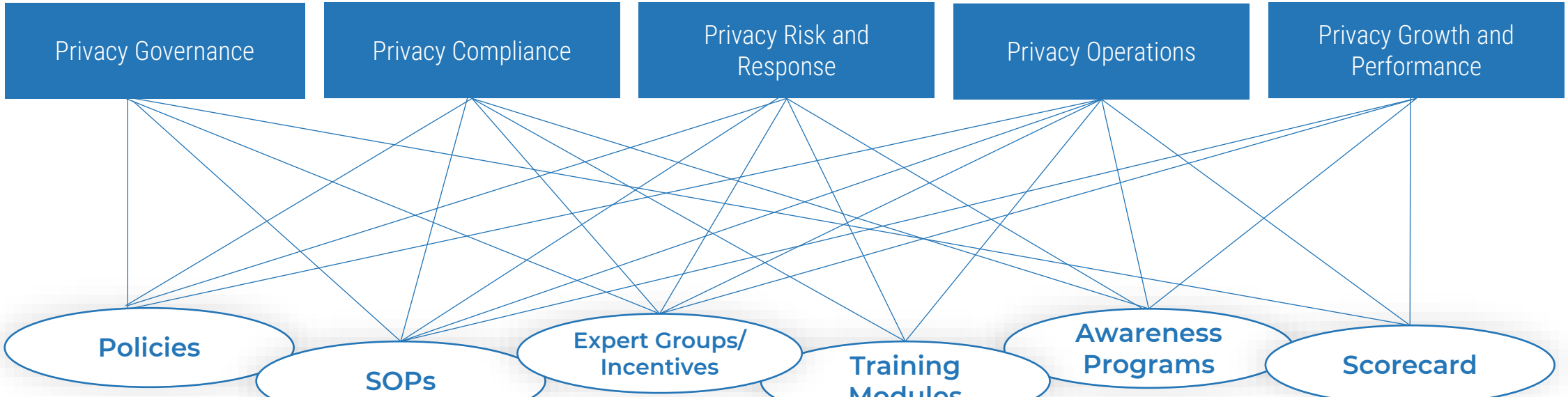
1. Total number of staff training modules completed
2. Total number of privacy/security awareness campaigns active
3. Change in number of privacy violations since last year
4. Change in number of security incidents reported since last year
5. Number of Privacy Champion team meetings conducted
6. Number of Security Governance cross-functional meetings conducted

Leadership Privacy and Security Scorecard

1. Department participation rate in privacy/security training modules
2. Department participation rate in privacy/security awareness campaign training activities
3. Percentage of incidents in department appropriately escalated
4. Number of privacy violations within department
5. Number of active Privacy/Security Champions within department

Map engagement enablers to privacy pillars

Each of the five pillars of privacy will be supported by enablers to promote engagement across the organization's various departments, business units, and employees.



- Privacy charter
- External/internal privacy policy/statement
- HR privacy policy
- Data breach response policy
- Data classification policy
- Data retention policy
- Vendor privacy management policy

- PIA process
- Data classification process
- DSAR handling process
- Business SOPs
- Data breach response SOPs
- Procedures for data de-identification/ anonymization

- Ownership/sponsorship
- Privacy steering committee
- Privacy core team
- Privacy Champions
- Educational/certification-based incentives

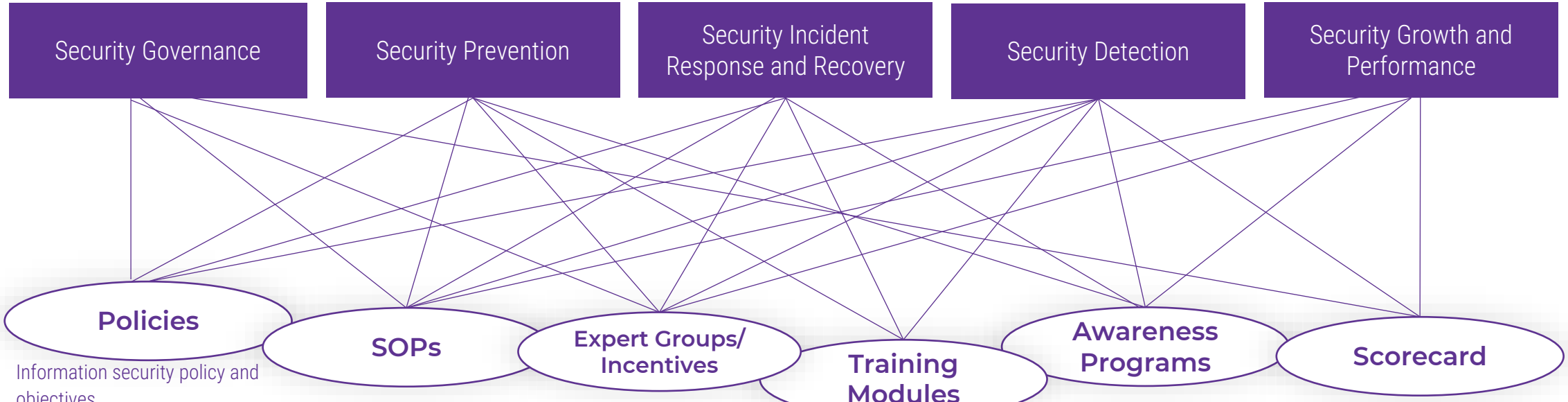
- Privacy regulation interpretation and mapping
- Data classification training
- PIA methodology
- Privacy by design training/ Data protection by design training
- Data security training
- Data retention training

- Executive training
- Basic employee privacy awareness training
  - Data protection principles
  - Data subject rights
  - Do's and don'ts
- Business-process-related awareness training

- Executive scorecard
  - Enterprise-wide measurement and trends
- Business leadership scorecard
  - Business-process-related measurement and trends

Map engagement enablers to security pillars

Each of the five pillars of security will be supported by enablers to promote engagement across the organization's various departments, business units, and employees.



- Information security policy and objectives
- Security risk management policy
- Information classification policy
- Supplier security policy
- Access control policy
- Mobile/corporate device policy
- Physical security policy
- Acceptable use policy
- Removable media policy

- Incident response and reporting SOPs/runbooks
- System updates/ patching SOPs
- Business SOPs
- Role/department-specific operations

- Ownership/sponsorship
- Security steering committee
- Security team
- Security Champions
- Educational/certification-based incentives

- Security risk assessment and treatment methodology
- Security engineering
- Wi-Fi spoofing/secure network practices
- Clean workspace training
- Remote work protocols training module
- Email safety training

- Executive training
- Business-scenario-related awareness training
- Basic employee cybersecurity awareness
  - Cybersecurity concepts
  - Acceptable use
  - Identity and password protection

- Executive scorecard
  - Enterprise-wide measurement and trends
- Business leadership scorecard
  - Business-process-related measurement and trends

2.2.1 Identify and align privacy and security enablers (optional)

30-45 minutes

1. As a group, review slides 52 to 60 to understand what the six types of enablers represent and to see examples of these enablers in the context of the privacy program.
2. Review the completed *Privacy and Security Engagement Charter* and determine which initiatives can be supported by enablers already in use at the organization and which enablers will need to be developed. Make a note of any enablers that need to be created or updated; you will use this information later.
    - Remember: The point of this exercise is to ensure that privacy and security are represented in the workflows of all of your organizational groups. Assigning each group the appropriate enablers will help ensure this happens.
3. Repeat these actions for security enablers.

Info-Tech Insight

Organizations developing their privacy or security initiatives from scratch will benefit most from this exercise. As privacy and security initiatives mature, they often become less generalized and may not map as neatly to a single enabler, so higher maturity organizations can skip this exercise if desired.

Input

- Outputs from Activity 1.2.2
- *Privacy and Security Engagement Charter*

Output

- A set of privacy and security enablers that map to the organization's privacy and security initiatives and objectives

Materials

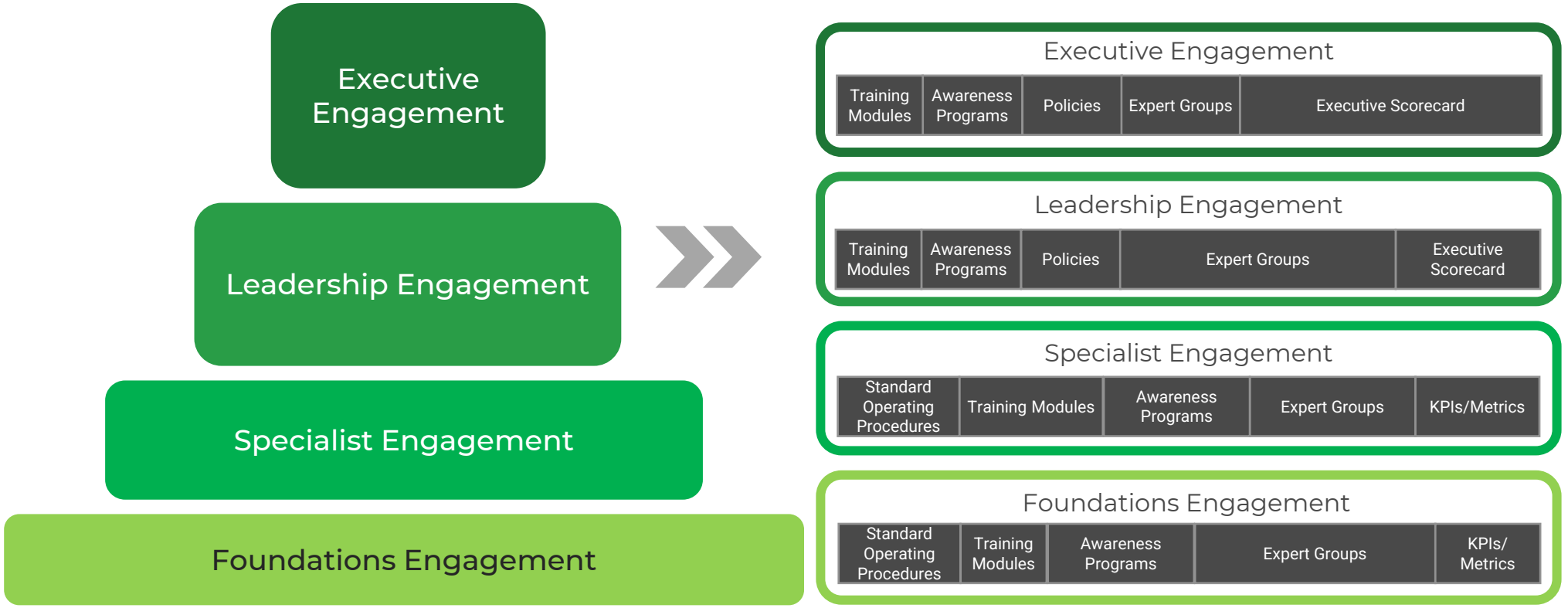
- Laptop
- Sticky notes (five different colors, or stickers to put on each sticky note)
- Markers

Participants

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead

Map engagement enablers to the organization's structure

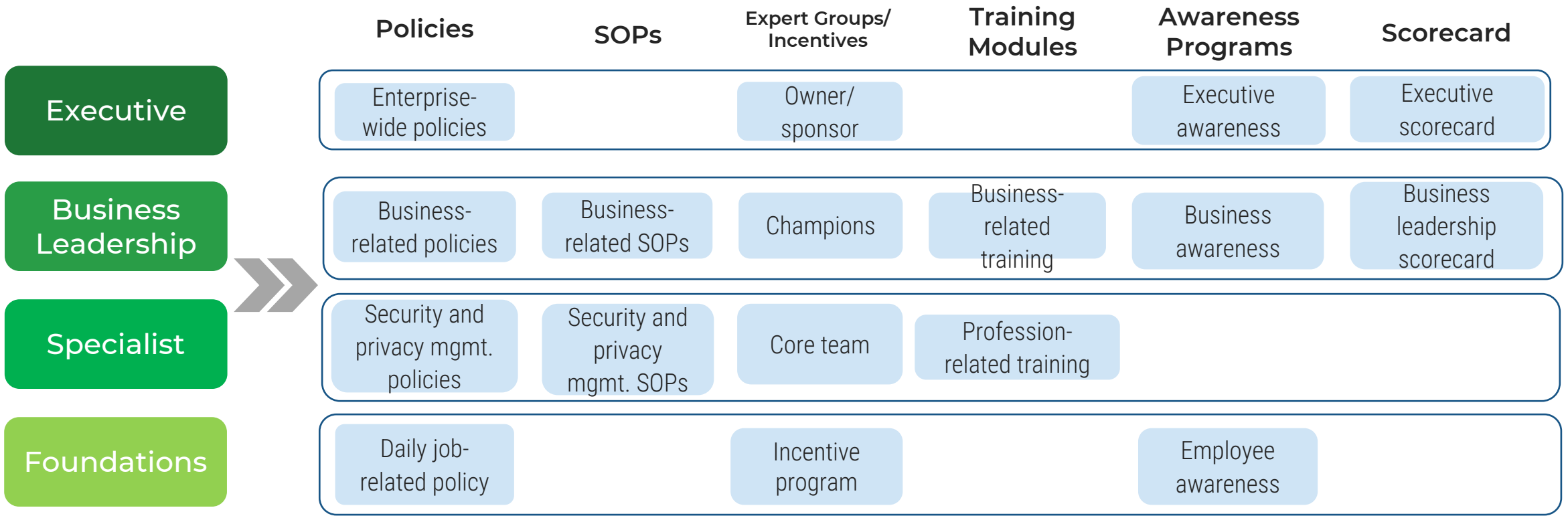
Each employee has a different role, responsibility, and level of accountability with respect to privacy and security. Align your privacy and security engagement enablers in a manner that takes into account the role and function that the individual fulfills.



Certain enablers will align more closely with specific organizational groups. For example, the Executive Scorecard will heavily align with the Executive team, somewhat align with the Leadership team, and likely not be relevant for the Specialist and Foundations groups.

Example: Map engagement enablers to the organization's structure

Each employee has a different role, responsibility, and level of accountability with respect to privacy and security. Align your privacy and security engagement enablers in a manner that takes into account the role and function that the individual fulfills.

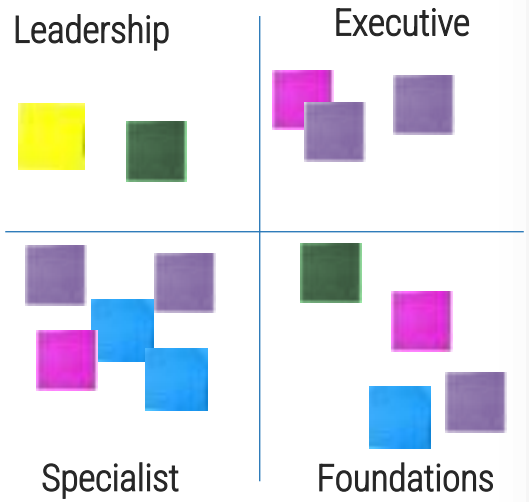


Certain enablers will align more closely with specific organizational groups. For example, the Executive Scorecard will heavily align with the Executive team, somewhat align with the Leadership team, and likely not be relevant for the Specialist and Foundations groups.

2.2.2 Assign enablers to organizational groups

30-45 minutes

1. Review slides 62 to 63 as well as the output from activity 2.2.1, if applicable. Do this activity as one large group to ensure appropriate representation and input.
2. On the whiteboard, list the organizational groups *(Executive, Leadership, Specialist, Foundations)* and discuss which enablers are appropriate for each group (i.e. through what means will they engage with privacy and security as part of their workflow). Keep in mind not all groups will have equal amounts of engagement.



   - Note: Some sticky notes will require duplication because they will apply to two different organizational groups. If this is the case, obtain group consensus and then duplicate and place in appropriate quadrant.
3. Discuss results as a group and document in tab 1, Enabler Mapping, of the *Privacy and Security Business Alignment Tool*, which will help you keep track of which enablers will be applied to each organizational group.

↓ Download Info-Tech's *Privacy and Security Business Alignment Tool*

Input

- Output from Activity 2.2.1

Output

- Completed tab 1 of the *Privacy and Security Business Alignment Tool*
- Enablers mapped to each of the organization's different business units/departments and functional groups

Materials

- Laptop
- Sticky notes
- Markers
- *Privacy and Security Business Alignment Tool*

Participants

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead

Step 2.3

Match Employee Attributes and Behaviors

Activities

2.3.1 Map Behaviors to Enablers

Map Your Privacy and Security Enablers

This step will walk you through the following activities:

- Map behaviors to enablers.
- Complete the *Privacy and Security Business Alignment Tool*.

This step involves the following participants:

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead

Outcomes of this step

Understanding of the employee attributes and behaviors that will promote a culture of privacy and security and will drive engagement in the organization.

2.3.1 Map behaviors to enablers

45-60 minutes

1. On the whiteboard, write down each of the privacy and security behaviors (negative and positive) identified during Activities 1.1.1 and 1.1.2.
2. As a group, start with the positive behaviors and map each one to the security and privacy enablers that reinforce it.
    - Note: Watch for any positive behaviors that are not supported by enablers. If this occurs, discuss why and determine whether new enablers should be created or if existing enablers need to be modified to accommodate these outliers.
3. Repeat this exercise for the negative behaviors. This time, however, you want to map enablers that **help to rectify each of the negative behaviors**. For this part of the activity, ensure that each of the organizational groups (Executive through to Foundations) is left with no negative privacy or security behaviors unaccounted for. Every negative behavior should be assigned an enabler to correct it.
4. Discuss, review, and validate results, then document them in the Additional Notes and Comments section of slides 15 to 18 in the *Privacy and Security Engagement Playbook*.

↓ Download Info-Tech's *Privacy and Security Engagement Playbook*

Input

- Outputs from these activities:
    - 1.1.1
    - 1.1.2
    - 2.1
    - 2.2.1
    - 2.2.2

Output

- Privacy and security behaviors mapped and supported/rectified by corresponding enablers

Materials

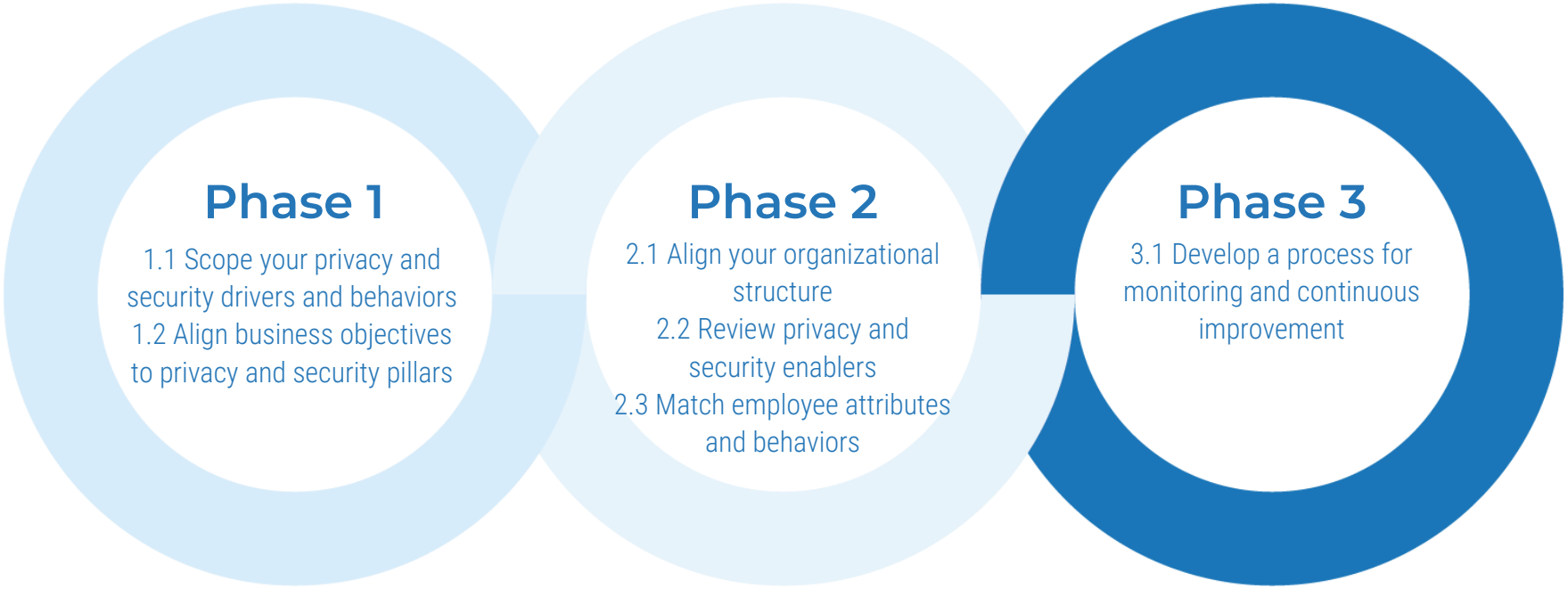
- Laptop
- Whiteboard
- Markers
- *Privacy and Security Engagement Playbook*

Participants

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead

Phase 3

Identify and Track Your Engagement Indicators



Embed Privacy and Security Culture Within Your Organization

This phase will walk you through the following activities:

- Develop a process for monitoring and continuous improvement.

This phase involves the following participants:

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead
- Members of the executive leadership team

Step 3.1

Develop a Process for Monitoring and Continuous Improvement

Activities

3.1.1 Select Your Program Metrics

3.1.2 Assign Ownership for Reviewing and Reporting

3.1.3 Create and Communicate the *Privacy and Security Engagement Playbook*

Phase Title

This step involves the following participants:

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead
- Members of the executive leadership team

Outcomes of this step

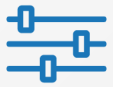
Ability to measure and manage privacy and security engagement.

Executive presentation to summarize initiative.

Give your privacy and security engagement program visibility

Make it visible, actionable, and repeatable

- Now that you've customized your privacy and security engagement program, your final step is to ensure that your progress can be measured.
- Assigning a quantitative value to culture and engagement is challenging, but with a business-informed approach, it's achievable.
- Ensuring that your program is iterative, has accountability and ownership, and has space to evolve as it matures is key for success.



Measure

Identify a set of metrics that shed visibility on the privacy and security engagement program while ensuring that the overarching business goals and objectives are supported.

Own

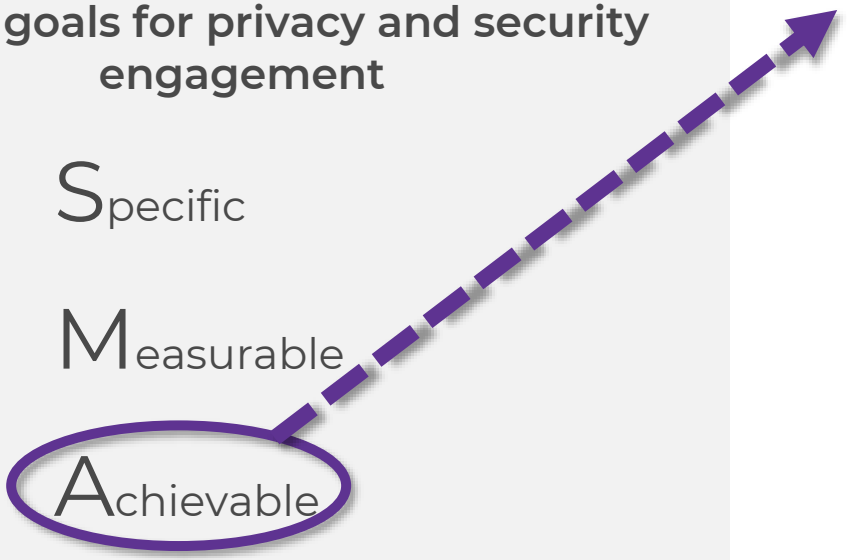
Accountability and ownership at all levels are integral to ensuring that the privacy and security engagement program functions and matures. Start by identifying metric owners as a part of the program's continuous improvement.

Communicate

An effective communication plan ensures buy-in from the top as well as from the ground up across the organization. Clear communication and transparency are the final step in getting the engagement program off the ground.

Tie your privacy and security engagement metrics to goals to make them worthwhile

Develop SMART metrics to support SMART goals for privacy and security engagement



Download Info-Tech's *Build a Security Metrics Program* for a step-by-step process on how to develop effective and relevant metrics for your security program.

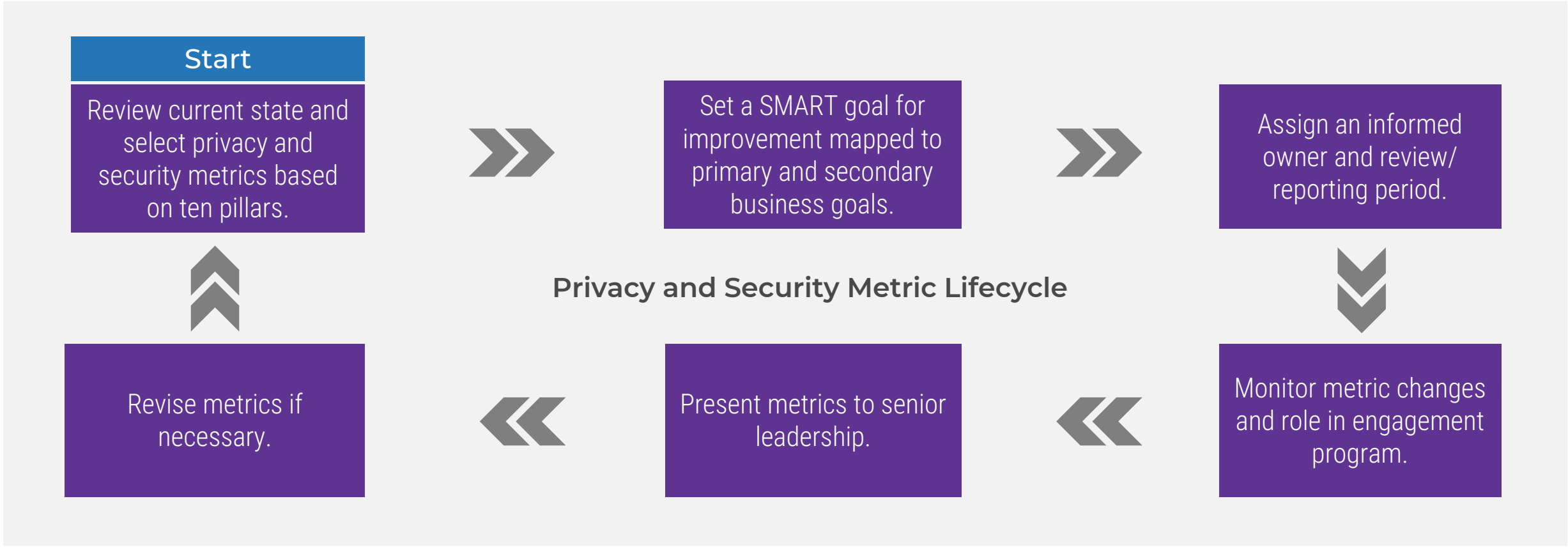
What is an achievable metric?

When we say that a metric is achievable, we imply that it is tied to a goal of some kind – the thing we want to achieve.

How do we set a goal?

1. **Determine what outcome you are trying to achieve.**
   - This can be small or large (e.g. "I want to determine what existing systems can provide metrics" or "I want a 90% pass rate on our monthly phishing tests").
2. **Decide what indicates that you've achieved your goal.**
   - At what point would you be satisfied with the progress made on the initiative(s) you're working on? What conditions would indicate victory for you and allow you to move on to another goal?
3. **Consider the role of key performance indicators (KPIs) to measure progress toward that goal.**
   - Now that you've defined what you're trying to achieve, find a way to indicate progress in relative or relational terms (e.g. percentage change from last quarter, percentage of implementation completed, ratio of programs in place to those still needing implementation).

Implement an iterative approach to privacy and security engagement metrics



Download Info-Tech's *Build a Security Metrics Program* for a step-by-step process on how to develop effective and relevant metrics for your security program.

Privacy metrics examples (KPIs)

Track and monitor the success of your privacy engagement program with tailored privacy metrics mapped to your privacy pillars. Use the following examples as starting points.

Privacy Governance

- Draft policy suite (% complete)
- % of policies receiving annual review
- % of policies needing updates
- % of privacy committee meetings held (vs. planned)

Privacy Compliance

- Familiarization with relevant compliance regulations (% complete)
- Progress toward compliance goal (% of initiatives complete)

Privacy Risk and Response

- % of projects receiving privacy risk assessment
- % relevant projects receiving data protection impact assessment/privacy impact assessment
- Privacy risk score or ratio (% away from target state)

Privacy Operations

- % of DSARs completed within target window
- % of DSARs not completed
- % of relevant processes that include privacy by design

Privacy Metrics

- % of new hires completing privacy training within target window
- % of underprotected data (by repository)
- % of staff hitting targets for privacy training
- % in attendance of privacy awareness training sessions (by department)

Security metrics examples (KPIs)

Track and monitor the success of your security engagement program with tailored security metrics mapped to your security pillars. Use the following examples as a starting point.

Security Governance

- % of business initiatives involving security
- % of security recommendations implemented by the business
- % of incidents related to governance gaps (e.g. missing policy or process)

Security Prevention

- % of data misclassified/classified
- % of shadow IT systems eliminated or formally adopted
- % of sensitive data with appropriate security controls applied (encryption, obfuscation, etc.)

Security Detection

- % of incidents detected inside of target window
- % of critical data loss prevention alerts
- % of data loss incidents reported inside of target window

Security Incident Response & Recovery

- % of incidents responded to inside of target window
- % end-user-detected incidents reported within target window
- % of incidents escalated using appropriate process

Security Metrics

- % of successful phishing tests/social engineering attempts
- % of staff receiving security training
- % pass/fail on security training

3.1.1 Select privacy and security engagement metrics

1-2 hours

For each primary and secondary business goal and supporting privacy and security initiative, identify a corresponding metric or set of metrics to demonstrate the progress of the engagement program.

1. Document your goals on the whiteboard and discuss as a group what would indicate that progress is being made toward those goals (i.e. completing the initiatives that support them).
    - In many cases, your initiatives will focus on implementing something absent. A percent-complete metric works well for these (see examples on slides 72 to 73).
    - As you mature, initiatives will likely focus on improvement by setting targets that you want to meet. In these cases, percent of cases within/outside target often works well.
    - Try to frame all your metrics in terms of percent, which helps give context when reporting. To calculate these, you will likely need to draw from a few technical measures (e.g. number of incidents, mean time to respond).
2. Review the metrics assigned to each goal. Select two or three metrics per business goal and document on slides 15 to 18 of the *Privacy and Security Engagement Playbook* and on tab 5 of the *Privacy and Security Business Alignment Tool*.

↓ Download Info-Tech's *Privacy and Security Engagement Playbook*

Input

- Outputs from Phase 2
- *Privacy and Security Engagement Charter*
- *Privacy and Security Business Alignment Tool*

Output

- Privacy and security engagement metrics mapped to business goals

Materials

- Laptop
- Markers
- Whiteboard
- *Privacy and Security Engagement Playbook*

Participants

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead

Who owns privacy and security culture?

Culture and engagement are shared responsibilities.

- Trying to measure culture, or to quantitatively assess on a qualitative concept, requires more than just a numerical value.
- Creating meaningful metrics for privacy and security engagement goes beyond identifying the number of security incidents reported, or the number of privacy violations, and monitoring the changes on an ongoing basis.
- Behaviors, actions, and awareness are all core components of a workforce that is engaged with privacy and security and should be considered when developing the corresponding set of privacy and security engagement metrics.
- While the privacy and security programs may rest solely on the shoulders of IT, InfoSec, and Compliance, your engagement program relies on ownership from the top down and bottom up.
- The ongoing success of the program should be monitored with the help of specific metric owners, each of whom has a vested interested in and substantial knowledge of each of the primary and secondary business goals, the supporting privacy and security initiatives, and the corresponding set of privacy and security enablers.

"Measuring privacy and security culture involves measuring the humans that support and drive this culture. What you have to remember is that humans are more than just numbers."

– Tom Pendergast, MediaPRO

3.1.2 Assign ownership for reviewing and reporting

30-45 minutes

1. As a group, review the outputs from Activity 3.1.1 as well as the final version of the *Privacy and Security Engagement Charter* and the *Privacy and Security Business Alignment Tool*.
2. Discuss who the owners will be for each of the indicators identified in Activity 3.1.1.
    - Note: Metric owners should be individuals that have a robust understanding of what data the metric involves, how it directly impacts its corresponding pillar of privacy and security, and how it impacts the business goals and objectives.
    - They should have a stake in the privacy and security engagement program and a solid understanding of the organization's privacy and security goals.
    - The metric owner may need to recruit the assistance of other staff (often from IT) to pull the relevant data that supports the metric.
3. In tab 2 of the *Privacy and Security Business Alignment Tool*, document the assigned metric owners and target percentages (e.g. 100% of relevant reviews completed, 10% or fewer processes causing legitimate friction).
    - Note: Metrics are meant to be iterative and flexible. As the maturity of the organization's Privacy and Security Engagement program grows, the metrics chosen to represent and gauge progress should change.
4. Document your metrics on slides 15 to 18 of the *Privacy and Security Engagement Playbook*.

Input

- Outputs from Phase 2
- Outputs from Activity 3.1.1
- Completed *Privacy and Security Business Alignment Tool*
- Completed *Privacy and Security Engagement Charter*

Output

- Completed *Privacy and Security Engagement Playbook*

Materials

- Laptop
- *Privacy and Security Business Alignment Tool*
- *Privacy and Security Engagement Charter*
- *Privacy and Security Engagement Playbook*

Participants

- CISO/InfoSec lead
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead

3.1.3 Compile and communicate the Privacy and Security Engagement Playbook

60 minutes

1. Once all outputs from Phase 1, 2, and Activities 3.1.1 and 3.1.2 have been added to the playbook template, schedule time to communicate the *Privacy and Security Engagement Playbook* to your senior leadership or executive team and all other relevant stakeholders.
2. Prior to presenting, ask the following questions:
    - What is the objective in presenting this report? What do we want to achieve?
    - Is there a clear and logical link between the outputs from this program and the business objectives and goals of the organization?
    - How does this incorporate the organization's current approach to privacy and security awareness and training efforts, and what are the key differences between this program and a traditional awareness and training program?
    - What are the core value adds or business benefits of the privacy and security engagement program, and how can we ensure these are highlighted upfront?
3. Add or remove slides and text to the playbook template. When all of the above points are accounted for, it is ready to present.

Input

- Outputs from Phase 2
- Outputs from Activities 3.1.1 and 3.1.2
- Completed *Privacy and Security Business Alignment Tool*

Output

- Completed *Privacy and Security Engagement Playbook*

Materials

- Laptop
- *Privacy and Security Engagement Playbook*

Participants

- CISO/InfoSec lead
- Executive leadership/senior leadership team
- InfoSec managers and team
- Privacy officer/privacy program manager
- Compliance manager/lead

Summary of Accomplishment

You've laid the foundation for organizational privacy and security engagement

By embedding privacy and security engagement within your organization's business objectives and using enablers to integrate this engagement into every level of your organizational groups, you have successfully laid the foundation an effective privacy and security culture can grow from.

By clearly indicating when, where, and through what means staff at all levels will engage with security or privacy, these things become tangible and straightforward as opposed to an intimidating set of complex rules that seem to hinder business operations. Instead, they will serve to enrich business operations and allow the organization to better serve its clientele.

If you would like additional support, have our analysts guide you through other phases as part of an Info-Tech workshop.

Contact your account representative for more information.

workshops@infotech.com
1-888-670-8889

Additional Support

If you would like additional support, have our analysts guide you through other phases as part of an Info-Tech Workshop.

To accelerate this project, engage your IT team in an Info-Tech workshop with an Info-Tech analyst team.

Info-Tech analysts will join you and your team at your location or welcome you to Info-Tech's historic Toronto office to participate in an innovative onsite workshop.

Contact your account representative for more information.

workshops@infotech.com 1-888-670-8889

The following are sample activities that will be conducted by Info-Tech analysts with your team:

Identify Security Drivers

During this activity, your team will address identified drivers from both a security and privacy culture perspective. An Info-Tech analyst will guide the discussion around leveraging these drivers to align privacy and security engagement with organizational performance.

Assign Enablers to Organizational Groups

This activity guides the alignment of the different departments and roles within the organization with the privacy and security enablers that promote engagement. An Info-Tech analyst will help you understand which roles best align with the four hierarchical groupings.

Research Contributors and Experts

Steve Stalder
Senior Program Manager, Privacy, Ancestry
CIPP/US, CSM

Robert J. Toogood
Subject Matter Expert (SME) in Digital Risk | Specialist Expertise in Cybersecurity, Data Protection and Privacy, Information Security, Business Resilience, Governance, and Risk | Advisory, Audit & Assurance Services

Tom Pendergast, Ph.D.
Writer, Security and Privacy Awareness Specialist, Speaker

Related Info-Tech Research

Build a Security Metrics Program to Drive Maturity

- Many security leaders put off adding metrics to their program because they don't know where to start or how to assess what is worth measuring.
- This blueprint will help you to select effective security metrics and align your metrics to goals to ensure that you are collecting metrics for a specific purpose rather than just to watch the numbers change.

Build a Data Privacy Program

- Sell privacy to the business by speaking a language they understand. IT and InfoSec leaders need to see privacy as not just compliance but also a driver of business efficiency.
- Integrate and build by developing a program that promotes freedom of information and establishes privacy and security standards with respect to access of this information.

Develop a Security Awareness and Training Program that Empowers End Users

- One-time, annual training is no longer sufficient for creating an effective security awareness and training program.
- Create a training program that delivers smaller amounts of information on a more frequent basis to minimize effort, reduce end-user training fatigue, and improve content relevance.

Bibliography

"2020 State of Privacy and Security Awareness Report." *MediaPRO.* 2020. Accessed November 2020.

"2020 Thales Data Breach Report." *Thales, IDC.* March 2020. Accessed 3 January 2021.

Auxier, Brooke, et. al. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." *Pew Research Center.* 15 November 2019. Accessed December 2020.

Breaux, Travis D. "An Introduction to Privacy for Technology Professionals." 2020.

California Consumer Protection Act of 2018. Sections 1798.100 – 1798.199. 2018. Accessed November 2019.

Cavoukian, Ann. "Privacy by Design, The 7 Foundational Principles." *IPC Privacy by Design,* January 2011. Accessed January 2020.

Cisco. "Consumer Privacy Survey 2019." *Cisco.* November 2019. Accessed January 2021.

Cisco. "From Privacy to Profit: Achieving Positive Returns on Privacy Investments." *Cisco Data Privacy Benchmark Study 2020.* 2020. Accessed December 2020.

Cisco. "Maximizing the Value of Your Data Privacy Investments: Data Privacy Benchmark Report." *Cisco.* January 2019. Web. January 2021.

Cukier, Michel. "*Study: Hackers Attack Every 39 Seconds." A. James Clark School of Engineering, University of Maryland. 2007*. Web. December 2020.

Densmore, Russell,. "Privacy Program Management: Tools for Managing Privacy Within Your Organization." *IAPP,* 2019.

General Data Protection Regulation. Chapters 1-11. May 2018. Web. December 2020.

Government of Canada. "The Personal Information Protection Electronic Documents Act." April 2000. Web. December 2020.

IAPP. "IAPP-EY Annual Privacy Governance Report 2019." *IAPP,* 2019. Web. December 2020.

IBM Security. "Cost of a Data Breach Report, 2020." *IBM*, *Ponemon Institute*. 2020. Web. January 2021.

Mühlberg, Byron. "Companies With Data Privacy Practices Enjoy Big Financial Benefits." *CPO Magazine*, 12 February 2020. Web.

"New data protection law gives people greater control over their own information." Information Commissioner's Office (ICO), 6 March 2017. Web.

Newby, Adrian. "Why Privacy is the New Corporate Culture." *PrivSec Report.* 26 April 2018. Web. December 2020.

NIST. "NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management." *NIST,* 16 January 2020. Web. January 2020.

PayScale. "Average Principal Management Consultant Salary." *PayScale.* 2 February 2021. Web. February 2021.

Roer, Kai, Petric, Dr. Gregor, et al. "Measure to Improve: Security Culture Report 2020." *KnowBe4.* 2020. Web. January 2021.

Romeo, Chris. "6 Ways to Develop a Security Culture from Top to Bottom." *TechBeacon.* Web. December 2020.

Salesforce. "State of the Connected Customer: Third Edition." *Salesforce.* 2019. Web. February 2021.

"Study: Mature Privacy Programs Experience Higher ROI." *IAPP,* 27 January 2020. Web. January 2021.

UNCATD. ""Data Protection and Privacy Legislation Worldwide." *United Nations Conference on Trade and Development."* April 2020. Web. January 2021.

INFO~TECH
RESEARCH GROUP