Managing the Privacy Maturity of a Standalone Subsidiary

How to assess, measure, and improve the privacy profile of a standalone subsidiary after the acquisition is completed

Laurel Strand
Senior Privacy Analyst, Intel Privacy Office

Daniel Christensen
Senior Privacy and Security Counsel, Intel

Executive Summary

Intel developed a privacy maturity assessment process to help manage standalone subsidiary privacy and protect the personal information of employees, customers, and partners. The process assesses the privacy program of a subsidiary after the acquisition is completed, measures the privacy maturity, and develops a roadmap to help the subsidiary improve privacy practices as appropriate. This white paper reviews the process in detail and illustrates how Intel applies it to new standalone subsidiaries after the acquisition is completed.

"The privacy maturity model allows me to quickly and objectively gauge the health and status of privacy in an acquisition and facilitates decision making with company leaders."

—Malcolm Harkins
Intel VP and Chief Security and Privacy Officer

Business Challenge

Intel is a proponent of responsible privacy and data protection. Respect for privacy is fundamental to our culture and helps us to maintain an environment where individuals can trust Intel and its technologies.

Acquisitions are a critical component of Intel's growth strategy. Intel is a multinational corporation that currently has many wholly-owned companies across the globe. The acquisition of a company requires the responsibility to protect the privacy of customers, consumers, suppliers, partners, and employees of both that acquisition and Intel.

In most of our acquisitions, we fully integrate the subsidiary into Intel. The integration process includes assessments of employee personal information, data, products, or services that have been acquired. The personal information of the new employees is protected by a system of controls, such as Intel Corporate Privacy Rules, privacy training, and information security policies.

In acquisitions where the acquired company will be held and operated as a standalone subsidiary, or even in cases where the acquired company will be gradually assimilated into Intel over time, Intel needs to assess and measure the new acquisition's level of privacy maturity. We created the privacy maturity assessment process to evaluate the privacy program of a new standalone subsidiary, measure its current level of privacy maturity, and, if necessary, determine a course of action for improving privacy (see Figure 1).

The following are common privacy issues that we may need to assess when acquiring smaller companies:

- Determine a legal basis for international transfer, such as U.S. Safe Harbor, Model Contract Clauses, or Binding Corporate Rules
- Confirm that Human Resources (HR) supplier contracts contain the appropriate controller or processor language, including responsibilities for breach response handling

Table of Contents

- Evaluate personal data use and retention policies with corresponding security policies
- Research whether subsidiary has employee notices or consent agreements for corporate computing devices and data on their personal devices, such as smartphone and other personal electronic devices; for example, bring your own device (BYOD).
- Determine if there are programs to help comply with local data protection regulations, such as database registration or data protection officer appointments

Because smaller companies may lack the in-house expertise to address all areas of a mature privacy program, Intel works with the subsidiary to develop a roadmap and shares its own policies and practices in order to enhance privacy maturity of the subsidiary.

Privacy Maturity Assessment Process

When Intel is considering whether to acquire a company, part of the pre-acquisition due diligence includes assessing privacy practices to see if there are any changes to the valuation of the acquisition or obstacles to completing the acquisition. After the acquisition is completed, we administer the privacy maturity assessment process, taking into consideration related information gathered during the due diligence period. The process has three phases:

- **Phase 1.** Assess privacy program using information gathered during due diligence and administration of the privacy management questionnaire.
- **Phase 2.** Measure privacy maturity using Intel's privacy maturity model (PMM), which is based on Generally Accepted Privacy Principles (GAPP) and other existing industry models.
- **Phase 3.** Establish a privacy roadmap and, if needed, a compliance plan of record.

One benefit we have recognized as we administer this process is the opportunity to build relationships with subsidiary employees with whom we will be working to assess and improve privacy maturity. These relationships help us assess whether proper resources exist to achieve the desired level of privacy maturity; if they do not, additional resources may be needed, which could affect the timelines in the privacy roadmap.

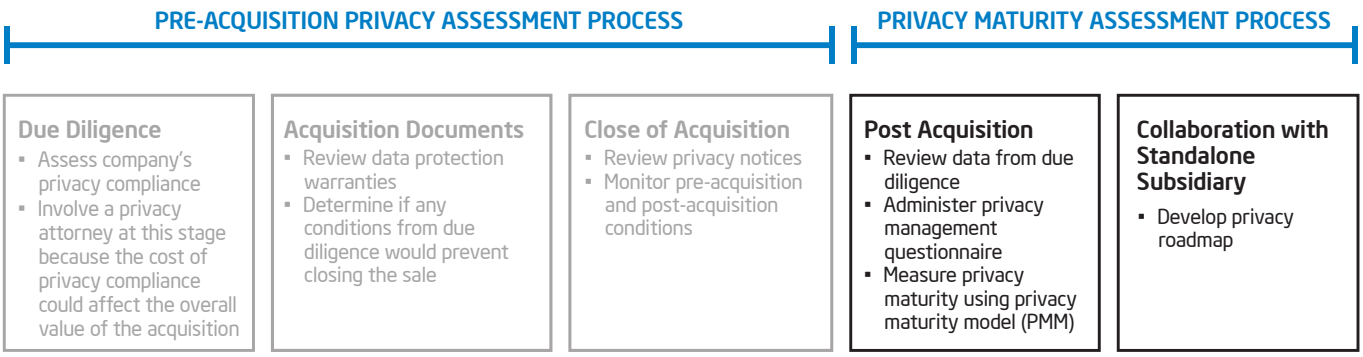

Figure 1. This sequence depicts when the privacy program is assessed during an acquisition. Privacy maturity assessment begins at the Post-Acquisition stage.

Phase 1: Assess Privacy Program

Intel starts its dialogue with key subsidiary stakeholders using the privacy management questionnaire. This assessment uses a list of privacy- and security-related questions (see Table 1) that are customized for each subsidiary based on a variety of factors, such as size, products and services produced, and locations of employees and customers. We also use the data that emerges from the pre-acquisition privacy assessment in due diligence to narrow the focus of the privacy maturity assessment.

Completing the assessment involves a three-step process:

1. Schedule meetings with stakeholders that handle the subsidiary's privacy issues.
2. Determine which questions apply to specific stakeholders and then review the customized questionnaire.
3. Document the responses.

Meetings with all key subsidiary stakeholders may take several weeks. In-person meetings are most effective if the subsidiary is in the same area. Otherwise, we set up 30-minute telephone interviews with stakeholders, making an effort to accommodate time zone differences if they are in other countries. Prior to each meeting, we customize the privacy management questionnaire to address the interviewee's specific functional area.

TABLE 1. SAMPLE QUESTIONS FROM THE PRIVACY MANAGEMENT QUESTIONNAIRE

TYPES OF PRIVACY ISSUES	SAMPLE QUESTIONS
Notice and Policy	Does your company have external privacy notices? If so, where are they located?
	Does your company have internal privacy notices? If so, where are they located?
	Do you have privacy and data protection in your contract and purchase order templates?
Breach Process	Do you have a privacy breach response process? If so, please describe it.
	Have you ever had a data or security breach?
	How many data or security breaches have you had in the last two years?
Accountability	Who is responsible for information security in your organization?
	Who is responsible for privacy compliance in your company?
	Are the following roles represented in your organization: Privacy Legal, Corporate Privacy Office, Chief Information Security Officer, and Data Protection Officer?
	Who manages privacy-related complaints, opt-out, and subject access requests? How does this work?
	Do you have a method to measure the effectiveness of your privacy program?
Products	Do you conduct privacy assessments or reviews for products and services?
	Are there guidelines for incorporating privacy into product design and development?
	Is privacy part of the product life cycle?
Security	In which countries do you have employees?
	Do you manage payroll internally or through a vendor?
	Do you have documented controls or policies for protecting employee data?
	Do you allow employees to use their personal devices at work?
	Where is your customer data stored?
	Where is your supplier data stored?

Building Relationships While Managing Privacy

One of the benefits of conducting the private maturity assessment process has been the relationships the Intel privacy and security experts have developed internally and externally. We have a strong working relationship with our Information Security team and often team up with them on site visits and interviews. These onsite visits provide insight into the subsidiary's corporate culture and help identify who is accountable for privacy. Privacy and Security teams work together regularly to provide subsidiary status updates to senior compliance managers at Intel, such as the chief information security and privacy officer, global director of privacy, and chief privacy and security counsel.

Privacy by Design

Intel's goal for a subsidiary that designs products or services is to have it align with Privacy by Design (PbD) principles. This means that a company should include privacy and data protection throughout the life cycle of a product or service, from its development to its end of life. Industry architects follow PbD by building privacy checkpoints in various phases of development, increasing traceability back to the privacy requirements gathering process.

Phase 2: Measure Privacy Maturity

The findings from the privacy assessment (Phase 1) provide input to help measure privacy maturity using the PMM, which is based on GAPP and AICPA/CICA models. The PMM provides a common framework for assessing a privacy program. It also helps assess and communicate the current and target maturity levels of privacy at the subsidiary. This second phase involves the following:

1. Establish a baseline privacy maturity score (1–5) by evaluating the data gathered in the privacy management questionnaire through the lens of the PMM (see Table 2). This model examines 12 privacy categories and rates a subsidiary's maturity level in each category. From low to high, these maturity levels are ad hoc, repeatable, defined, managed, and optimized.
2. Average the individual scores to formulate the overall score, then determine a target score to work toward based on risk factors.
3. Share the results with the subsidiary and Intel management so all stakeholders involved in the acquisition are aware of and agree on the recommended privacy improvement areas. In some cases, the legal team and stakeholders may challenge a finding because of a misunderstanding or incorrect information.

Phase 3: Establish a Privacy Roadmap

After identifying possible privacy improvements or enhancements, we use the privacy roadmap to identify the goals, timing, and commitment needed to achieve the target maturity level (see Figure 2 for an example). Since the maturity level and remedies vary according to individual subsidiary privacy profiles, each roadmap is unique. Depending on its overall PMM score, the subsidiary can be rated at one of three levels of privacy maturity: low, mid, or high.

- A low-level-maturity subsidiary may have a single attorney maintaining all legal compliance areas. Intel would create a long-term privacy roadmap that prioritizes privacy improvement areas for this subsidiary. The unique privacy profile for each subsidiary depends on location of central data processing, location of employees and customers, and the type(s) of products or services produced.
- A mid-level-maturity subsidiary may have resources dedicated to manage privacy and comprehend local regulations. However, it may need to enhance its privacy and security programs, including implementing or improving Privacy by Design[1] (PbD) principles, improving policies and notices, and developing better training. The roadmap, in this case, would address these areas of improvement.
- A high-level-maturity subsidiary might continue operating as it has been with no need for a roadmap.

[1] Privacy by Design refers to a framework developed by Ontario's Information and Privacy Commissioner: www.privacybydesign.ca

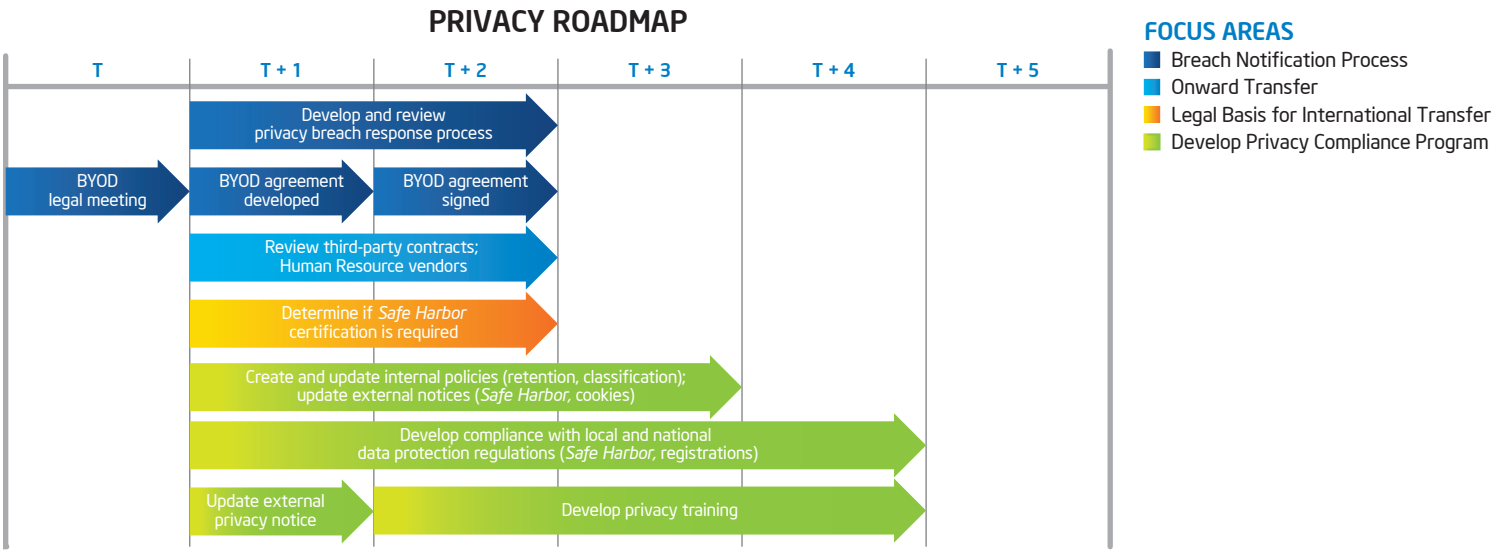

Figure 2. Example of a privacy roadmap. "T" is hypothetical and is not intended to indicate any specific measurement of time. FOR ILLUSTRATION PURPOSES ONLY.

TABLE 2. THE PRIVACY MATURITY MODEL (PMM) RATING SCHEMA FOR 12 PRIVACY CATEGORIES

PRIVACY CATEGORIES	MATURITY RATING 1 – AD HOC	2 – REPEATABLE	3 – DEFINED	4 – MANAGED	5 – OPTIMIZED
Privacy Policies	Subsidiary has policies, but they are not documented.	Subsidiary has policies that are documented, but they are neither comprehensive nor communicated.	Subsidiary has policies that are comprehensive, documented, well communicated, and consistent with laws and regulations.	Subsidiary makes changes in regulations that are also reflected in updates to policy. Employees that handle personal information are properly trained.	Subsidiary monitors and enforces policies, standards, and procedures.
Accountability	Management handles privacy issues reactively and has not defined roles that are accountable to privacy compliance.	Management assigns informal responsibility for compliance; however, resources are inadequate to meet all local compliance requirements.	Management has roles and responsibilities for compliance that are identified, communicated, and assigned to qualified personnel. Subsidiary addresses local data protection requirements.	Management monitors roles accountable for compliance and verifies compliance to local data protection requirements.	Management monitors the effectiveness of the privacy program.
Identification and Classification	Subsidiary does not classify personal information or have special handling procedures.	Some personal information is identified and classified, yet no formal classification program exists.	All personal information is identified and classified.	Subsidiary has procedures to ensure classifications are appropriately assigned and protected.	Subsidiary administers a formal risk management process to identify personal information and ensure compliance of business processes, systems, products, and services.
Incident and Breach Response	Subsidiary's response is reactive, and there are no documented procedures of how to manage incident response.	Some employees know how to respond to an incident, but response is informal and reactive.	Subsidiary has a privacy incident response process that is documented and includes identification, response, containment, and remediation.	Management conducts periodic reviews and walkthroughs of privacy incident response process.	Management assesses effectiveness of privacy incident response process and initiates improvements.
Notice and Use	Subsidiary provides notice of intended use of personal information, but it is not consistent or timely and may not cover all uses.	Subsidiary inconsistently provides notice of intended use of personal information, and may include a choice to allow use, type of use, and length of retention.	Subsidiary provides notice of intended use of personal information prior to collection, and includes a choice to allow use, a method to provide consent, describes the type of use, length of retention, and assurance of access and security.	Subsidiary provides notices that are easy to understand. Subsidiary conducts periodic reviews to ensure personal information uses are appropriate.	Subsidiary monitors use of personal information and verifies consent and notice.
Training	Subsidiary does not provide privacy training. New employees learn privacy knowledge from other employees.	Subsidiary administers a sporadic, inconsistent training program.	Employees who process personal information receive privacy training and are aware of documented policies and local regulations.	Subsidiary has a comprehensive privacy training program and monitors employee participation.	Subsidiary regularly updates privacy training to reflect regulatory changes and to incorporate learning situations specific to employee roles.
Privacy by Design (PbD)	Subsidiary does not have formal process to evaluate privacy risks in the products and services they create.	Subsidiary's development teams understand the concept of PbD, but do not consistently apply it.	Subsidiary has a documented process to assess privacy risks in products and services, and development teams are required to utilize the process.	Subsidiary has documented a PbD process, training is in place, and internal controls exist to make sure the process is consistently applied.	Subsidiary has documented best known methods for implementing PbD and collaborates with industry peers to influence PbD in other organizations.
Third-Party Transfer	Subsidiary does not have documented procedures or processes to ensure personal information that is shared with third parties is used only for the purpose stated in the notice and consent.	Subsidiary has documented procedures to ensure personal information shared with third parties is used only for the purpose stated in the notice and consent, but the process is not consistently applied.	Subsidiary has documented procedures to ensure personal information shared with third parties is used only for the purpose stated in the notice and consent, and the process is consistently applied.	Subsidiary has implemented procedures to obtain consent for any personal information to be disclosed to third parties.	Management ensures that the subsidiary obtained consent before disclosing personal information to third parties. Remediation plans are in place in case an inappropriate use of personal information is discovered.
Trans-Border Data Flows	Subsidiary does not have formal legal basis for international transfer of personal information.	Subsidiary has a process to obtain consent for international transfer of personal information, but the process is not consistently applied.	Subsidiary has an international transfer process that meets any required regulatory administrative measures.	Subsidiary has an international transfer process that includes public corporate commitments for any required regulatory administrative measures.	Industry peers and regulators recognize subsidiary as a leader and influencer for meeting international transfer regulatory requirements.
Access and Accuracy	Subsidiary has informal methods to access and update personal information, but they are neither documented nor consistently communicated.	Subsidiary's methods to access and update personal information are documented, but they are neither documented nor consistently communicated.	Subsidiary has privacy policies to address access and accuracy. Procedures for access are known by all employees and consistently applied across the organization.	Subsidiary has privacy policies that clearly address access by providing methods to update personal information. Individuals know what information about them exists and can update it.	Management monitors response time to requests for access. Subsidiary continuously implements improvements to the process.
Retention and Disposal	Subsidiary has started to define retention and disposal, but there is no formal documentation or consistent application.	Subsidiary has policies and procedures that define acceptable retention periods and destruction methods, but they are not consistently applied.	Subsidiary's use-of-information notices include retention and destruction policies and procedures. Employees are aware of the policies and consistently comply.	Subsidiary consistently documents retention periods and disposal methods for each collection and periodically reviews procedures for compliance.	Management monitors and enforces retention periods and disposal methods, and updates policies to reflect regulatory changes.
Security	Subsidiary does not have formal, documented security policies. Subsidiary's security measures are reactive.	Employees may be aware of personal information security requirements, but enforcement and documentation are inconsistent.	Subsidiary has privacy policies that reference applicable security policies. Employees are aware of security required to protect personal information.	Management monitors compliance to security provisions for personal information and makes required improvements.	Management monitors violations to security policies, conducts annual reviews of security, and implements improvements.

Case Study: Administering the Privacy Maturity Assessment Process

The data in this hypothetical case study is based on common issues of standalone subsidiaries.

Company Profile

ABC Company develops, licenses, distributes, and supports products and services. While based in the United States, it has locations in 17 other countries.

Phase 1: Assess Privacy Maturity

To identify key personnel in functional areas that process personal information, a privacy representative met with ABC Company's legal department to discuss what types of personal information they process. At this stage, the privacy representative addressed any concerns the ABC Company's legal team had regarding changes to corporate policy and using corporate resources. The representative then met with key people in business groups that either process or are exposed to personal information, such as HR, IT, Sales and Marketing, Product and Service Development, and Finance.

Phase 2: Measure Privacy Maturity

The first and second priorities were divided into a logical set of tasks that could be completed in a reasonable timeframe and were based on the privacy maturity profile of ABC Company (a business-to-business consumer model with employees in 17 countries).

These categories were given **first priority**:

- Incident and breach response (score: 1.5 out of 5) – IT department did not have a breach response process in place; however, they did have an informal process of escalation.
- International transfer (score: 1) – Determining the legal basis for international transfer will be complex given the many locations.
- Third-party transfer (score: 1) – HR vendor contracts and purchase orders must be reviewed for appropriate controller or processor language, including responsibilities for responding to a breach.

These categories were given **second priority**:

- Identification and classification (score: 1.5) – No classification schema for data exists.
- PbD (score: 1) – No skilled resources exist at ABC Company to perform this type of work, most products and software produced do not collect personal information.
- Privacy policies (score: 1.5) - Data privacy statement posted to intranet needs legal analysis. Separate link needed for privacy notice on external website.
- Security (score: 2) – HR database is not encrypted, and local data protection regulations differ in each country.
- Accountability (score: 1.5) – No single person is accountable for privacy compliance, and no formal privacy program exists. However, legal department manages privacy issues on an ad hoc basis.

Other concerns were discovered and were addressed after the first and second priority items are improved:

- Training (score: 1) – No formal privacy training exists.
- Retention and disposal (score: 1) – No retention policies exist at this time; however, IT works with the business to only maintain relevant information.
- Notice and use (score: 2) – Plans to enhance network security may require notice to employees.

The privacy representative shared all of this information with ABC Company and internal stakeholders and created an overall privacy maturity score summary (see Figure 3), which was shared with stakeholders and was used to track improvement over time. ABC Company was classified as a low-level-maturity subsidiary, with an overall score of 1.5.

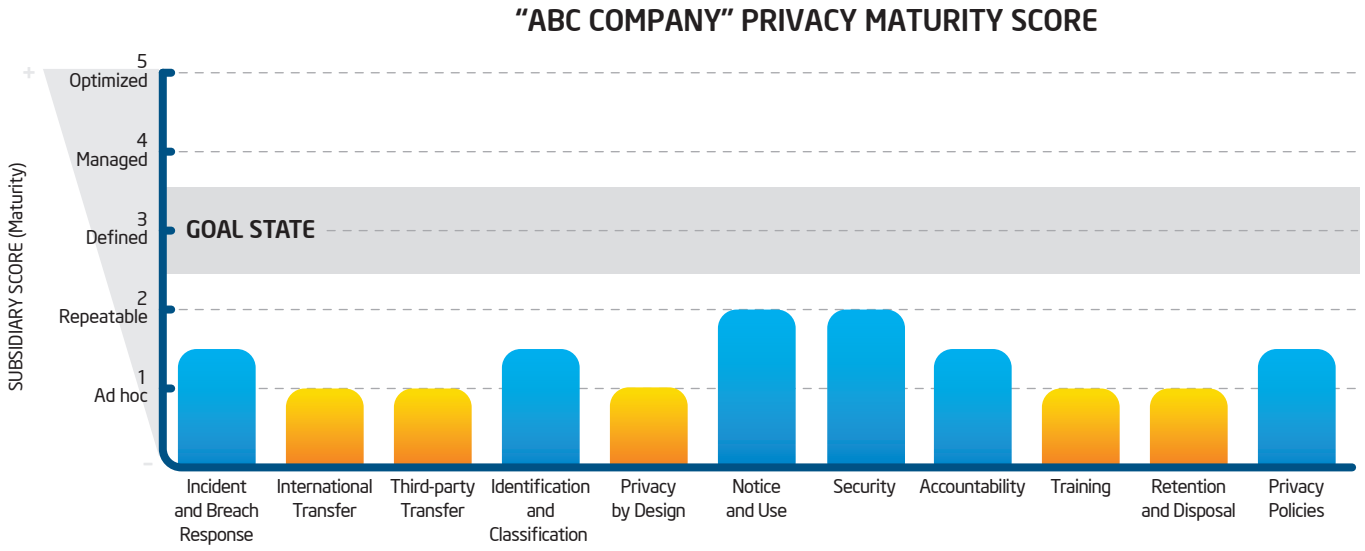

Figure 3. The overall privacy maturity score summary shows ABC Company's current privacy assessment scores and allows improvements to be tracked over time. The data in this hypothetical case study is based on common issues of standalone subsidiaries. FOR ILLUSTRATION PURPOSES ONLY.

Phase 3: Establish a Privacy Roadmap

At this time, the privacy representative shared the completed PMM with ABC Company's legal team and critical stakeholders to verify findings (Table 3). All parties then worked together to develop a long-term privacy roadmap (Figure 4), factoring in additional time to remediate other risks that were not privacy-related. Initial priorities to be addressed first included the concerns associated with incident and breach response, international transfer (for example, Safe Harbor certification), and third-party transfer (for example, Human Resource suppliers).

Results

The privacy assessment process helps identify the right stakeholders and involve them in measuring privacy maturity and establishing a privacy roadmap. The PMM establishes a privacy profile, provides a consistent method of communication, and provides input to the privacy roadmap. This information is then translated into an empirically measurable compliance plan of record. The ABC Company also reviews the roadmap and compliance plan of record on a regular basis and reports progress to stakeholders.

TABLE 3. ABC COMPANY'S PROFILE AND PRIVACY IMPROVEMENTS: THE ACQUIRING COMPANY SHARES THIS INFORMATION WITH THE SUBSIDIARY AND CORPORATE STAKEHOLDERS TO VALIDATE FINDINGS AND DEVELOP THE PRIVACY ROADMAP.

Company Profile	ABC Company develops, licenses, distributes and supports operating system software products "ABC Model" and "ABC Operating Sys," each of which is designed for use with a wide range of embedded hardware devices, along with a variety of additional software platforms, middleware, and tools. ABC Company also provides professional engineering and design services related to these offerings.		
Location of Legal Entities with Employees	▪ United States: 750 ▪ China: 350 ▪ Canada: 150 ▪ Romania: 105	▪ France: 80 ▪ Germany: 80 ▪ Japan: 80 ▪ South Korea: 80	▪ Sweden: 40 ▪ United Kingdom: 35 ▪ Italy: 20 ▪ India: 15
Location of Central Data Processing	United States		
Current Status	▪ Standalone ▪ Adopted Code of Conduct ▪ No formal Privacy Compliance or Information Security program		

Data Protection Improvements	▪ Data Breach Notification Process
	▪ Legal Basis for International Transfer
	▪ Third-party Transfer
	  ▪ HR outsourcing agreements
	  ▪ Vendor security		

Privacy Program Improvements	▪ Data Classification/Retention
	▪ Privacy by Design
	▪ Local Data Protection Regulations
	  ▪ DPO appointments
	  ▪ Data Processing Registration
	▪ Employee notices – BYOD and consent to transfer
	▪ HR data not encrypted
	▪ No single person accountable for privacy compliance		

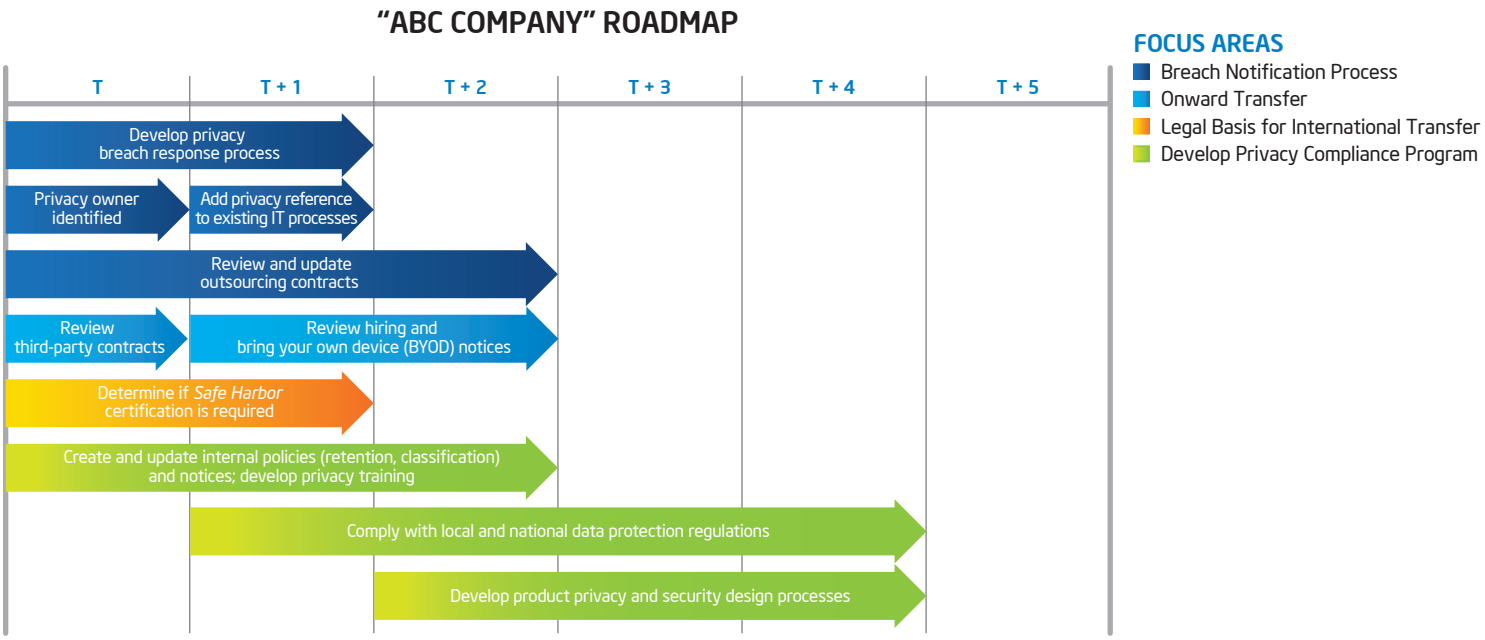

Figure 4. ABC Company's long-term privacy roadmap. The data in this hypothetical case study is based on common issues of standalone subsidiaries. "T" is hypothetical and is not intended to indicate any specific measurement of time. FOR ILLUSTRATION PURPOSES ONLY.

Conclusion

Acquisition of companies, people, or products is a key consideration in any business growth strategy. Whether we fully integrate employees or recognize the companies as standalone subsidiaries, managing the programs associated with privacy is essential to meeting our commitment to protecting the privacy of our employees, customers, and business partners, as well as enabling trust in our technology. With our privacy maturity assessment process in place, we have documented how to assess, measure, and remediate privacy concerns for standalone subsidiaries after the acquisition is completed. This process documents steps each subsidiary can take to reach a maturity level that is realistic for their organization, protects the privacy of subsidiary employees and customers, and sets the stage for improving privacy maturity.

Privacy and protection of personal information will continue to be a concern as we develop new technologies and acquire companies. The privacy maturity assessment process gives us a platform to address these concerns and take a leadership role in establishing privacy policy in our industry.

For More Information

- "Intel Corporate Privacy Rules"

Acronyms

BYOD	bring your own device
GAPP	Generally Accepted Privacy Principles
PbD	Privacy by Design
PMM	privacy maturity model

For more information on Intel privacy practices, visit **www.intel.com/privacy**.

Printed in USA 0913/LSTR/KC/PDF ♻ Please Recycle 329335-001US