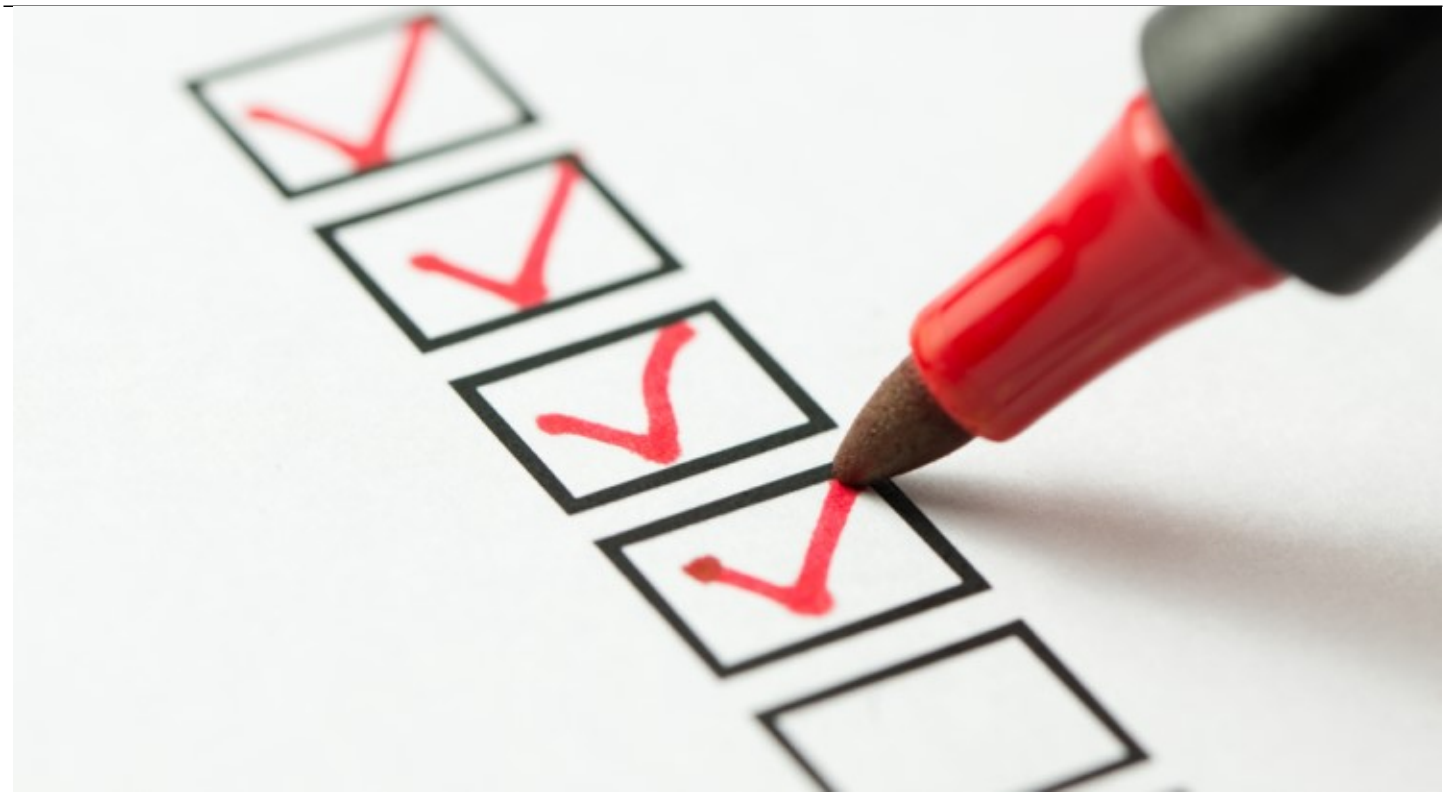
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

5 Questions Corporate Counsel Should Ask About Privacy Assessments

Technology, Privacy, and eCommerce



This is a follow-up to the authors' previous article "5 Questions Corporate counsel Should Ask About Cyber Risk Assessments."

Over the last few years, concerns about privacy have exploded into the public consciousness like never before. The news is filled with reports of social media giants facing huge regulatory fines, or newly implemented data protection laws. The privacy landscape is changing rapidly, from legislation and regulation to public opinion, and companies can no longer rely on piecemeal privacy compliance efforts that focus on highly regulated data or individual business units. How should businesses, and in-house counsel, respond to this brave new world of privacy?

Many businesses are turning to privacy assessments — comprehensive reviews of data collection, processing, and governance conducted under the supervision of counsel. Similar to the previously discussed cybersecurity assessments, privacy assessments combine the best elements of management consulting, technical review, legal risk evaluation, and legal advice to deliver actionable steps toward ensuring a business's privacy program can meet current and future legal risks. Here are five questions you should ask to determine whether and how to conduct a comprehensive privacy assessment in your organization.

1. Why conduct a privacy assessment?

Because the risk of adverse legal action has spiked in recent years. With the EU General Data Protection Regulation (GDPR) in effect since 2018, the California Consumer Privacy Act (CCPA) taking effect in 2020, and the slew of other legislative initiatives at multiple levels globally, organizations that previously only had to worry about one or two privacy laws now face myriad new risks and obligations.

Data that was previously unregulated might now be defined as "personal data" subject to disclosure, access, correction, and other individual rights. And companies face a variety of new requirements impacting internal privacy governance — conducting privacy impact assessments, managing vendor contract requirements and oversight, and developing mechanisms for the exercise and monitoring of individual rights, to name a few.

Privacy assessments help companies come to grips with this ever-changing legal environment. By taking a comprehensive view of an organization's privacy practices and challenges, these assessments help create proactive, agile privacy programs. The goal of performing a comprehensive assessment is not merely to find gaps between an existing program and current laws.

Instead, your goal should be to use the results to help create a privacy and data governance program that can quickly adapt to new products and legal developments by being truly embedded within your organization. An effective privacy assessment produces the birds-eye perspective necessary to develop this type of flexible program.

2. What stakeholders should be included in the privacy assessment?

In order to successfully complete a privacy assessment, it is critical that the right internal stakeholders are involved from the beginning. Every organization is different, but a few common stakeholders include:

- Legal and compliance departments, including in-house and outside counsel as well as any internal employees focused on vendor contracting and risk management;
- Information security, as security and privacy obligations are increasingly overlapping and operationally interdependent;

- Marketing and sales, which are increasingly the target of privacy regulations and therefore crucial to be adequately represented in privacy assessments;
- IT, web administration, and any “shadow IT” divisions handling sensitive organizational data outside of formal information technology, as well as any outsourced service providers on which the organization relies;
- Research and development, to ensure that new products and research are developed with “privacy by design” — having privacy considerations “baked in” from the start of product development; and
- Human resources, as employee data continues to be subject to privacy laws and scrutiny from regulators.

Each of these stakeholders will play an important role in gathering, and then implementing, their respective portions of a privacy assessment.

3. How do you define the scope of a privacy assessment?

It is easy enough to call an assessment “comprehensive,” but ultimately decisions must be made about who and what will fall within the assessment’s scope. Identifying the relevant stakeholders in an important first step for this work, but it is far from the only relevant line of inquiry. Fundamentally, a company must decide on the key regulatory and business goals for privacy, including which state, country, and/or industry frameworks it wants to include in the assessment.

Here is one practice tip that all in-house counsel can appreciate: performing a cost-benefit analysis. Determine your project budget and anticipated work product upfront. These are key considerations that will help you determine a realistic scope for the assessment.

4. How do you translate the assessment final product into action?

Finishing a privacy assessment is the start of the real work: taking the gaps, recommendations, and remediation steps and beginning to remodel and rework your privacy program accordingly. Although the scope of the final work product can vary, most assessments conclude with a roadmap for remediation and building out privacy governance.

In order to effectively implement this roadmap, in-house counsel needs to stay active by engaging the relevant stakeholders and communicating the necessary action items to company employees, officers, and executives.

To whom will you need to talk? Often this task involves “managing up” to the general counsel and company executives to make sure priorities are adequately set. And it usually involves difficult conversations with employees in all the participating business units about changes to the status quo and reorganization of responsibilities.

5. What is your role in overseeing privacy assessments?

Vendors who conduct privacy assessments are not lawyers. So where does counsel fit in? The answer can vary depending on the goals of the assessment, but there are several reasons that in-house or outside counsel should at the least be involved in the initial scoping, direction, and creation of final work product for the assessment. In-house counsel are often best equipped to identify stakeholders and properly scope the engagement (and handle contracting issues) compared with

other internal parties.

Equally as important, engaging counsel will maximize the company's ability to perform the assessment under the attorney-client privilege and work-product doctrine. While a roadmap/gap assessment can be invaluable for privacy compliance, it can also be indispensable evidence for a regulator or plaintiffs' counsel to identify noncompliance — a risk that is particularly significant during the early stages of remediation, where some action items may be left undone.

Protecting the final product under work-product or attorney-client privilege can be an important role of counsel, in-house and out. For this reason, counsel should be involved in written work product, which is ideally viewed in draft form and refined by counsel before consumption by the organizational client.

Conclusion

The role of in-house counsel is to manage legal risk. With increasing regulatory, legal, and public scrutiny over the safekeeping of consumer data, in-house counsel must rise to the challenge in meeting these new obligations. Performing a comprehensive privacy assessment, and following the principles discussed steps above, will help practitioners meet that challenge.

Robert Kang

Professorial Lecturer

George Washington University Law School

Robert Kang is a Professorial Lecturer at the George Washington University Law School, and a consultant. He is also a former in-house legal executive focusing on technology, cybersecurity and national security. Robert serves as a member of the ACC Foundation's Cybersecurity Advisory Board.

Mike Morgan

Partner

McDermott Will & Emery in Los Angeles and Menlo Park

Morgan is co-chair of the firm's Global Privacy & Cybersecurity practice.

Jessi Sawyer

Associate

McDermott Will & Emery’s Global Privacy & Cybersecurity practice

Sawyer counsels clients on compliance with US and international cybersecurity and privacy regulations.

Austin Mooney

Associate

McDermott Will & Emery’s Global Privacy & Cybersecurity practice