TechTarget ComputerWeekly.com E-guide

CW+ Content

The components and objectives of privacy engineering

The components and objectives of privacy engineering:

In the last years, the growing public concern around data usage, the development of strict compliance regulations and the increase of cyber threats have put data privacy as one of the greatest challenges facing enterprises today.

With privacy now at a high-level concern, organizations were prompted to revamp their information architecture, integrating privacy practices into their processes and seeking for professionals to help reevaluate their data strategy.

Privacy experts say more and more companies are hiring full-time privacy engineers or training existing developers on the principles of privacy engineering as a response to these challenges. Apple, Facebook and Google are among the companies staffing teams with these experts.

In this e-guide, read more about the differences and similarities of privacy by design and privacy engineering, the main components and objectives of privacy engineering, and how privacy engineers can help promote innovation and trust among employees and clients.

In this e-guide

The intersection of privacy by design and privacy engineering

Isabella Harford, Assistant Site Editor

Collecting and analyzing massive quantities of data has revolutionized enterprises, helping them reduce costs, streamline processes, minimize inefficiencies and improve customer experiences.

With these benefits, however, comes a major question: How do organizations use data, while simultaneously ensuring the privacy of their employees and customers?

"One of the objectives of privacy by design and privacy engineering is to provide technical and managerial safeguards to privacy, while enabling a high degree of utility," said William Stallings, author of *Information Privacy Engineering and Privacy by Design.*

The proactive processes of privacy by design and privacy engineering foster trust by integrating privacy into the development cycle, rather adding them on pre-deployment.

Compliance regulations are also changing the way privacy is approached. GDPR, for example, mandates privacy by design and privacy by default. CCPA does not explicitly require privacy-by-design practices, but organizations must identify personal data within their designs to ensure users are notified about data use.

With immense quantities of data, growing public concerns and stricter regulations, it's more important than ever for organizations to incorporate privacy into their development cycles.

Here, Stallings, who has more than 30 years of technical experience, discusses how privacy by design and privacy engineering operate together, who is responsible for implementing these processes, how organizations can balance utility and usability with privacy, and more.

Editor's note: This transcript has been edited for length and clarity.

How do privacy by design and privacy engineering operate together?

William Stallings: Privacy by design is the keystone of information privacy management. It assures privacy features are designed into a system before implementation begins. It dictates how privacy is realized at every stage of the systems development lifecycle [SDLC]. Specifically, it involves privacy planning and policy, privacy risk and impact assessment, and the selection of privacy controls.

Privacy engineering covers privacy during the entire lifecycle of information and communication technology systems. This process ensures privacy is incorporated during system integration, privacy tests, evaluations, auditing and incident response. One company that is a leader in privacy engineering is the Mitre Corporation. Mitre developed a free privacy engineering framework and uses the same framework as the basis for its privacy work.

In the SDLC, privacy by design precedes privacy engineering. Privacy by design translates privacy requirements into an implementation plan. Privacy engineering, on the other hand, is the actual implementation, operation and maintenance.

How are these concepts different from how privacy was addressed in the past?

Stallings: The contemporary approach is much more systematic and complex. It borrows concepts such as risk analysis from information security. Two primary trends have converged. First, privacy regulations from government bodies, such as GDPR, and standards, such as ISO 27701, have spelled out more elaborate requirements and dictated specific technical and management approaches to satisfying these requirements.

Second, organizations, particularly midsize and larger organizations, have developed institutional privacy governance policies and personnel to develop privacy policies and procedures. Most organizations now have a chief privacy officer [CPO] and other full-time privacy employees.

As an indicator of the interest in privacy engineering, technology career site Dice.com has more than 400 job openings for privacy engineers as of November 2021.

What is required to change mindsets and achieve the goals of privacy by design and privacy engineering?

Stallings: A workforce with a high level of privacy awareness and appropriate privacy training is as important, if not more important, than any other privacy countermeasure or control. Organizations should have a comprehensive program consisting of four levels:

1. **Awareness.** This set of activities explains and promotes security, establishes accountability and informs the workforce of security news. Participation in security awareness programs is required for all employees.
2. **Cybersecurity essentials.** Intended to develop secure practices in the use of IT resources, this level is needed for all employees involved with any IT systems, including contractors. It provides a universal baseline of key security terms and concepts.
3. **Role-based trainings.** Provide the knowledge and skills specific to an individual's roles and responsibilities. Training helps personnel understand and learn how to perform their security role.
4. **Education and certification.** These integrate all the security skills and competencies of the various functional specialties into a common body of knowledge and add a multidisciplinary study of concepts, issues and principles.

Who is responsible for privacy by design? For privacy engineering?

Stallings: In midsize and large organizations, several people will hold responsibilities in this area. CPOs should have the authority to lead and direct their organization's privacy program. They must ensure compliance with all relevant privacy laws and regulations.

A data protection officer [DPO] has the responsibility to highlight any issues or concerns related to their organization's compliance with privacy regulations and laws.

The DPO is typically responsible for performing internal audits and handling complaints.

The term *privacy leader* is becoming increasingly widespread. In general, a privacy leader is head of privacy compliance and operations. The privacy leader is responsible for developing, implementing and maintaining a privacy program to manage privacy risks, develop and evaluate privacy policies, and ensure compliance with all applicable statutes, regulations and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personal information by programs and information systems.

How can privacy engineers ensure privacy is integrated without disrupting operations?

Stallings: A great deal of research and development has been done to address this issue. The NIST Computer Security Resource Center has a vast collection of documents widely used in industry. These documents include an extensive, well-described set of privacy controls, both computer-based and management-based, as well as documents for privacy engineers.

How can privacy teams quantify utility over privacy and vice versa?

Stallings: Utility and privacy are competing requirements. Any access of data that contains or is derived from personal data has the potential to leak important information. On the other hand, increasing privacy restrictions on information limits the flow of useful information. It is difficult to quantify utility or privacy on a common scale, and thus, more subjective measures must be used, such as by relying on user surveys and on the degree of perceived risk that has been reduced.

How can usability and privacy be balanced?

Stallings: Usability and utility are distinct concepts. Usability refers to the ease of use of privacy features. Utility refers to the functionality available for databases containing personal data with privacy protection in place. Both concepts need to be considered through the design, implementation and operation of IT systems containing personal data. Even more than with utility, usability can generally only be assessed by subjective measures. Again, privacy by design and privacy engineering best practices are intended to ensure a high level of both usability and privacy.

About the author

William Stallings has made a unique contribution to understanding the broad sweep of technical developments in computer security, computer networking and computer architecture. With more than 30 years of experience, he has been a technical contributor, technical manager and executive with several high-technology firms. Stallings has authored 18 textbooks and, counting revised editions, a total of 70 books on various aspects of these subjects. He holds a Ph.D. from MIT in computer science and a Bachelor of Science from Notre Dame in electrical engineering.

Next article

The components and objectives of privacy engineering

Isabella Harford, Assistant Site Editor

Data privacy is one of the greatest challenges facing enterprises today. Growing public concern, *strict compliance regulations* and increased cyber threats are making the integration of privacy into organizations' processes and practices a high priority.

To properly implement privacy, two concepts are emerging: privacy by design and privacy engineering.

"Privacy by design translates privacy requirements into an implementation plan," said William Stallings, author of *Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices.* "Privacy engineering is the actual implementation, operation and maintenance."

In the past, privacy often wasn't considered until right before deployment, if at all. Today, privacy must be *integrated into the entire development* and deployment process. But how?

In this excerpt from Chapter 2 of *Information Privacy Engineering and Privacy by Design,* learn how to get started with privacy engineering, and discover how security risk assessments and risk management contribute to privacy engineering activities.

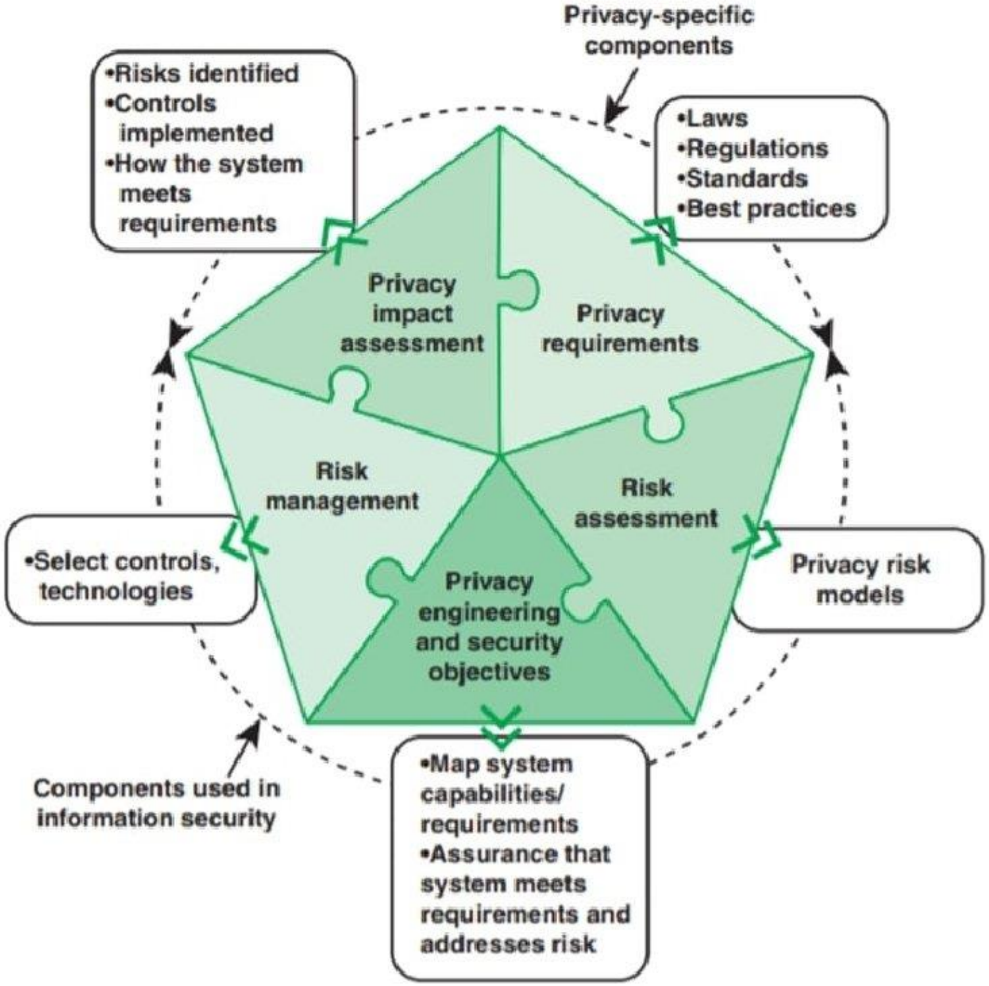
Download a PDF of Chapter 2 to read more on privacy by design, privacy and security, privacy versus utility and usable privacy.

2.3 Privacy Engineering

Privacy engineering encompasses the implementation, deployment, and ongoing operation and management of privacy features and controls in systems. Privacy engineering involves both technical capabilities and management processes. The primary goals of privacy engineering are to:

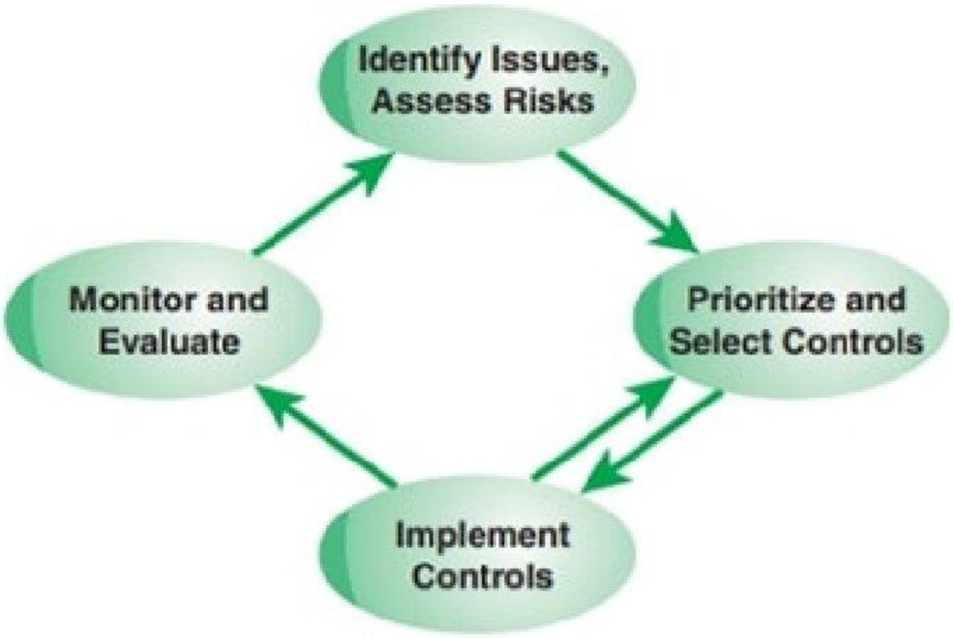
- Incorporate functionally and management practices to satisfy privacy requirements
- Prevent compromise of PII
- Mitigate the impact of breach of personal data

Although Figure 2.1 shows privacy engineering as being distinct from, and following on, PbD, the term ***privacy engineering*** is often used to encompass privacy-related activities throughout the system development life cycle. An example of this is shown in Figure 2.3, adapted from NISTIR 8062.


Privacy-specific components
•Risks identified
•Controls implemented
•How the system meets requirements
•Laws
•Regulations
•Standards
•Best practices
Privacy impact assessment
Privacy requirements
Risk management
Risk assessment
Privacy engineering and security objectives
•Select controls, technologies
Privacy risk models
•Map system capabilities/ requirements
•Assurance that system meets requirements and addresses risk
Components used in information security

As illustrated in Figure 2.3, the NIST document lists five components of privacy engineering -- two that are specific to the privacy engineering process and three that are components typically used in information security management. The components are:

- **Security risk assessment:** A security risk is an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. Security risk assessment is a process that systematically (a) identifies valuable system resources and threats to those resources, (b) quantifies loss exposures (i.e. loss potential) based on estimated frequencies and costs of occurrence. Thus, risk assessment follows two parallel paths. First, for each threat to a resource, the value of the resource is assessed and the potential impact, or cost, if the threat to that resource becomes a successful threat action. Second, based on the strength of a threat, the probability of the threat becoming an actual threat action. Finally, the potential impact of the threat and the likelihood of its success are factors in determining the risk.
- **Risk management:** NIST SP 800-37 (*Risk Management Framework for Information Systems and Organizations*) states that risk management includes a disciplined, structured, and flexible process for organizational asset valuation; security and privacy control selection, implementation, and assessment; system and control authorizations; and continues monitoring. It also includes enterprise-level activities to help better prepare organizations to execute the RMF at the system level. Risk management is an interactive process, as illustrated in Figure 2.4, based on one in ITU-T X.1055 (*Risk management and risk profile guidelines for telecommunication organizations*), consisting of four steps:

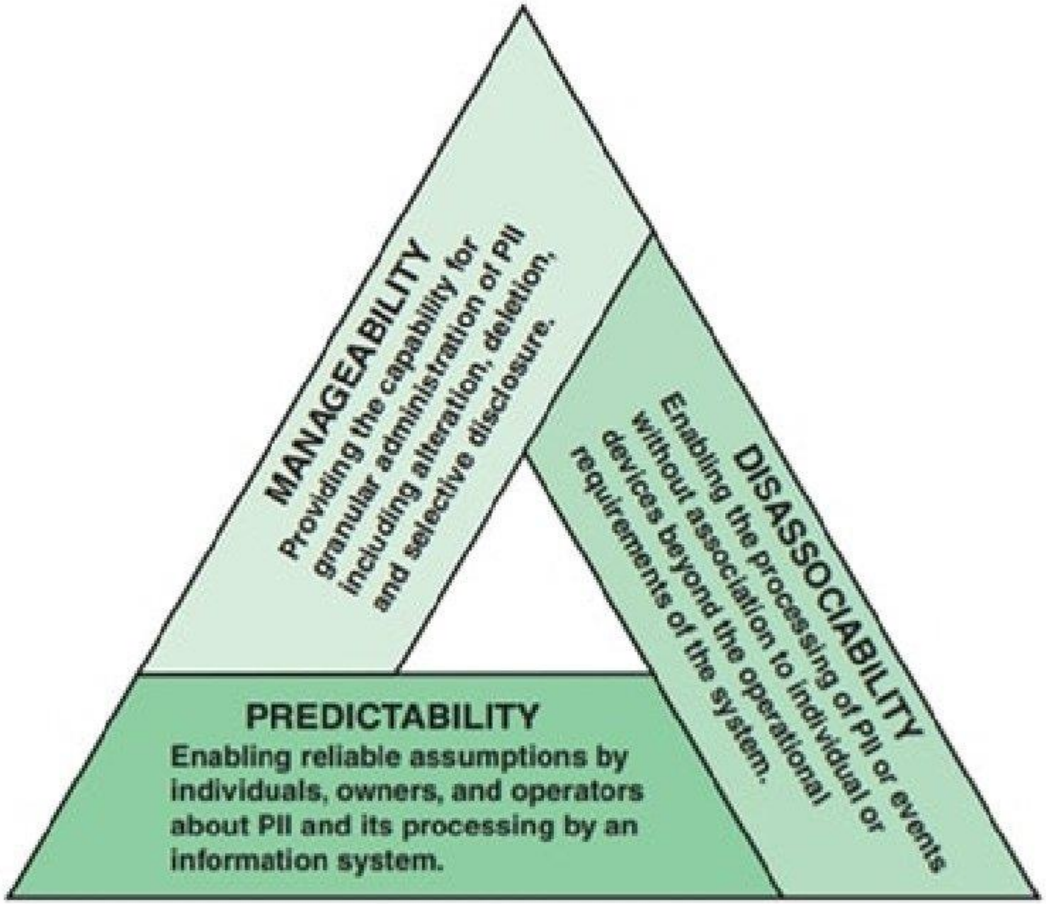


1. Assess risk based on assets, threats, vulnerabilities, and existing controls. From these inputs determine impact and likelihood and then the level of risk. This is the risk assessment component described in the preceding bullet.
2. Identify potential security controls to reduce risk, prioritize their use, and select controls for implementation.
3. Allocate resources, roles, and responsibilities and implement controls.
4. Monitor and evaluate risk treatment effectiveness.

In the context of privacy engineering, the emphasis is on privacy risk and the implementation of privacy controls. Chapter 11 discusses risk management.

- **Privacy requirements:** There are system requirements that have privacy relevance. System privacy requirements define the protection capabilities provided by the system, the performance and behavioral characteristics exhibited by the system, and the evidence used to determine that the system privacy requirements have been satisfied. Privacy requirements are derived from a variety of sources including laws, regulations, standards, and stakeholder expectations. Chapter 3 examines privacy requirements.
- **Privacy impact assessment:** The NIST Computer Security Glossary (https://csrc.nist.gov/ glossary) defines a PIA as an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. In essence, PIA consists of privacy risk assessment followed by a selection of privacy and security controls to reduce the risk. Chapter 11 examines the PIA.
- **Privacy engineering and security objectives:** Information security risk assessment focuses on meeting the common security objectives, including confidentiality, integrity, and availability (Figure 1.1). Similarly, privacy engineering objectives focus on the types of capabilities the system needs in order to demonstrate implementation of an organization's privacy policies and system privacy requirements. NISTIR 8062 proposes three privacy objectives, illustrated in Figure 2.5. Chapter 3 expands on this topic.

In this e-guide


MANAGEABILITY
Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure.
DISASSOCIABILITY
Enabling the processing of PII or events without association to individual or devices beyond the operational requirements of the system.
PREDICTABILITY
Enabling reliable assumptions by individuals, owners, and operators about PII and its processing by an information system.

Next article

How privacy engineers promote innovation and trust

Mary Pratt, Contributor

With privacy now a board-level concern, some of the largest companies have added a new type of specialist to their workforce: the privacy engineer. Apple, Facebook and Google are among the companies staffing teams with these experts. They are just the start.

Privacy experts said more and more companies, including those outside of the tech sector, are hiring full-time privacy engineers or training existing developers on the principles of privacy engineering. This is in response to growing privacy concerns from regulators, executives and customers.

What is a privacy engineer?

A privacy engineer is a trained and skilled specialist who builds privacy into products and services at the technical level. This specialist can bring together the legal and compliance elements of privacy and work them into the organization's systems as they are developed.

"The heart of it lies in ensuring that technical teams understand privacy principles," said Caitlin Fennessy, research director at the International Association of Privacy

Professionals and leader of its privacy engineering initiative. "It's about building privacy into the technology, and that's demanded now by both laws and by people's expectations."

Demand for privacy engineers and the discipline of privacy engineering has grown in recent years. The demand comes as organizations contend with more privacy-related laws and growing customer expectations around enterprise data. Organizations are also experiencing increased pressure to collect and access various types of data to drive digital services, automation and other competitive initiatives.

As a result, organizations need experts who understand regulatory restrictions, technology requirements and -- perhaps most importantly -- how they fuse together.

"Privacy engineering helps limit risk, and it also helps you get ahead of the legal landscape at a time when the legal landscape for privacy is changing so quickly," Fennessy said. "If you start by designing privacy at the start of products and services, you're able to stay ahead."

Privacy as a priority?

Enterprise leaders are paying more and more attention to privacy.

ISACA's "Privacy in Practice 2021: Data Privacy Trends, Forecasts and Challenges" noted: "Boards of directors generally recognize the importance of a strong privacy program. Hefty fines for violating privacy regulations have made headlines, and reputational harm from violating customer privacy can be irreparable." The report further said privacy is not just a cost center, but that it can add value by driving customer trust.

However, the adoption of privacy is not as widespread as it should be. In surveying more than 1,800 of its constituents, ISACA found 52% of privacy professionals believe their board of directors adequately prioritizes privacy. The same report challenged enterprise privacy programs. Nearly 50% of respondents said they had inadequate privacy budgets, compared to 34% who said their privacy budgets were adequately funded.

While 64% cited poor training or a lack of training as a common privacy failure, 53% of respondents listed failure to perform a risk analysis as a fault, and 50% listed bad or nonexistent detection of personal information.

The evolution of privacy professionals

Privacy leaders said they expect those figures to improve as more organizations adopt privacy by design and add privacy engineers to their teams.

Such moves will help enhance enterprise privacy, said Lorrie Cranor, engineering and public policy professor at Carnegie Mellon University and co-director of the master's degree program in privacy engineering.

"When companies first started hiring for privacy, they hired privacy lawyers. But they realized over time that there were a lot of privacy issues that they really needed to solve with technology and not just with policy," Cranor said.

In response, organizations hired technologists with privacy expertise or hired security experts and trained them in privacy. Neither group fully understood the IT component -- either how to use technology to address privacy concerns or how to build digital products and tech services.

Thus, privacy remained an afterthought at many organizations. Product teams and enterprise leaders would often wait until the end of the development cycle, when issues were most difficult to address, to consider security, experts said.

"That's not ideal for incorporating privacy best practices because, by that time, the products have already been worked on for months and it's too late for changes to be made. There's too much pressure to move forward," said Tyrone Jeffress, vice president of engineering and U.S. information security officer at digital consultancy Mobiquity.

The need for privacy engineers who can work privacy into systems earlier in the process finally became more apparent.

"Privacy engineering makes sure organizations are embedding privacy best practices and key principles into the design and development of their solutions," Jeffress said.

Hiring privacy engineers will most certainly improve security, he said, but organizations can still better their privacy posture by training developers in privacy engineering even if they never advance into full-scale privacy engineers.

"You don't necessarily need the privacy officer or a privacy expert in every development meeting, but you do need someone at the get-go who is a privacy champion," he said.

Getting more CW+ exclusive content

Images; Fotalia