CALVIN
INSTITUTE OF TECHNOLOGY
God's People for God's Glory

Keamanan dan Pengelolaan Data

Minggu 3

Dosen Pengajar: Steven Bandong S.Si., M.T

Tata Tertib Kelas

- Dosen dan mahasiswa bersama-sama secara aktif membentuk komunitas belajar yang baik
- Silahkan bertanya kalau ada yang tidak dimengerti
- Laporan / program / tugas apa pun yang anda serahkan harus jelas beda dan jelas adalah kontribusi anda atau kelompok dan bukan dari orang lain (misnya: tugas proyek).

Topik Minggu Ini dan Capaian Pembelajaran

Topik minggu ini:

1. Menjelaskan konsep privasi
2. Menjelaskan Privasi by Design dan Privasi by Engineering

Indikator penilaian:

1. Ketepatan dalam menjelaskan konsep privasi
2. Ketepatan menjelaskan Privasi by Design dan Privasi by Engineering

Information Privacy Concepts

1980s–1990s

- 1984, the UK Passes the Data Protection Act
- 1995, the Data Protection Directive is Passed in the EU

2000

European Commission Decides

- U.S. Companies Complying With a Self-Certification Program Meets EU Req.'s ("**Safe Harbor Scheme**"); and
- Allows to Transfer Data From EU to U.S. ("**Safe Harbor Decision**")

2001

- **Sept. 11** Terrorist Attack
- **Oct. 26** the U.S. Congress Passes and President Bush Signs into Law the U.S. Patriot Act Which Enables the U.S. Gov't to Obtain Stored Data From any Company Without Court Order

2004–2005

- Canada Enacts PIPEDA
- Canada's British Columbia Privacy Commissioners Begins Exams U.S. Patriot Act; Creates Requirements
- Complaints From Canadian Imperial Bank of Commerce VISA Customers re: Cardholder Agreement Saying Bank is Using U.S. Providers and Data is Subject to U.S. Patriot Act

2008–2010

- **Dec. 2008**, Chris Connelly of Galexia, an Australian Consultancy Firm, Reports Problems With Safe Harbor.
- **Feb. 25, 2010**, the European Commission Adopts Standard Contractual Clauses to/From Countries Found "inadequate".

2011

- **April–June 2011** Zack Whittaker Reports on Google and UK Universities, and Microsoft
- **Oct. 2011** Dutch Minster of Safety and Justice Bans U.S. Cloud Providers But EU Struggles With Whether Ban Violates EU Competition and Internal Market Rules and WTO Govt's Procurement Agmt

June 2013

- Edward Snowden Begins to Reveal U.S. Surveillance Activities to the Guardian Including Project TEMPORA (UK's GCHQ Gathering and Sharing Intel Data Via Fiber Optics
- The German Member of European Parliament Calls for Infringement Proceedings Against U.K. (Article 16 of Treaties of EU)

Oct. 6, 2013

Austrian attorney, Max Schrems, files complaints with Ireland's Data Protection Authority against Facebook alleging Irish data transfer to U.S. inadequate in light to surveillance and no ability for EU citizen to control data.

Key Privacy Terminology

Privacy:

- Hak untuk "tidak diganggu" — artinya, bebas dari pengamatan atau gangguan.
- Kemampuan untuk mengontrol informasi yang dirilis tentang diri seseorang.

- Stanford Encyclopedia of Philosophy

Key Privacy Terminology

Information Privacy:
Hak individu untuk mengontrol atau memengaruhi informasi yang berkaitan dengan mereka, bagaimana informasi itu dikumpulkan, disimpan, dan kepada siapa serta bagaimana informasi itu diungkapkan.
- ITU-T X.800 (Security Architecture for Open Systems Interconnection)

Key Privacy Terminology

Information Privacy:
membuat informasi pribadi seseorang tidak tersedia untuk pihak-pihak yang seharusnya tidak memiliki informasi tersebut
- U.S. National Research Council report
(At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues)

informasi pribadi apa saja yang tidak boleh dishare?

Key Privacy Terminology

Privasi Informasi dan PII

PII➔personally identifiable information

Informasi yang dapat digunakan untuk mengidentifikasi atau melacak identitas seseorang

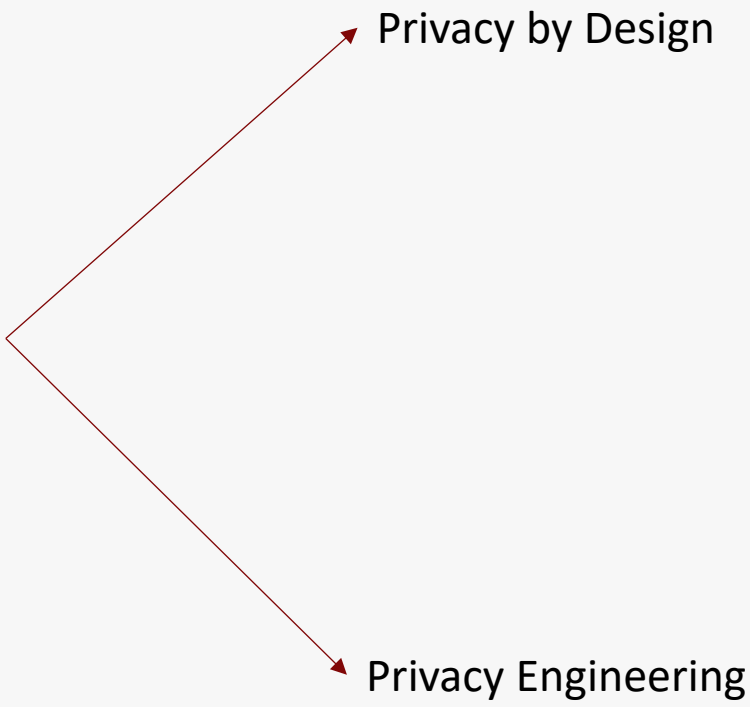

Why it is not advisable to share your ID card online.
ID
EXPLAINING WHY.COM

Key Privacy Terminology

Contoh PII menurut NIST SP 80-122 meliputi:

- Nama lengkap, nama gadis ibu, atau nama alias.
- Nomor identifikasi pribadi seperti nomor jaminan sosial, nomor paspor, atau nomor rekening.
- Informasi alamat seperti alamat rumah atau email.
- Informasi aset seperti IP Addres atau MAC Addres.
- Nomor telepon, termasuk nomor ponsel dan bisnis.
- Karakteristik pribadi seperti foto, sidik jari, atau data biometrik lainnya.
- Informasi tentang properti pribadi seperti nomor registrasi kendaraan.
- Informasi yang terkait dengan individu, seperti tempat lahir, agama, pekerjaan, pendidikan, atau informasi kesehatan.

Key Privacy Terminology

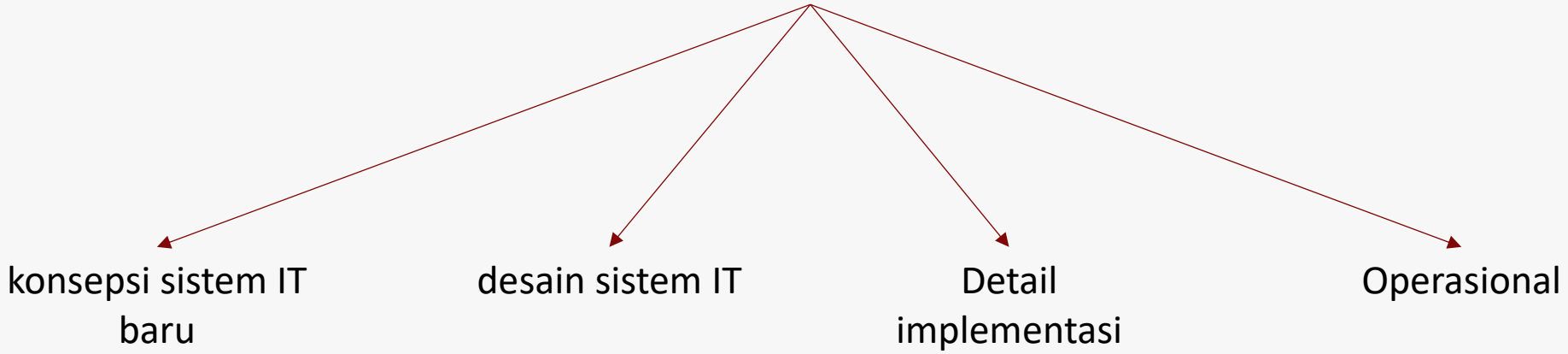


Key Privacy Terminology

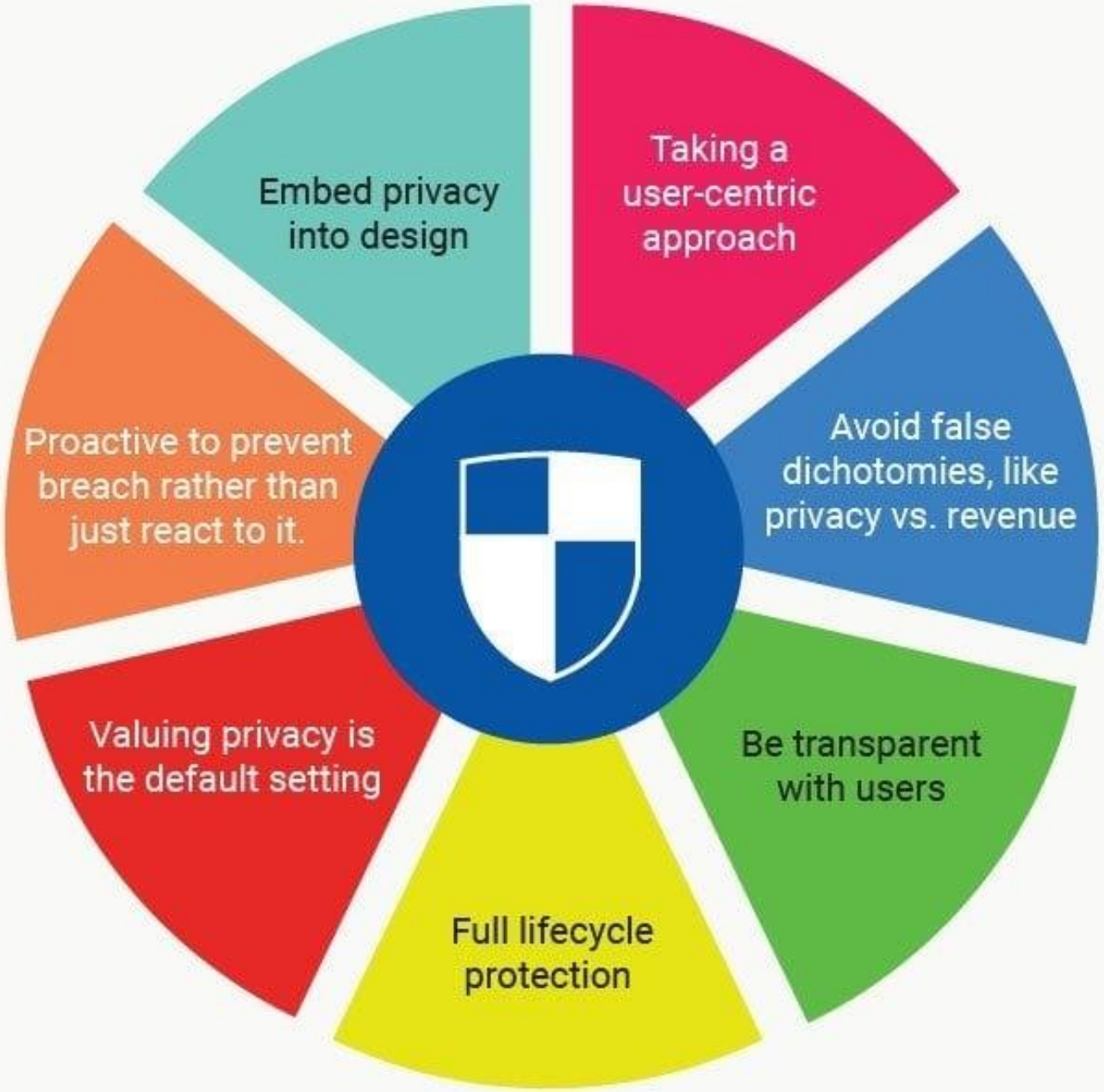
Privacy by Design

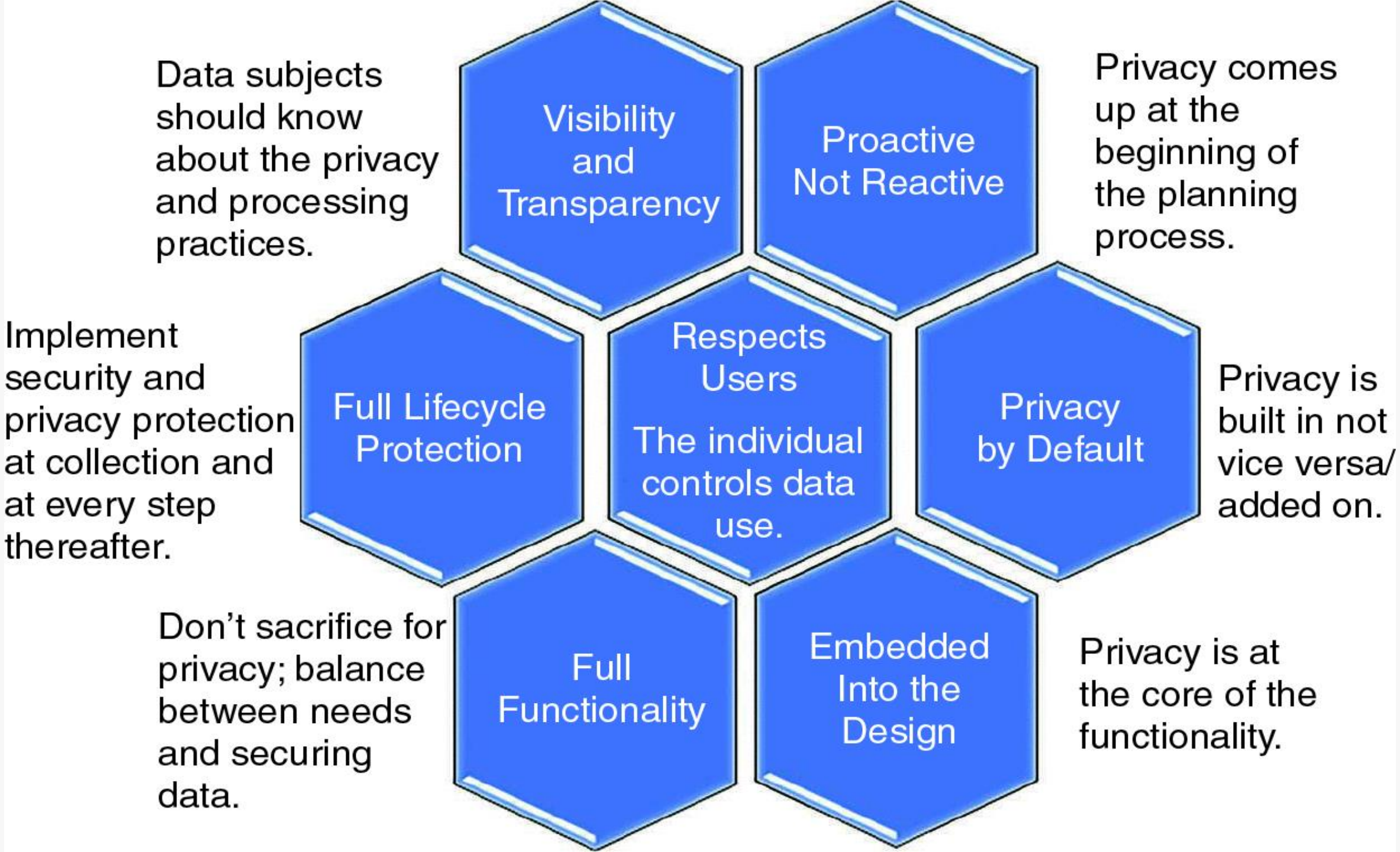
mempertimbangkan privasi sepanjang proses pengembangan sistem, mulai dari konsepsi sistem IT hingga desain sistem secara detail, implementasi, dan operasionalnya.

Praktik yang mempertimbangkan langkah-langkah perlindungan privasi sejak tahap desain sistem.
-**ISO 29100** (Information Technology—Security Techniques—Privacy Framework)



Privacy by Design




Data subjects should know about the privacy and processing practices.
Visibility and Transparency
Proactive Not Reactive
Privacy comes up at the beginning of the planning process.
Implement security and privacy protection at collection and at every step thereafter.
Full Lifecycle Protection
Respects Users
The individual controls data use.
Privacy by Default
Privacy is built in not vice versa/ added on.
Don’t sacrifice for privacy; balance between needs and securing data.
Full Functionality
Embedded Into the Design
Privacy is at the core of the functionality.

Key Privacy Terminology

Privacy Engineering

Privacy engineering is an emerging field that develops the tools, methodologies, and processes for meeting the privacy requirements and expectations of regulators and customers.
-**https://www.computer.org/csdl/magazine/co/2022/10/09903879/1H0G8Iq3qDu**

Key Privacy Terminology

Privacy Engineering

pertimbangan privasi selama siklus hidup sistem ICT (information and communications technology), sehingga privasi menjadi bagian integral dari fungsinya.

privacy engineering adalah disiplin khusus dalam *systems engineering* yang berfokus pada:
-**NISTIR 8062** (An Introduction to Privacy Engineering and Risk Management in Federal Systems)

bertujuan mengurangi risiko yang terkait dampak privasi dan memungkinkan pengambilan keputusan yang efisien tentang kontrol dan sumber daya

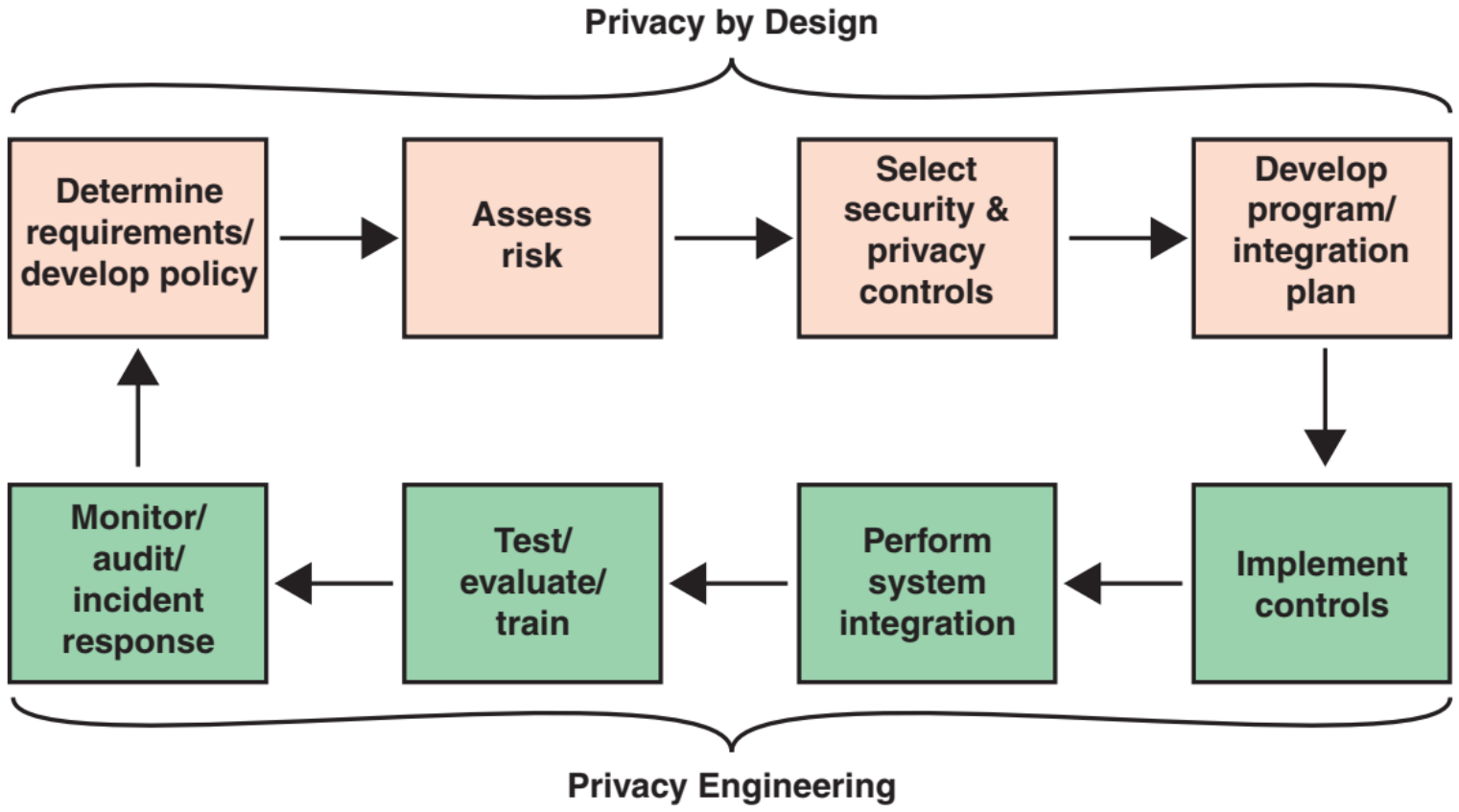
Hubungan antara Privacy by Design dan Privacy Engineering

prinsip Privacy by Design harus diterjemahkan ke dalam metodologi Privacy Engineering agar dapat diimplementasikan dengan baik.
-**European Data Protection Supervisor (EDPS)**

Hubungan antara Privacy by Design dan Privacy Engineering

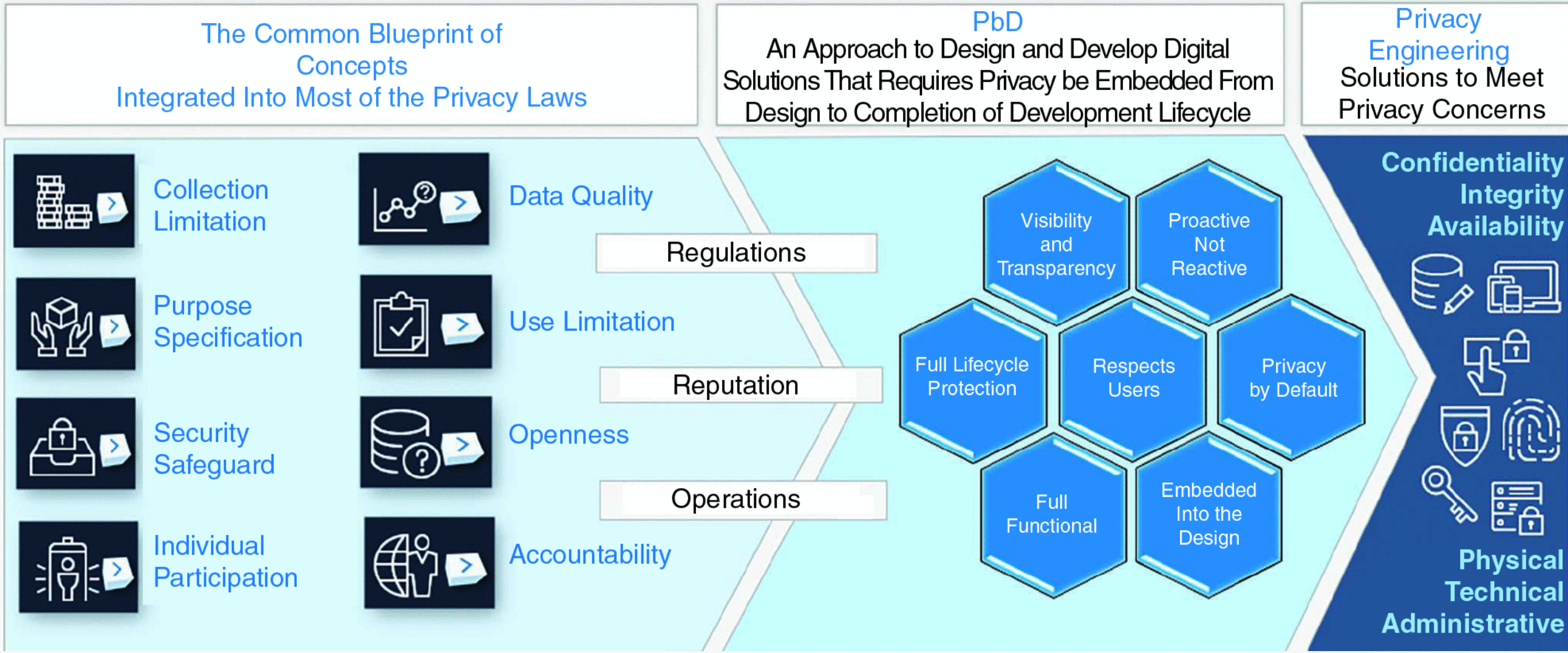
Alur mengintegrasikan perlindungan privasi ke dalam sistem informasi yang dikembangkan oleh organisasi

Fokus ke desain : menentukan kebutuhan dan cara memenuhinya



Information Privacy Development Life Cycle

implementasi dan operasional fitur privasi sebagai bagian dari sistem secara keseluruhan

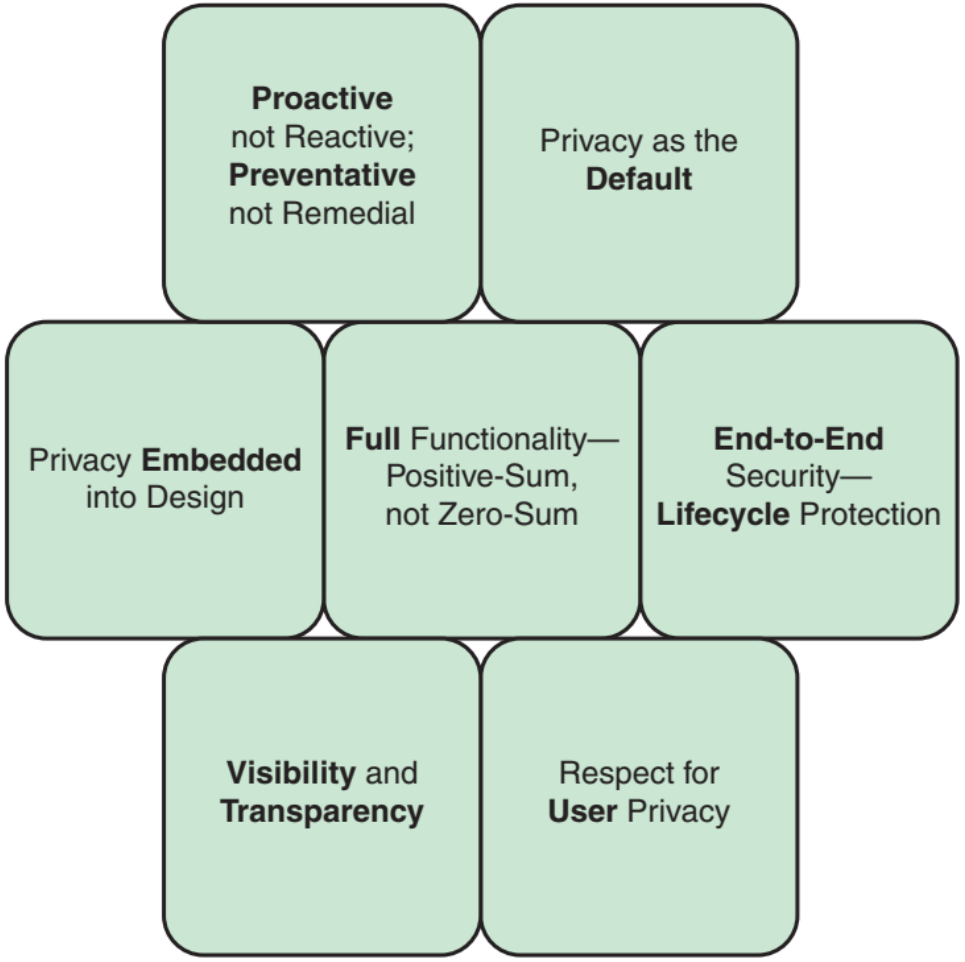

The Common Blueprint of Concepts Integrated Into Most of the Privacy Laws
PbD
An Approach to Design and Develop Digital Solutions That Requires Privacy be Embedded From Design to Completion of Development Lifecycle
Privacy Engineering
Solutions to Meet Privacy Concerns
Collection Limitation
Purpose Specification
Security Safeguard
Individual Participation
Data Quality
Use Limitation
Openness
Accountability
Regulations
Reputation
Operations
Visibility and Transparency
Proactive Not Reactive
Full Lifecycle Protection
Respects Users
Privacy by Default
Full Functional
Embedded Into the Design
Confidentiality
Integrity
Availability
Physical
Technical
Administrative

Privacy by Design

memastikan fitur-fitur privasi dirancang ke dalam suatu sistem sebelum implementasi dimulai

Prinsip-prinsip berikut diadopsi sebagai resolusi oleh banyak pembuat kebijakan pada Konferensi Internasional ke-32 Data Protection and Privacy Commissioners

Prinsip-prinsip PbD ini adalah persyaratan bagaimana cara sistem dirancang dan diimplementasikan.

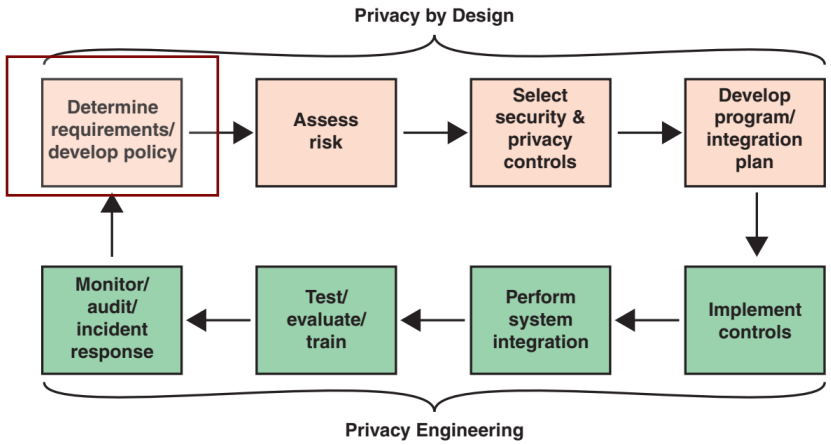


Foundational Principles of Privacy by Design

CALVIN INSTITUTE OF TECHNOLOGY

Privacy by Design

Requirements and Policy Development



Pelaku Utama:
Pemilik Sistem

Identifikasi persyaratan privasi yang menjadi dasar perencanaan

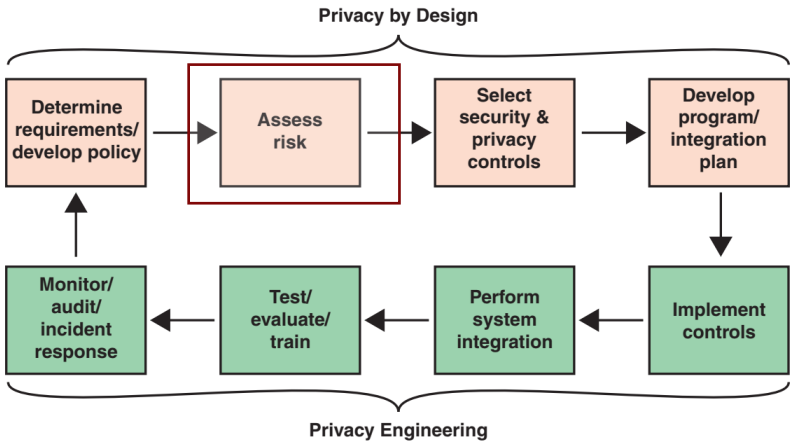
Regulasi

Standar

Komitmen kontraktual organisasi

Privacy by Design

Privacy Risk Assessment



Tujuan:
Membantu menentukan anggaran untuk melindungi privasi dan mengurangi risiko pelanggaran.

Elemen Penilaian

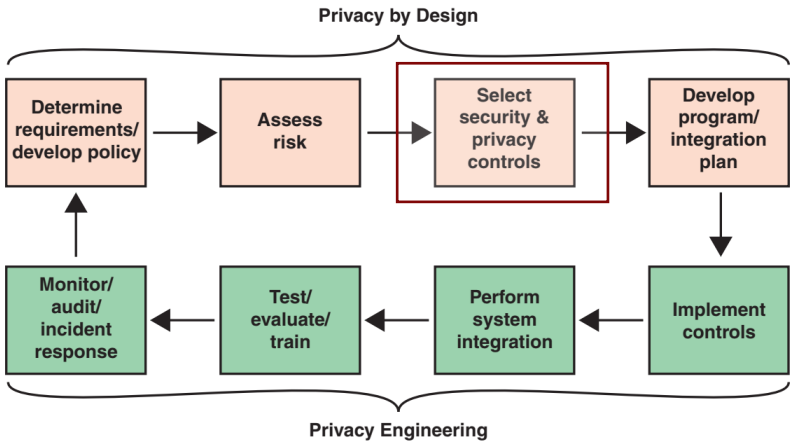
- Aset terkait privasi
- Ancaman privasi
- Kerentanan privasi
- Kontrol privasi

Langkah Penilaian

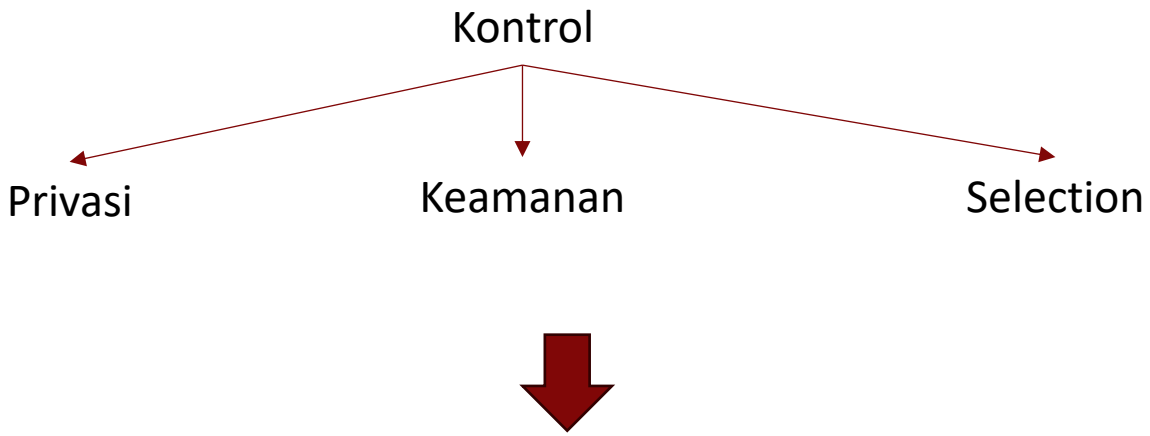
- Menentukan dampak
- Menentukan kemungkinan insiden privasi
- Menentukan tingkat risiko

Privacy by Design

Privacy and Security Control Selection



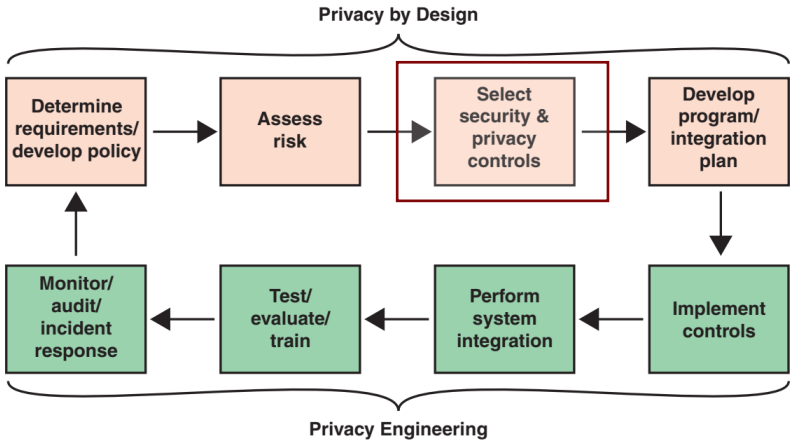
Kontrol:
langkah-langkah, mekanisme, atau tindakan yang diterapkan untuk melindungi privasi dan keamanan data



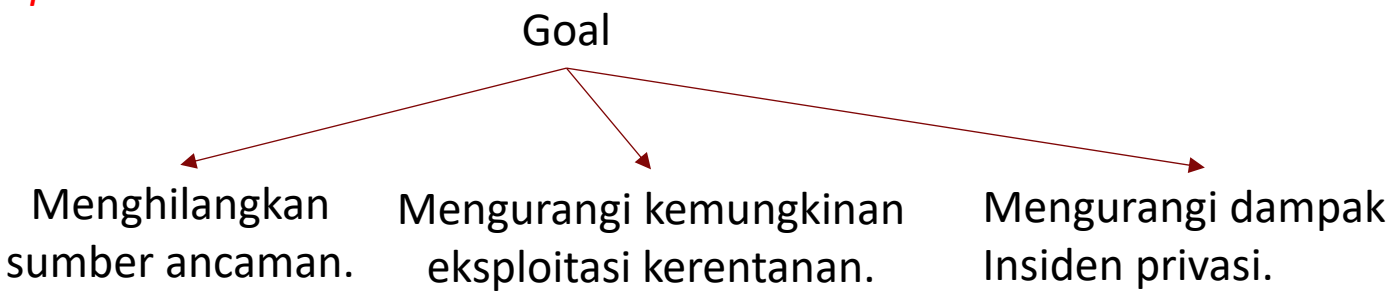
Perlindungan privasi PII (Personally Identifiable Information)

Privacy by Design

Privacy and Security Control Selection



Privacy Control:
langkah teknis, fisik, dan administratif (atau manajerial) yang diterapkan dalam sebuah organisasi untuk memenuhi standar privasi

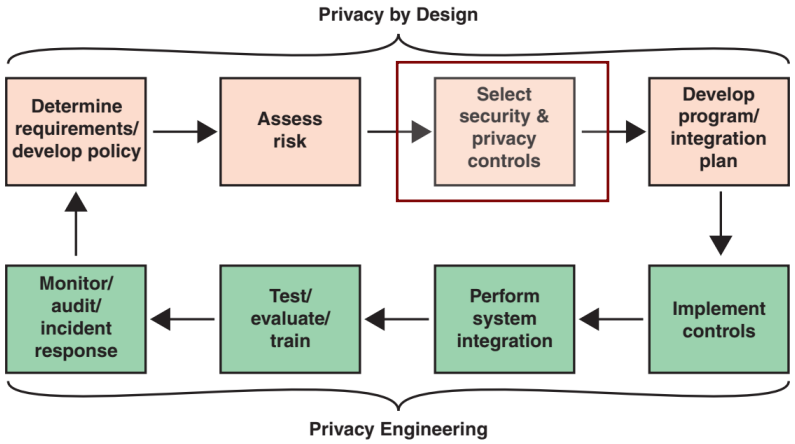


Panduan dalam pemilihan kontrol:

- NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations)
- ISO 29151 (Code of Practice for Personally Identifiable Information Protection)

Privacy by Design

Privacy and Security Control Selection



Security Control :
tindakan untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi dalam suatu sistem atau organisasi.

Contoh: mekanisme pengontrolan akses dapat digunakan untuk membatasi akses ke PII yang disimpan dalam basis data

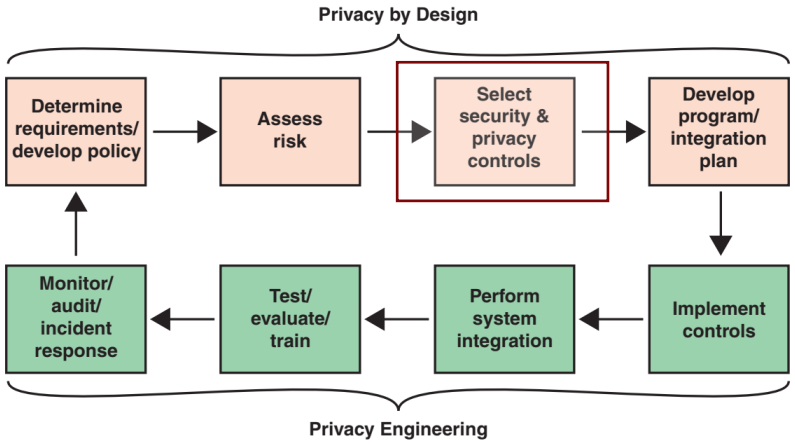
Ini termasuk Privacy Control atau Security Control?

Panduan dalam pemilihan kontrol:

- NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations)
- ISO 29151 (Code of Practice for Personally Identifiable Information Protection)

Privacy by Design

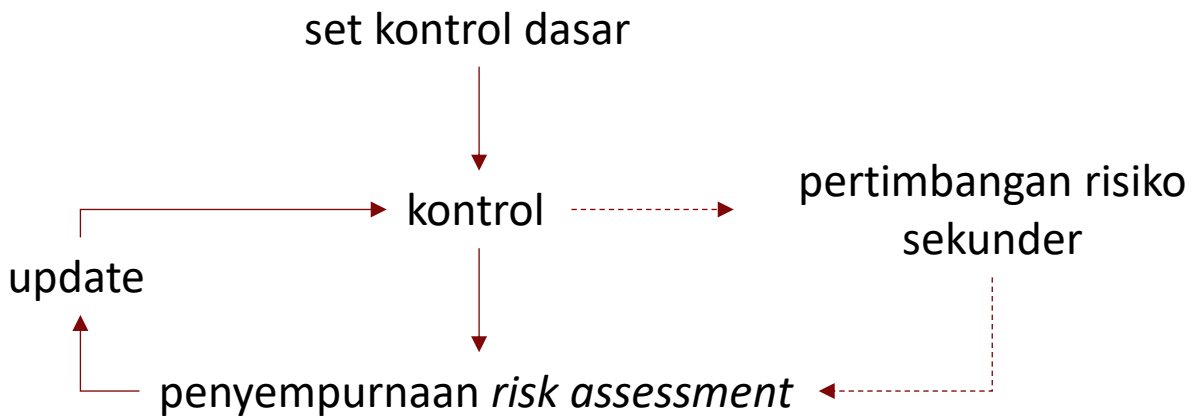
Selection Process



Selection Process:

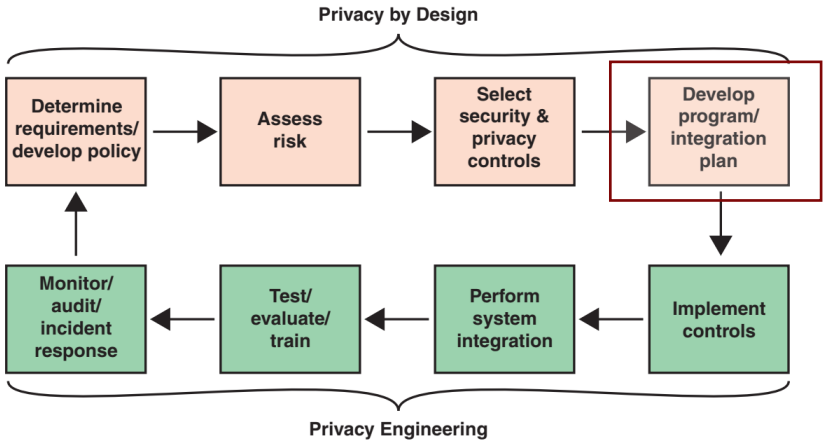
Pemilihan dan dokumentasi privacy and security control harus disinkronkan dengan aktivitas risk assessment.

Tahapan Pemilihan



Privacy by Design

Privacy Program and Integration Plan



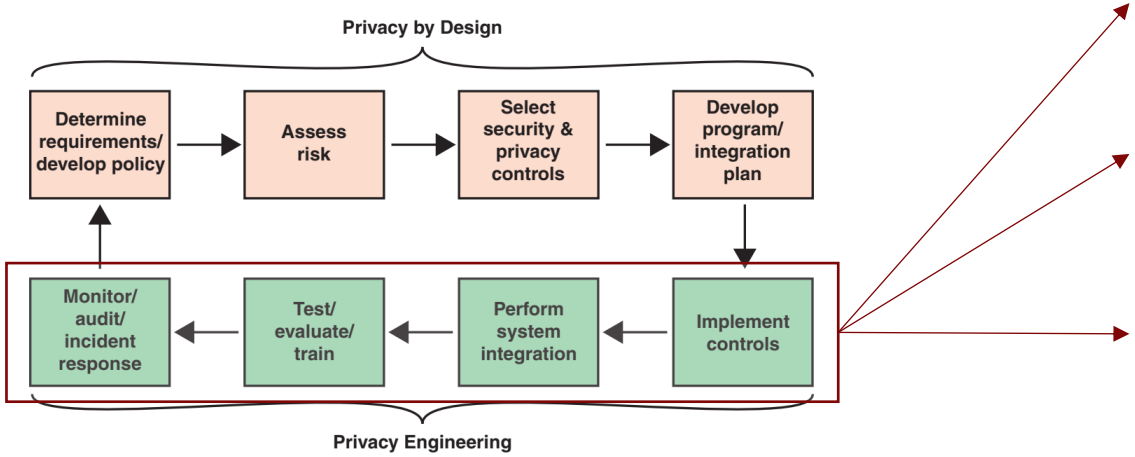
Meliputi:

- Mengidentifikasi peran privasi utama yang akan aktif selama desain dan implementasi sistem.
- Mengidentifikasi standar dan regulasi yang berlaku.
- Mengembangkan rencana keseluruhan untuk pencapaian privasi selama pengembangan sistem.
- Memastikan semua pemangku kepentingan memiliki pemahaman yang sama, termasuk implikasi, pertimbangan, dan persyaratan privasi.
- Menjelaskan persyaratan (*requirements*) untuk mengintegrasikan kontrol privasi dalam sistem dan proses untuk mengoordinasikan kegiatan rekayasa privasi dengan pengembangan sistem secara keseluruhan.

Output yang diperoleh:

- Skema integrasi privasi yang memberikan detail tentang di mana, dalam sistem, privasi diimplementasikan dan, jika berlaku, di mana mekanisme privasi digunakan bersama oleh beberapa layanan atau aplikasi.
- Daftar layanan bersama dan risiko bersama yang dihasilkan.
- Identifikasi kontrol umum yang digunakan oleh sistem.

Privacy by Engineering



implementasi

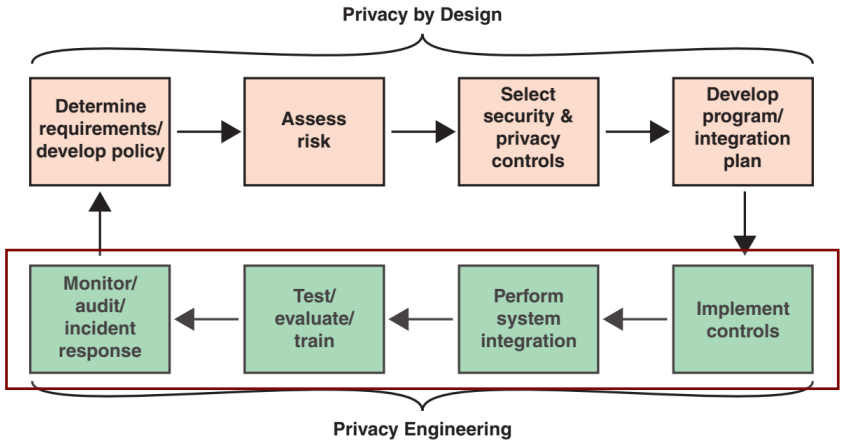
integrasi

Pengelolaan berkelanjutan

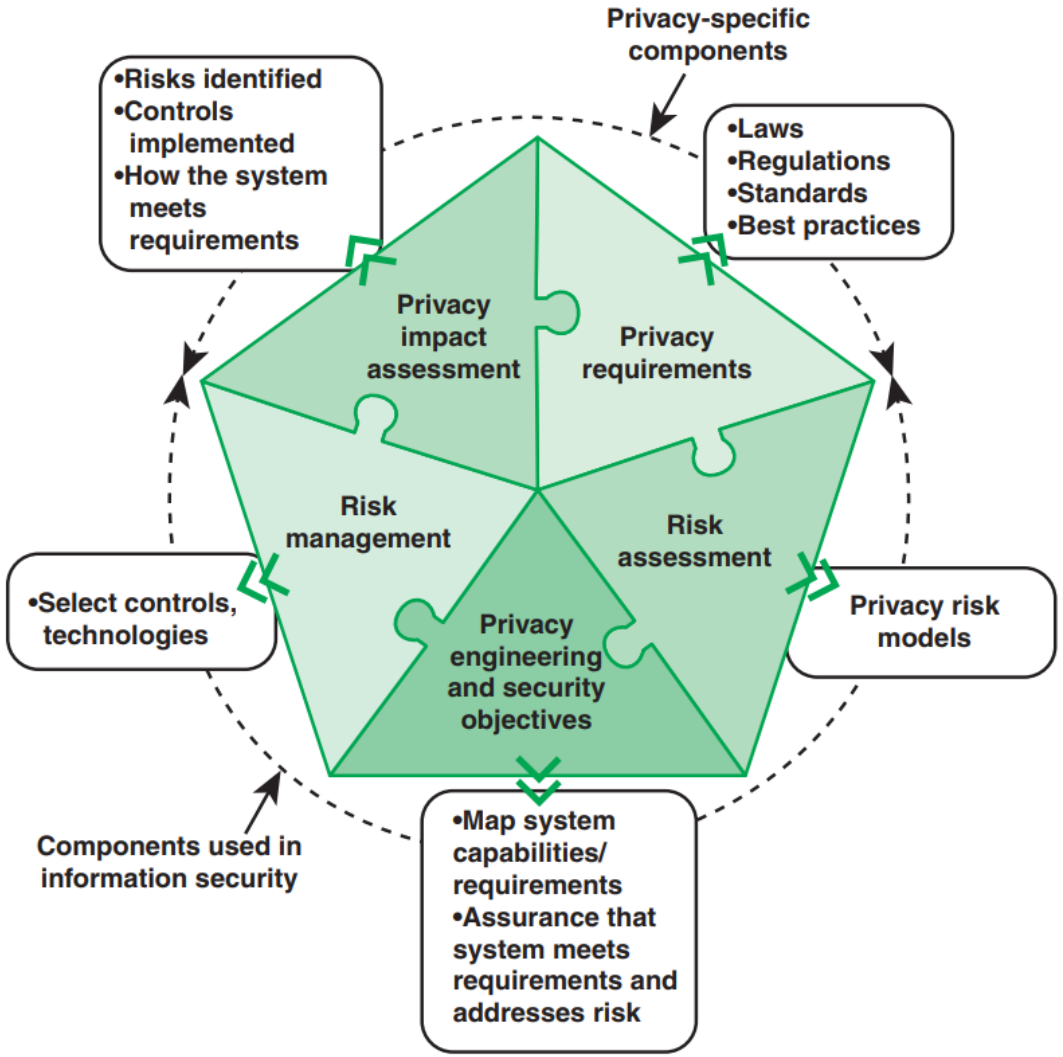
Tujuan utama rekayasa privasi

- Mengintegrasikan fungsionalitas dan praktik manajemen untuk memenuhi persyaratan privasi
- Mencegah kompromi atas PII (Informasi Identitas Pribadi)
- Mengurangi dampak pelanggaran data pribadi

Privacy by Engineering

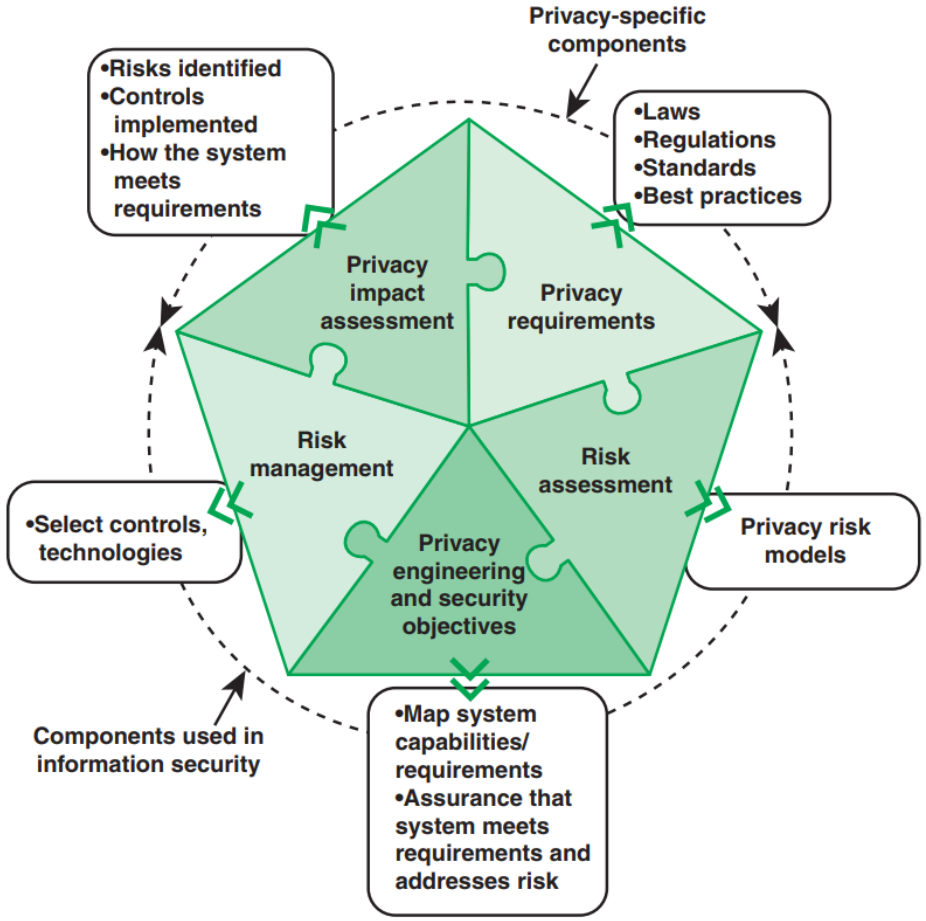


rekayasa privasi sering mencakup juga privacy by design

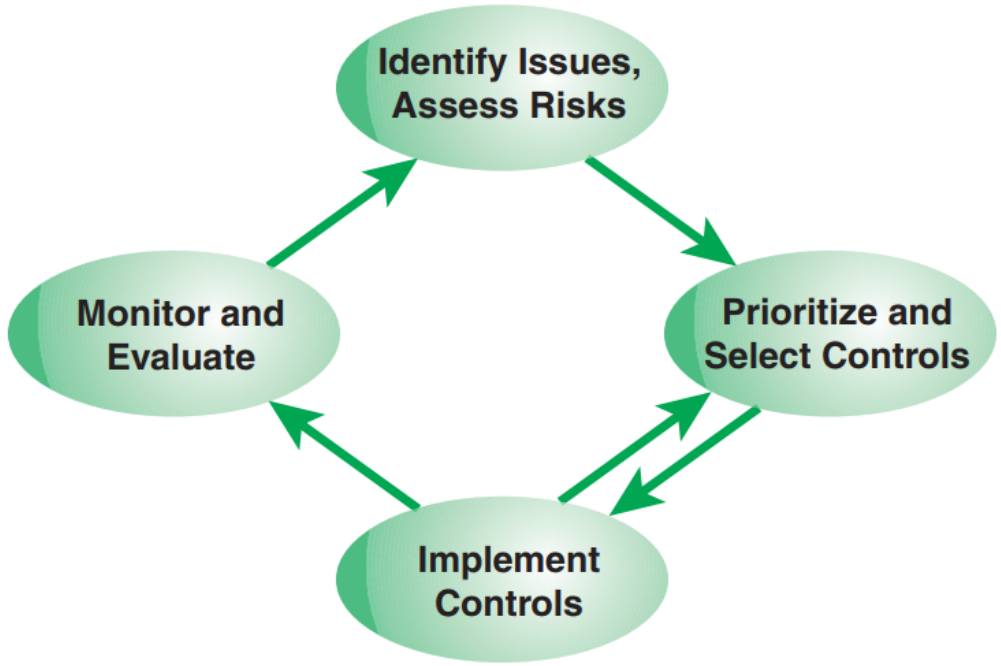


Components of Privacy Engineering (NISTIR 8062)

Privacy by Engineering

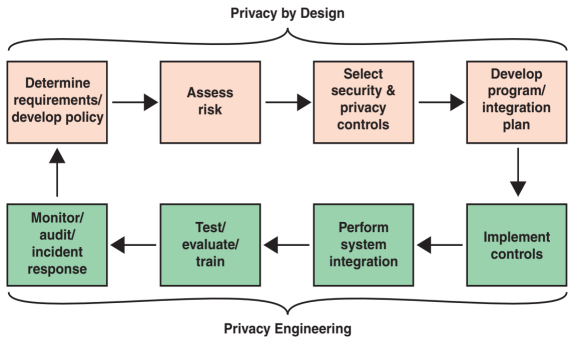


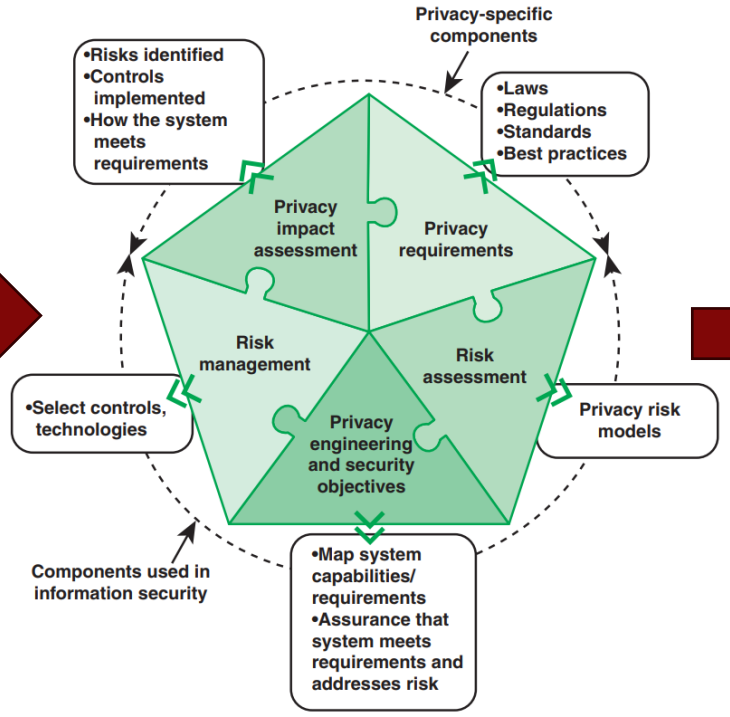
Components of Privacy Engineering (NISTIR 8062)



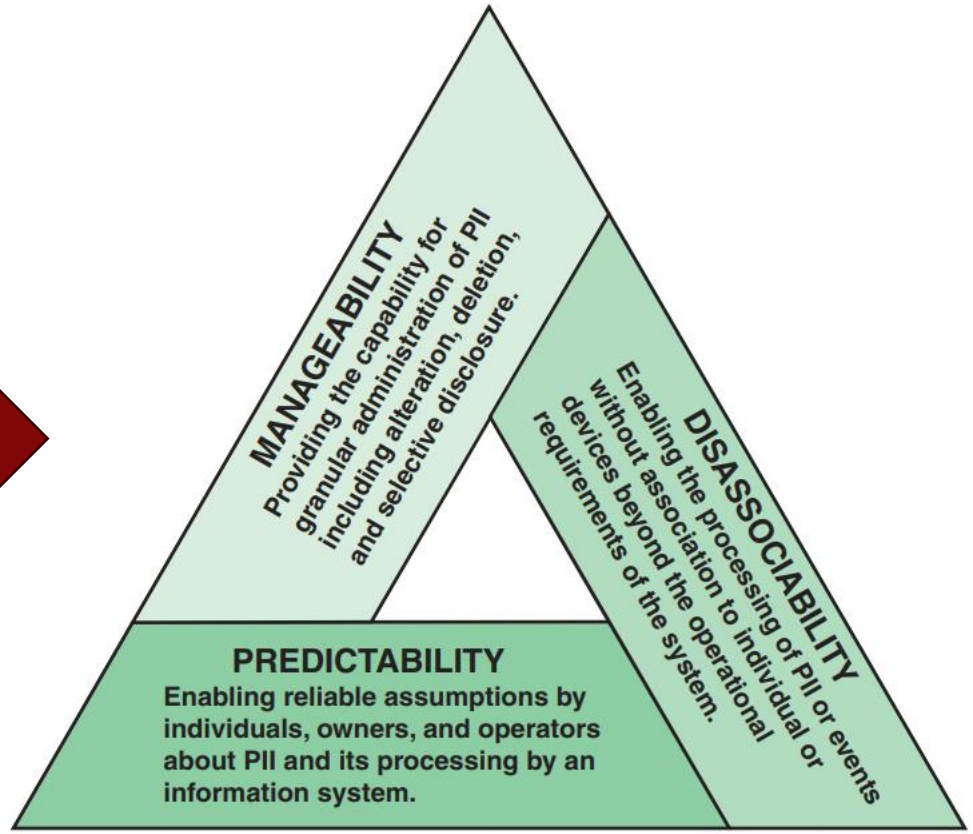
Risk Management Cycle

Privacy by Engineering





Components of Privacy Engineering (NISTIR 8062)

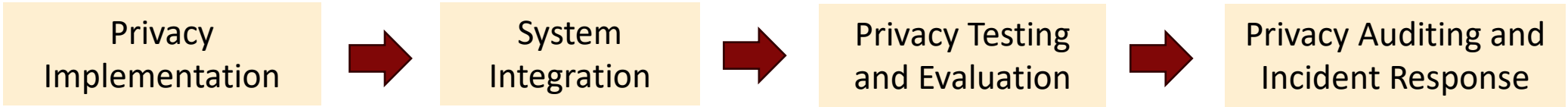


Privacy Engineering Objectives

CALVIN INSTITUTE OF TECHNOLOGY

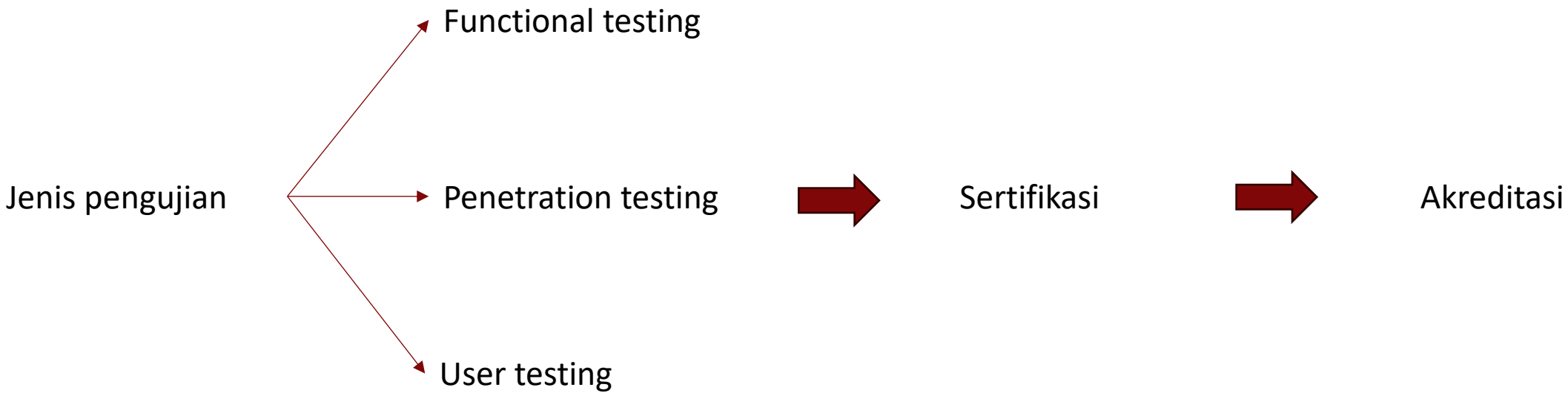
Privacy by Engineering

Tahapan Privacy Engineering



Privacy by Engineering

Privacy Testing and Evaluation



Privacy by Engineering

Privacy Auditing and Incident Response

Sistem dan produk yang telah dioperasikan dimonitor untuk memastikan kepatuhannya terhadap persyaratan privasi.

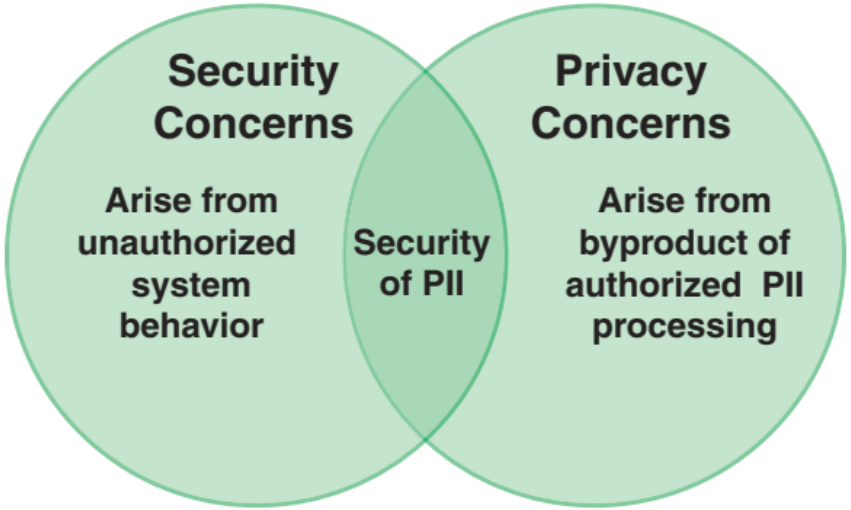
Audit

pemeriksaan independen untuk memastikan kepatuhan terhadap kontrol dan prosedur operasional serta memberikan rekomendasi perbaikan.

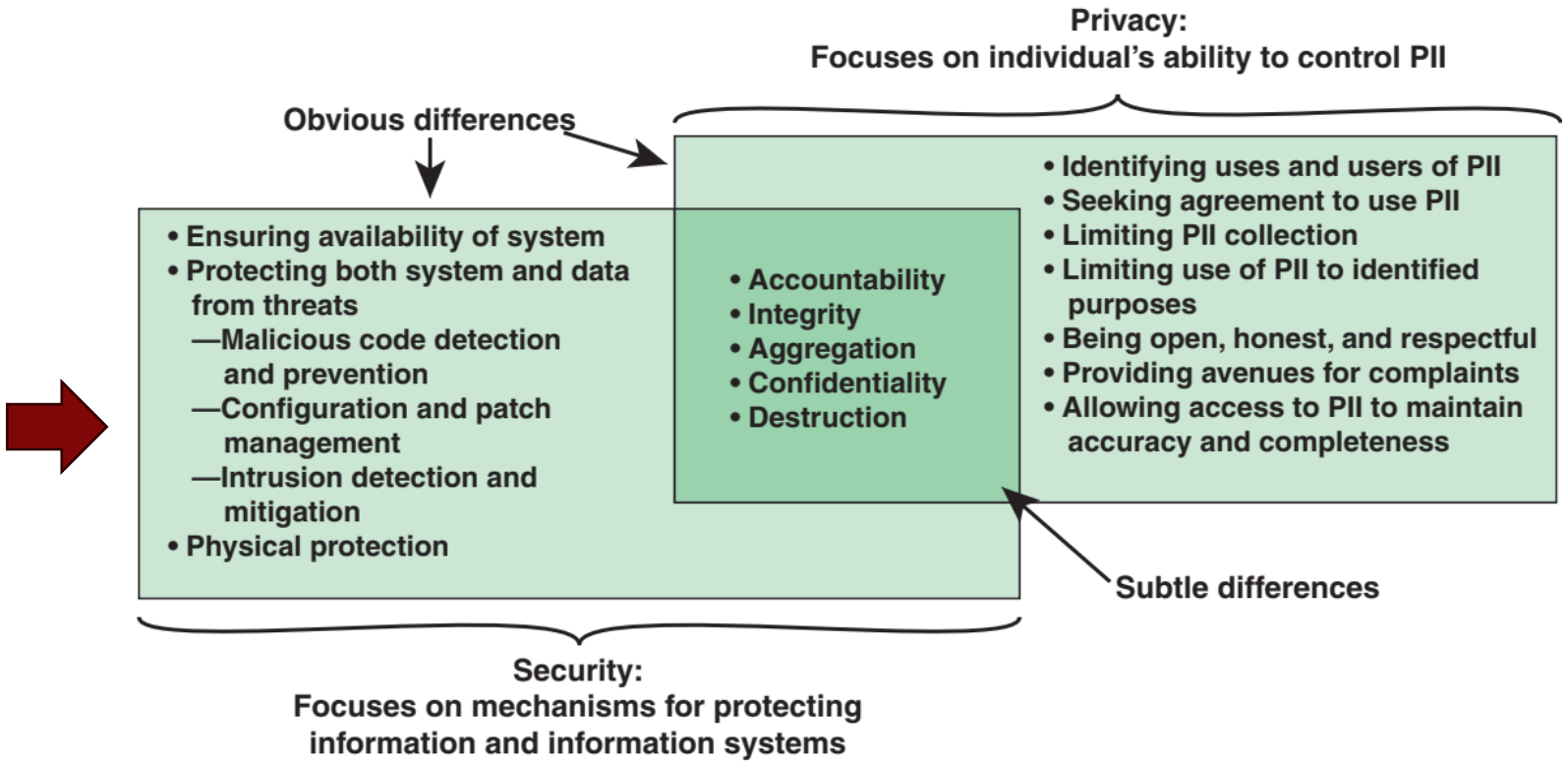
Tanggapan Insiden

proses penanganan dan mitigasi insiden keamanan IT dengan menerapkan kebijakan serta praktik yang tepat.

Privacy and Security



Overlap Between Information Security and Privacy



Privacy and Security Objectives

Privacy and Security

	Security	Privacy
Accountability	Focuses on tracking an individual's actions and manipulation of information	Focuses on tracking the trail of PII disclosure
Integrity	Protects against the corruption of data by authorized or unauthorized individuals	Seeks to ensure that inaccurate PII is not used to make an inappropriate decision about a person
Aggregation	Focuses on determining the sensitivity of derived and aggregated data so that appropriate access guidance can be defined	Dictates that aggregation or derivation of new PII should not be allowed if the new information is neither authorized by law nor necessary to fulfill a stated purpose
Confidentiality	Focuses on processes and mechanisms (e.g., authenticators) that prevent unauthorized access	Focuses on ensuring that PII is only disclosed for a purpose consistent with the reason it was collected
Destruction	Focuses on ensuring that the information cannot be recovered once deleted	Addresses the need for the complete elimination of collected information once it has served its purpose

Privacy and Security

Trade-Offs Antara Keamanan dan Privasi

langkah-langkah tertentu yang diambil untuk meningkatkan
keamanan siber juga dapat melanggar privasi

National Research Council berjudul *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*

CALVIN
INSTITUTE OF TECHNOLOGY
God's People for God's Glory

Terima Kasih
Tuhan Memberkati