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

Keamanan dan Pengelolaan Data

Minggu 4

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 Privasi by Design dan Privasi by Engineering
2. Panduan dan persayaratan Privasi Informasi

Indikator penilaian:

1. Ketepatan dalam menjelaskan konsep privasi
2. Memahami panduan dan persayaratan Privasi Informasi

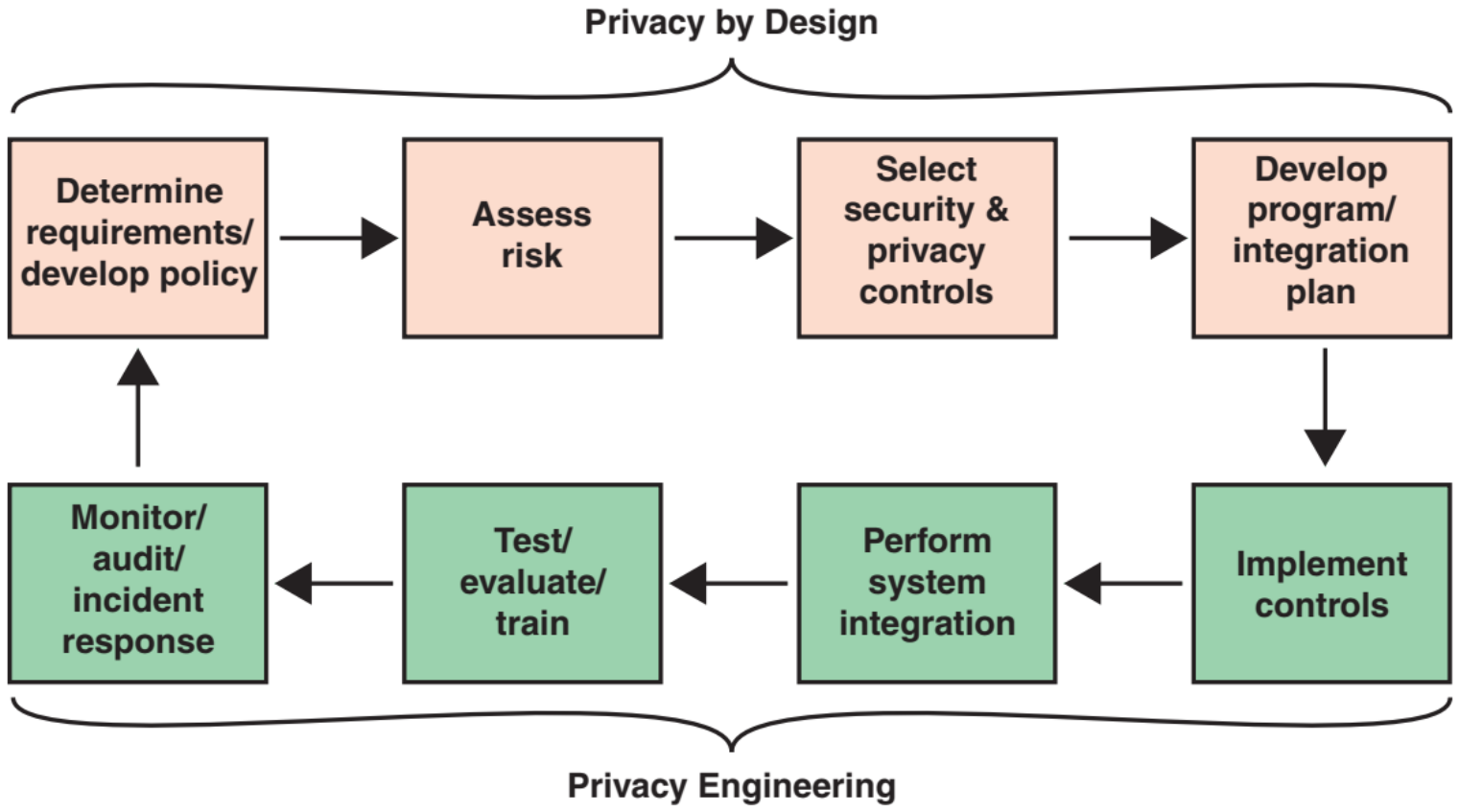
Hubungan antara Privacy by Design dan Privacy Engineering

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

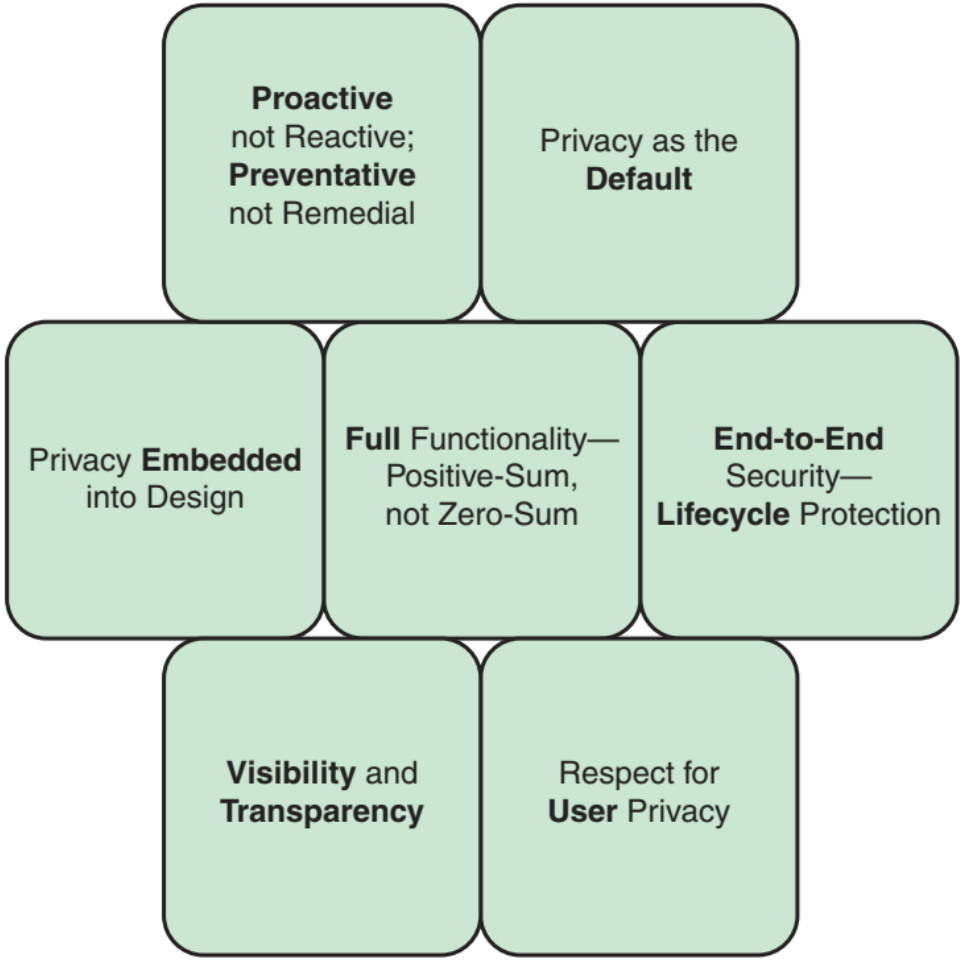
implementasi dan operasional fitur privasi sebagai bagian dari sistem secara keseluruhan

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.

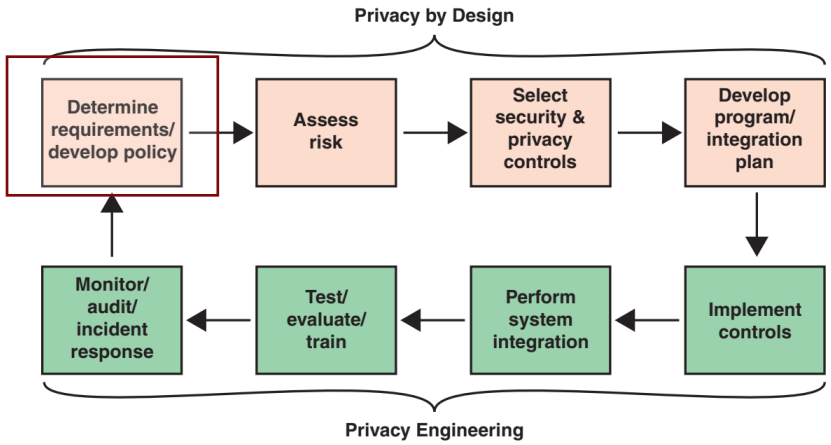


Foundational Principles of Privacy by Design

CALVIN INSTITUTE OF TECHNOLOGY

Privacy by Design

Requirements and Policy Development



Pelaku Utama:
Pemilik Sistem

Identifikasi persyaratan privasi yang menjadi dasar perencanaan

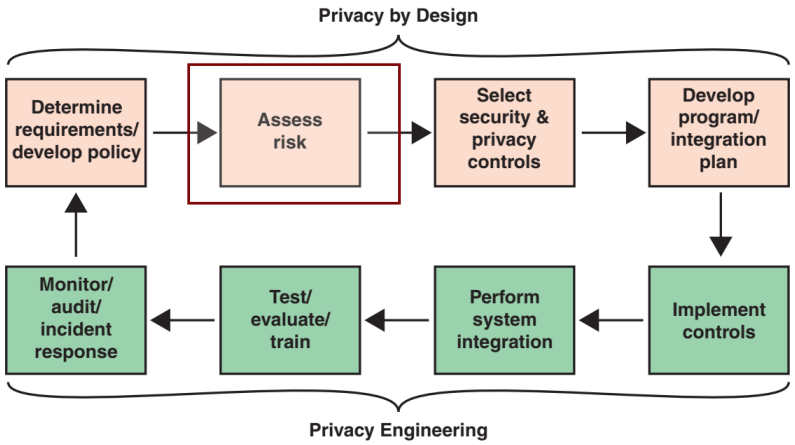
Regulasi

Standar

Komitmen kontraktual organisasi

Privacy by Design

Privacy Risk Assessment



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

Elemen Penilaian

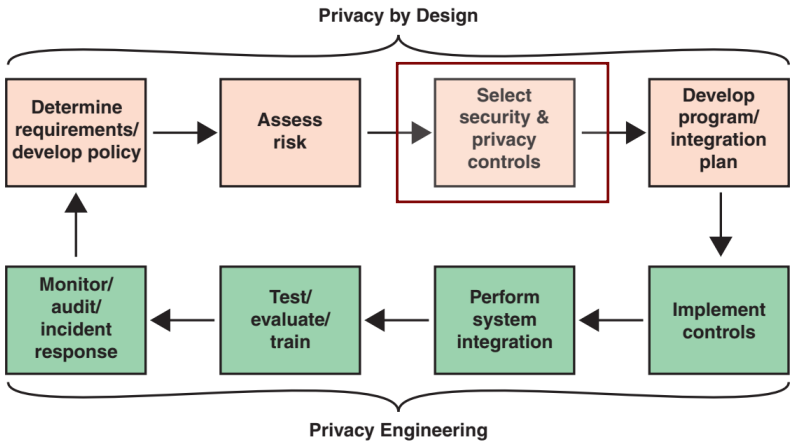
- Aset terkait privasi
- Ancaman privasi
- Kerentanan privasi
- Kontrol privasi

Langkah Penilaian

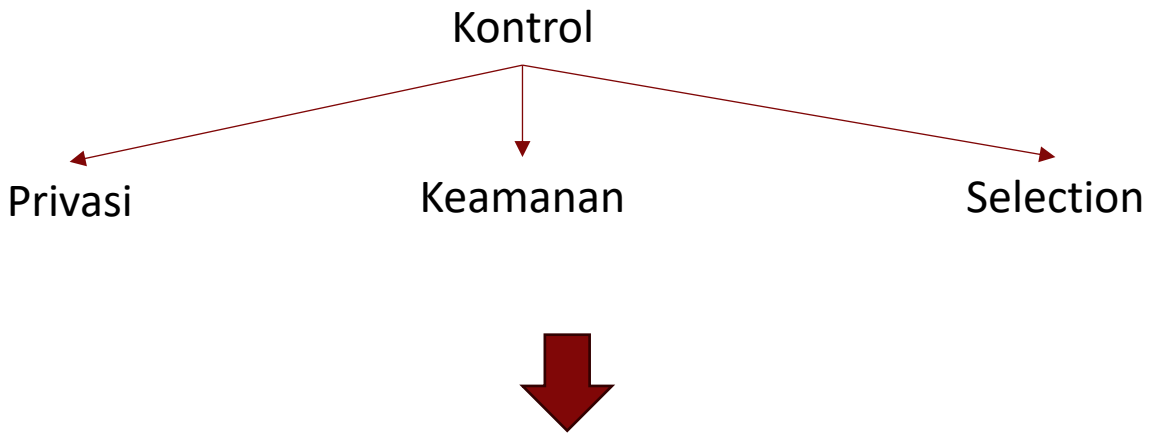
- Menentukan dampak
- Menentukan kemungkinan insiden privasi
- Menentukan tingkat risiko

Privacy by Design

Privacy and Security Control Selection



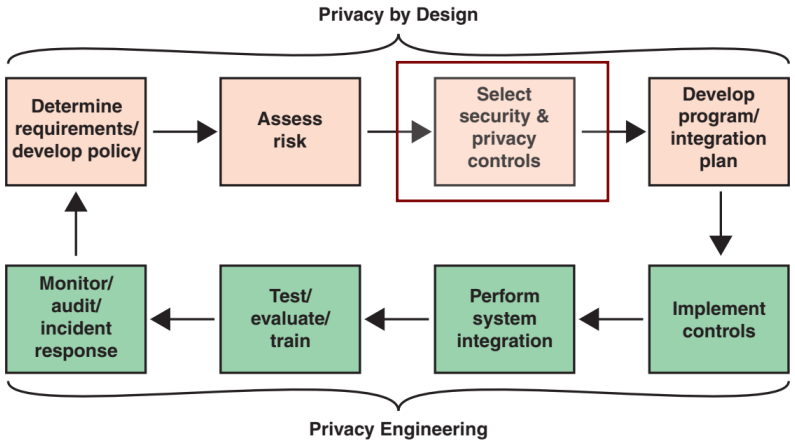
Kontrol:
langkah-langkah, mekanisme, atau tindakan yang diterapkan untuk melindungi privasi dan keamanan data



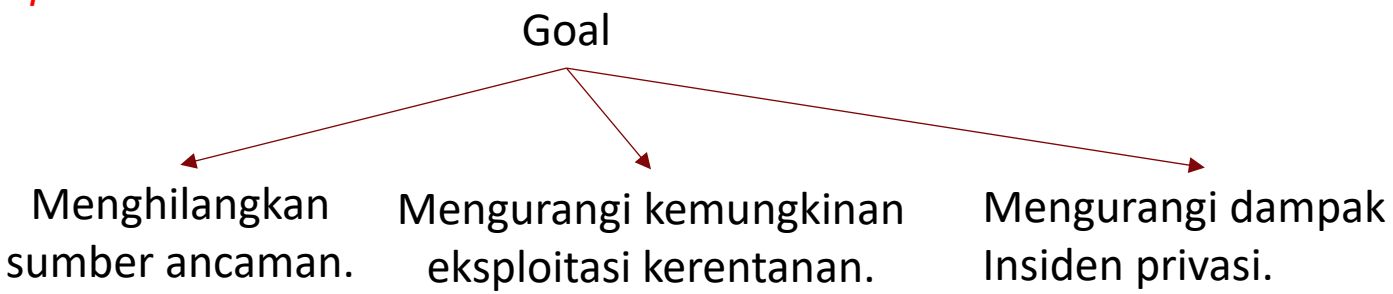
Perlindungan privasi PII (Personally Identifiable Information)

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

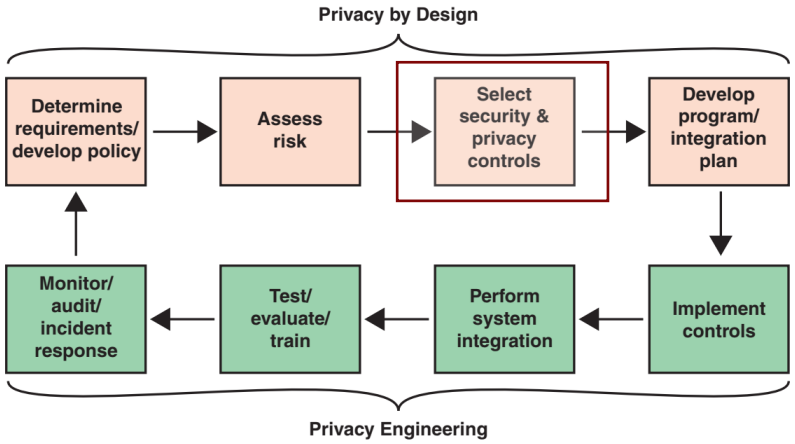


Panduan dalam pemilihan kontrol:

- 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

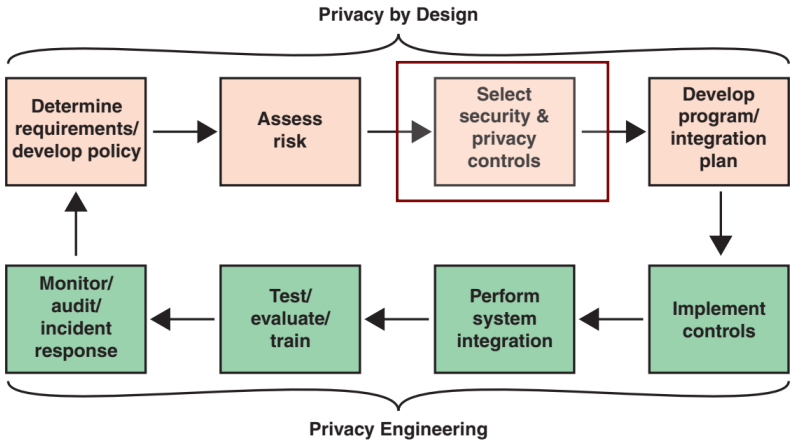
Ini termasuk Privacy Control atau Security Control?

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

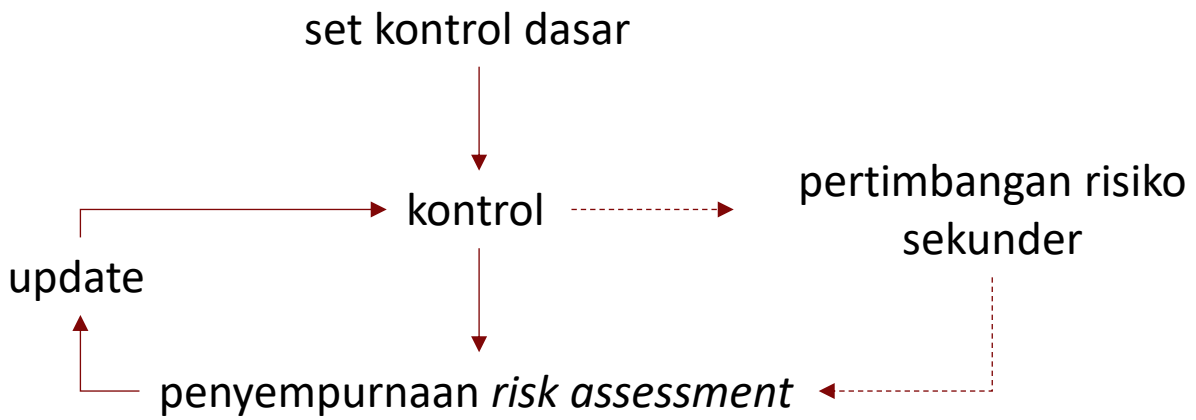
Selection Process



Selection Process:

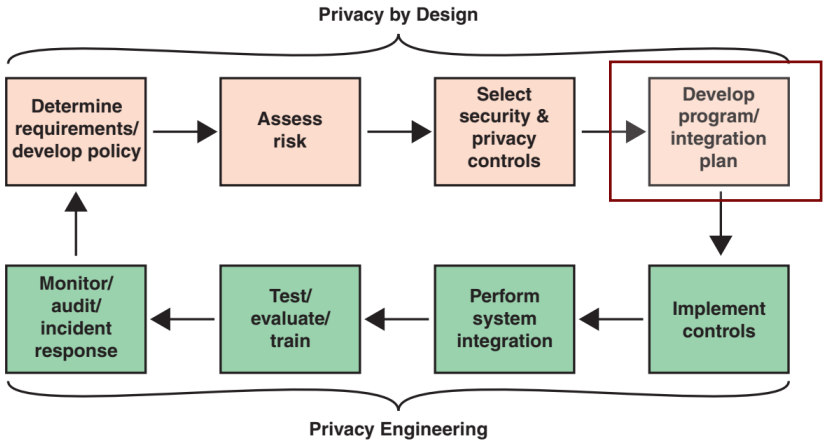
Pemilihan dan dokumentasi privacy and security control harus disinkronkan dengan aktivitas risk assessment.

Tahapan Pemilihan



Privacy by Design

Privacy Program and Integration Plan



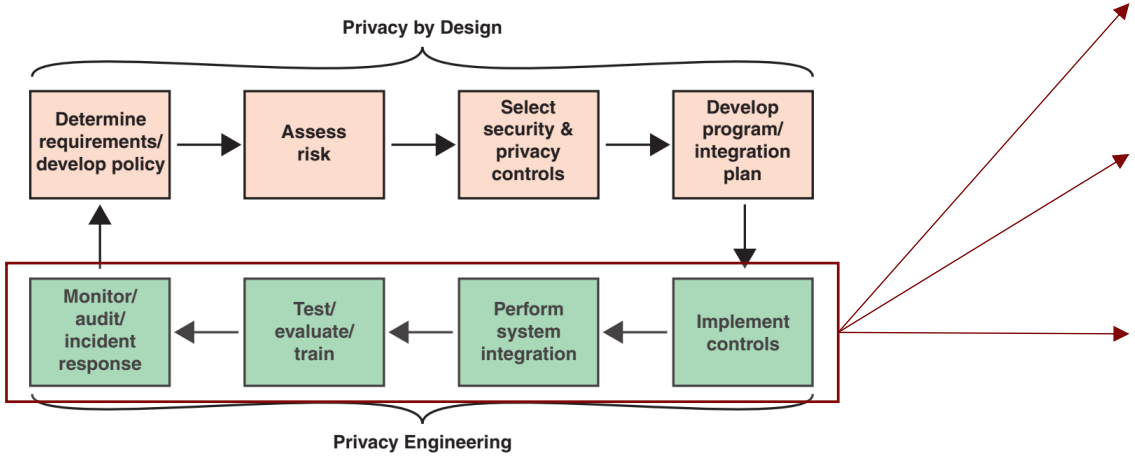
Meliputi:

- 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

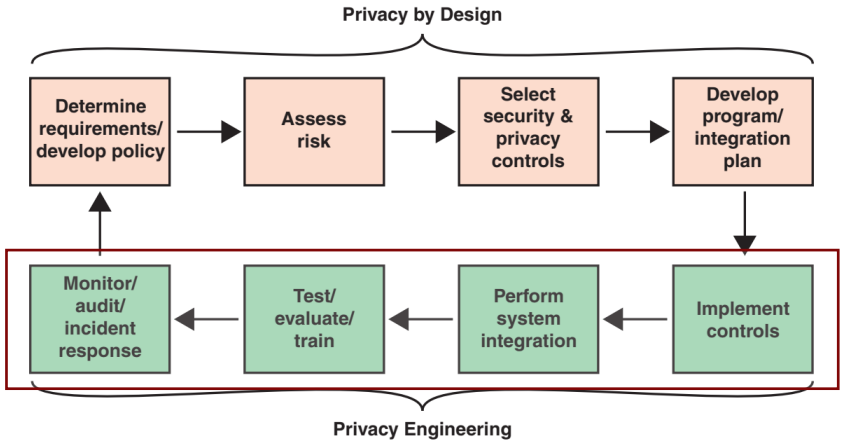
integrasi

Pengelolaan berkelanjutan

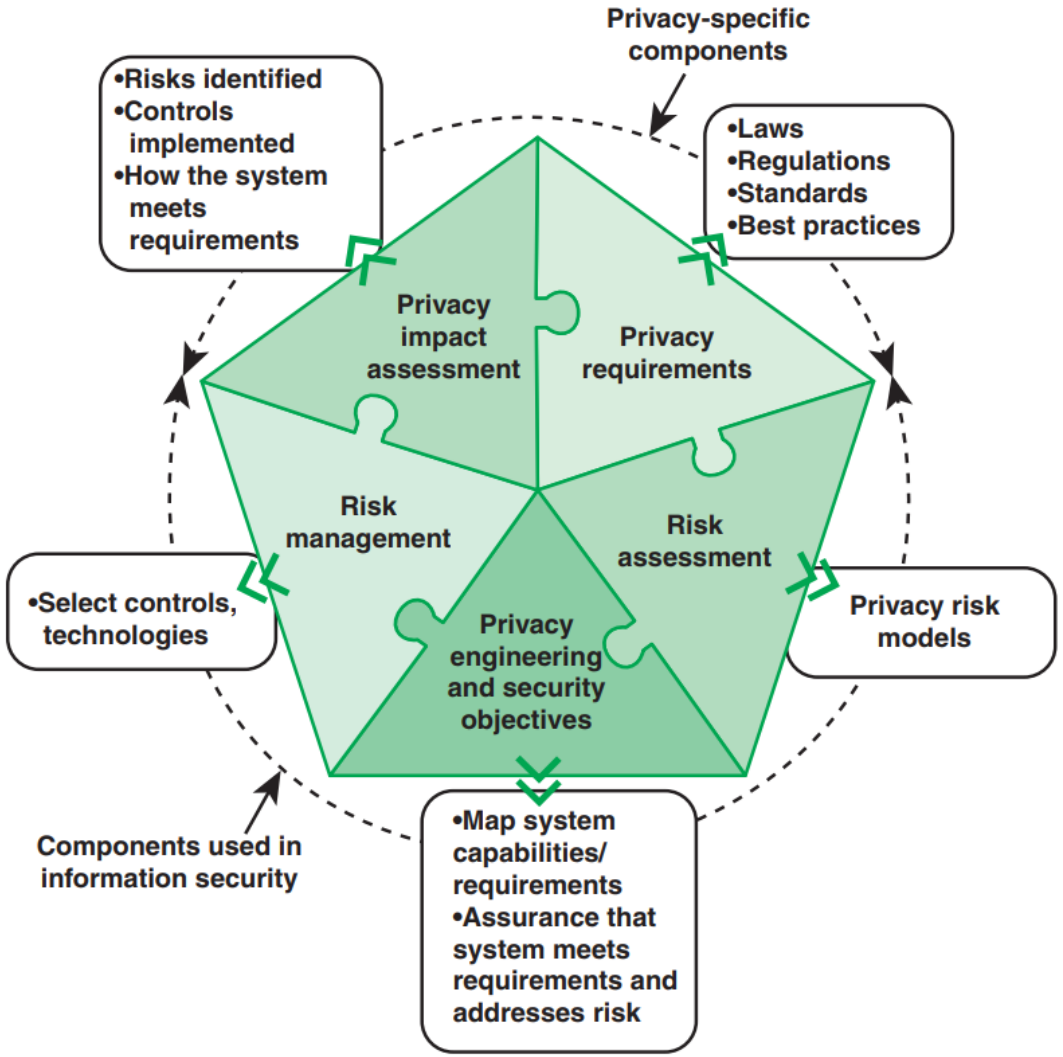
Tujuan utama rekayasa privasi

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

Privacy by Engineering

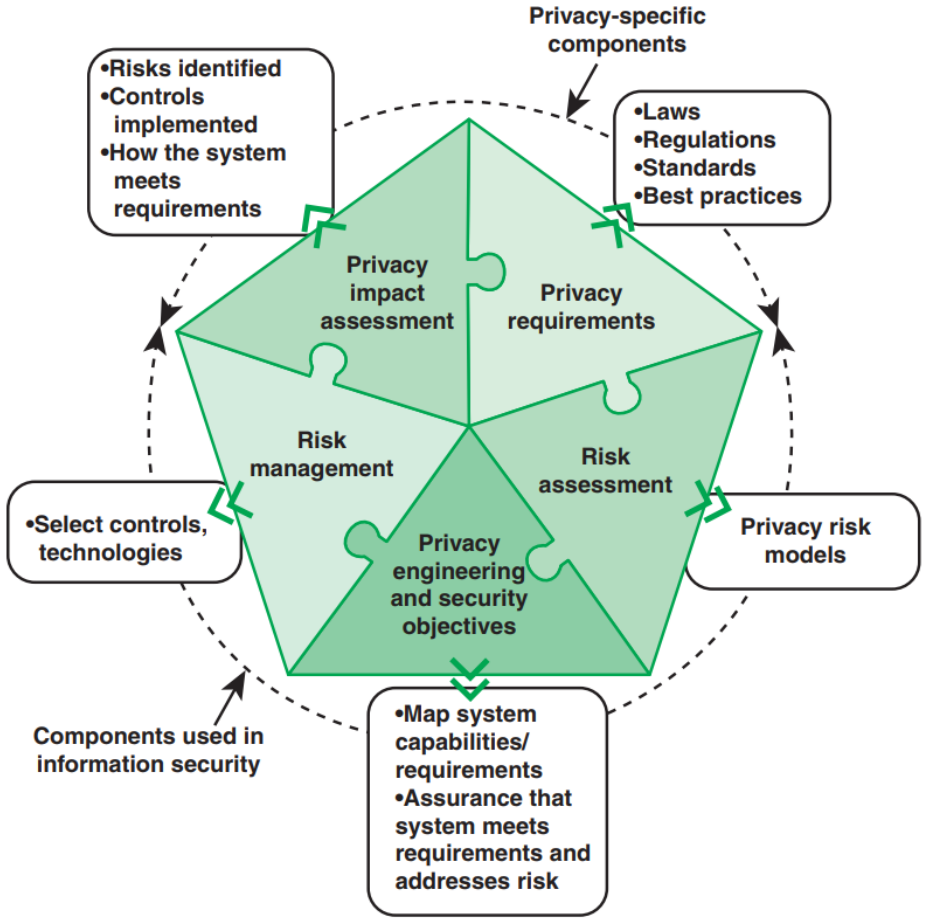


rekayasa privasi sering mencakup juga privacy by design

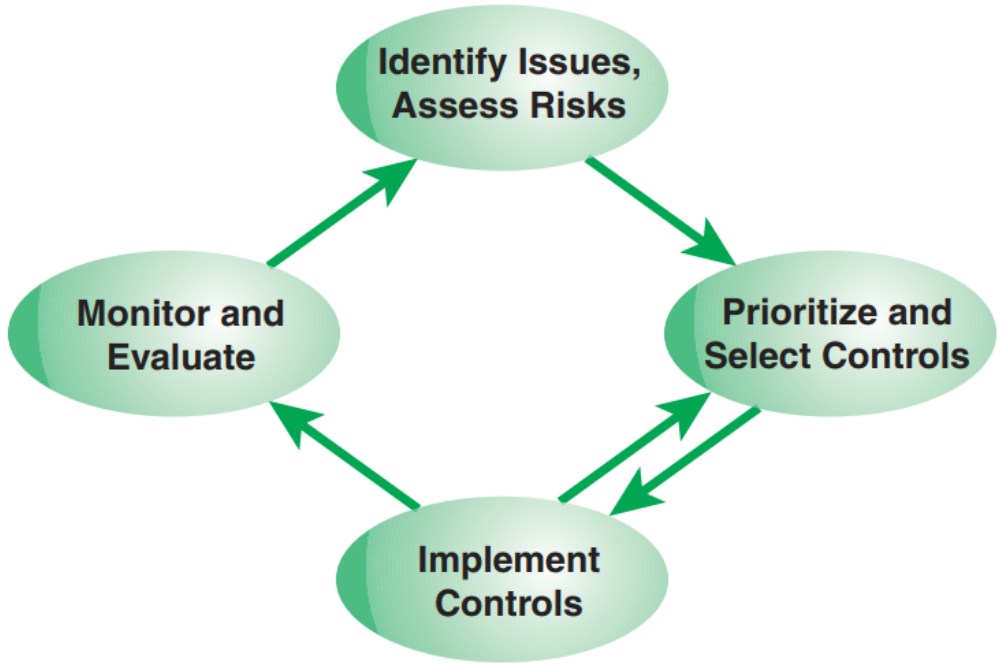


Components of Privacy Engineering (NISTIR 8062)

Privacy by Engineering

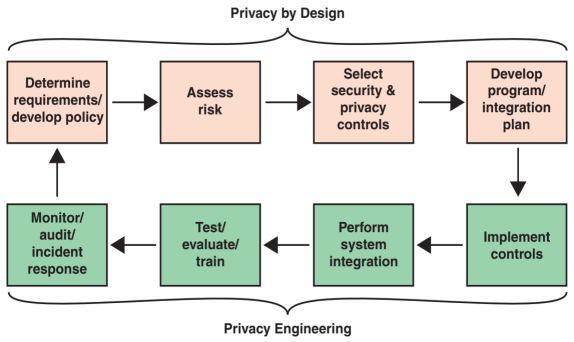


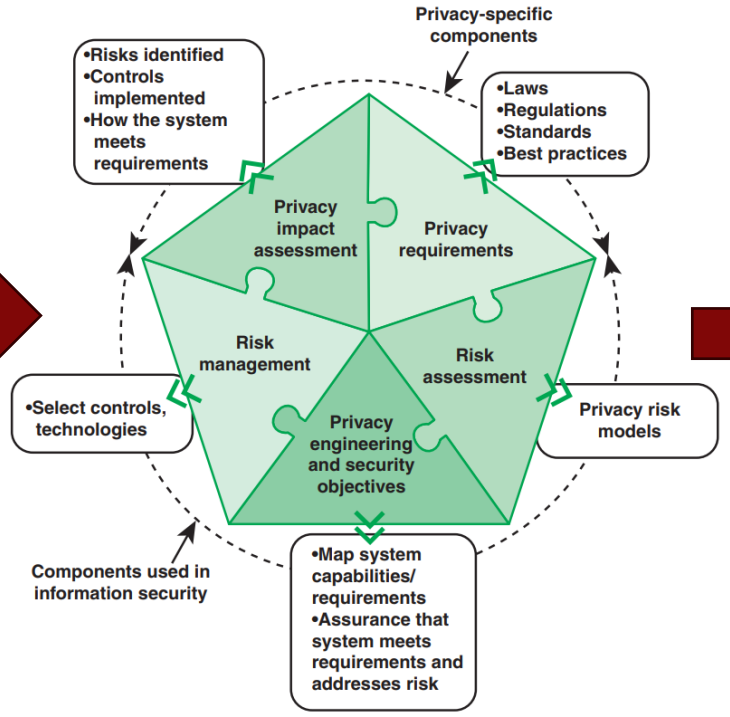
Components of Privacy Engineering (NISTIR 8062)



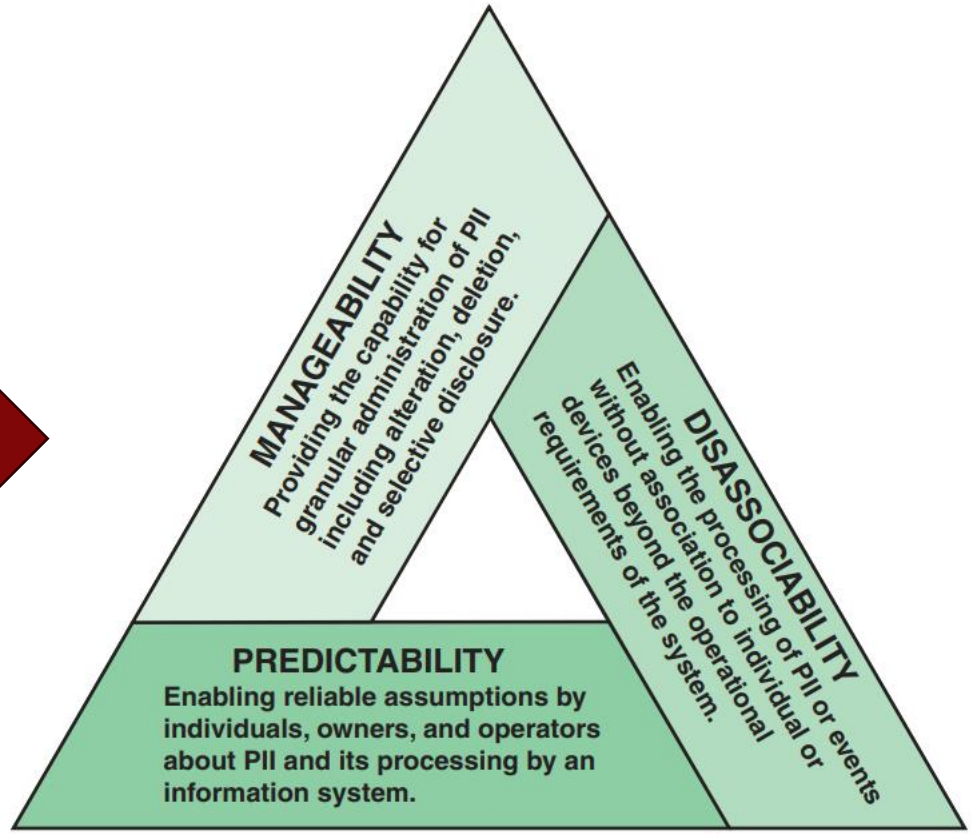
Risk Management Cycle

Privacy by Engineering





Components of Privacy Engineering (NISTIR 8062)

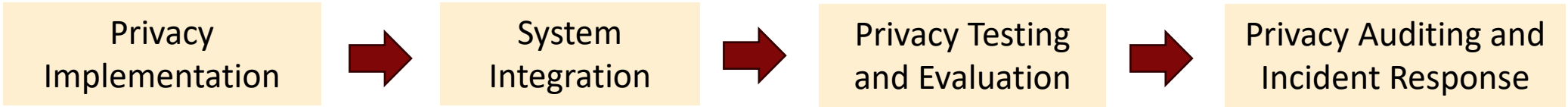


Privacy Engineering Objectives

CALVIN INSTITUTE OF TECHNOLOGY

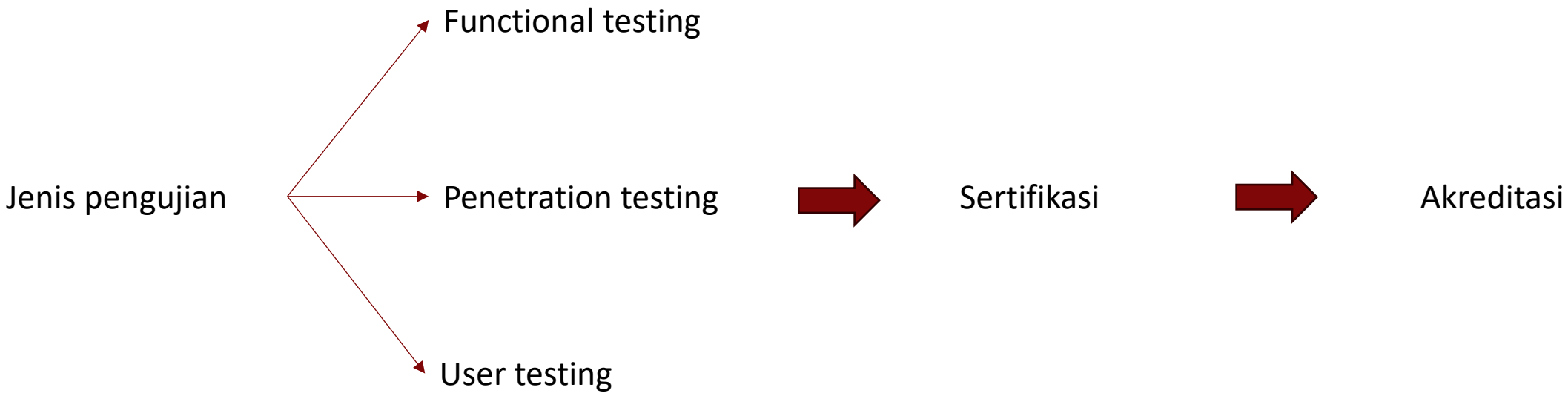
Privacy by Engineering

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.

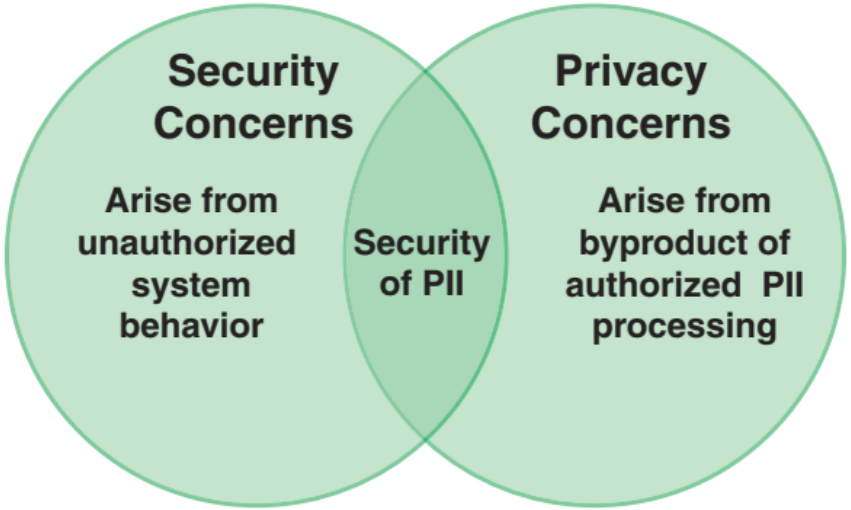
Audit

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

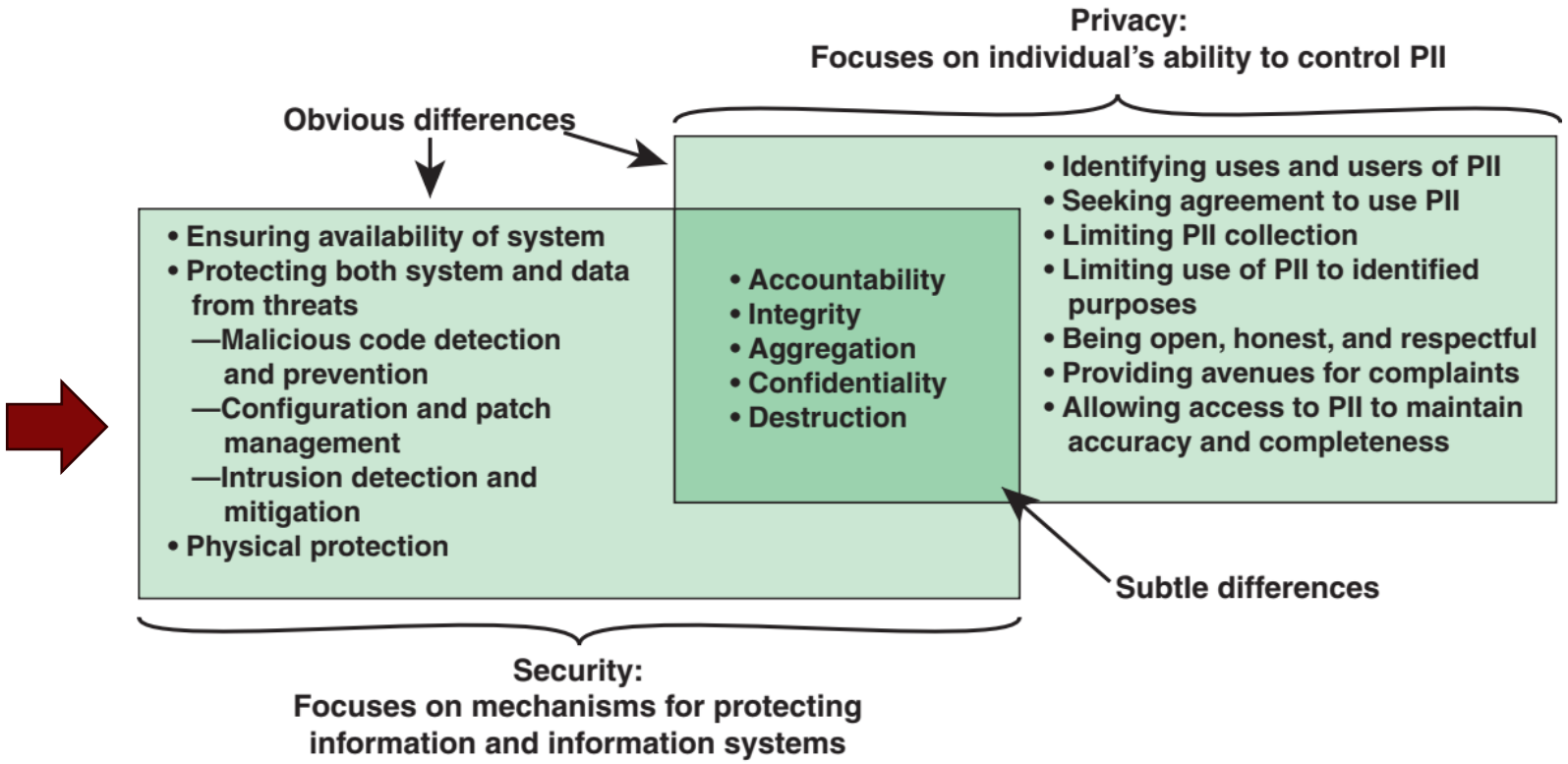
Tanggapan Insiden

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*

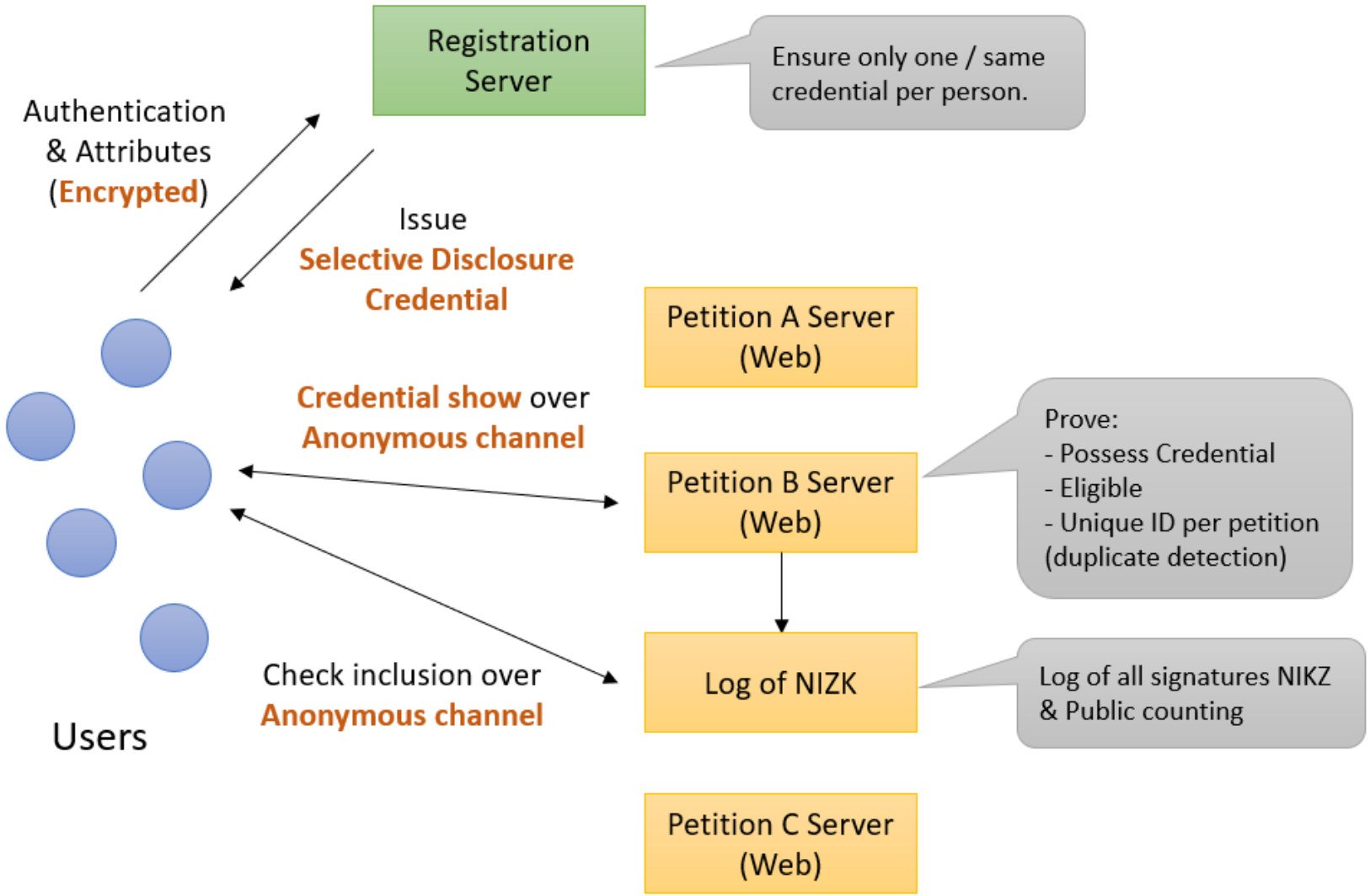
Case Study 1: e-petitions (Diaz et al. 2009)

- Petitions: a formal request to an authority.
  - E.g. EU Lisbon Treaty: 1M people across EU may request legislation.

- Two key risks:
  (1) Disclosure of who signed a petition (sensitive topics).
  (2) Discrimination or profiling on the basis of signing a petition.

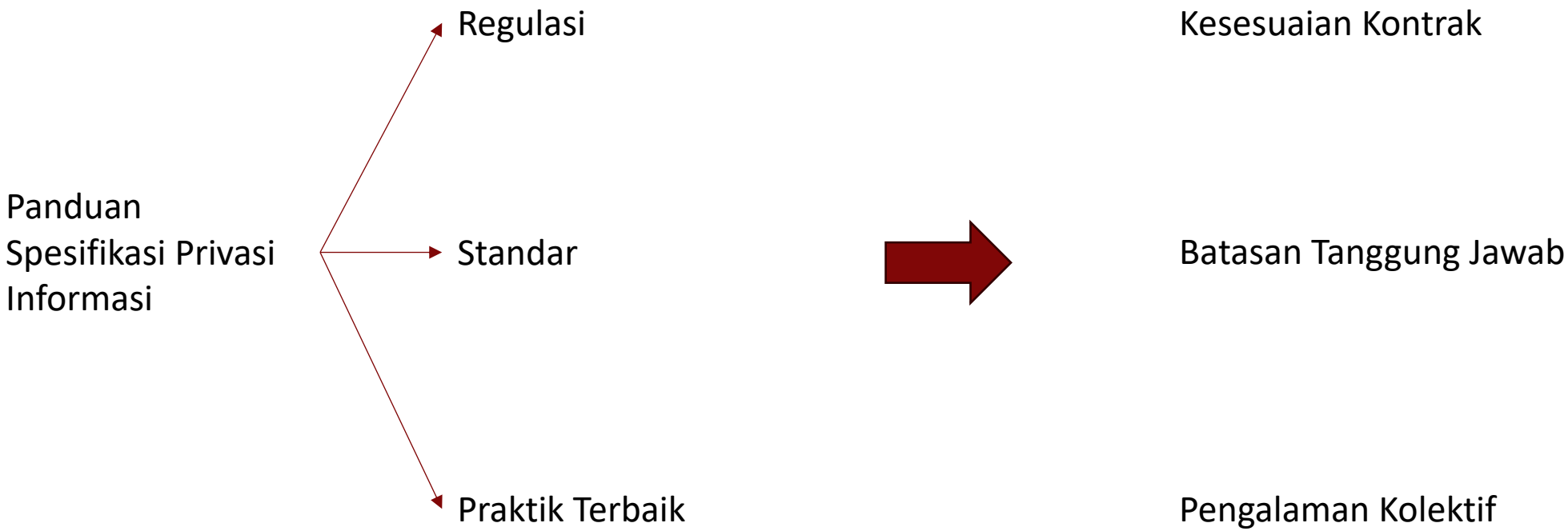
- Requirements:
  - “The signatures correspond to existing individuals.”
  - “Only individuals eligible to sign a petition are able to do so.”
  - “Each individual can sign a petition only once.”
  - “The number of signatures is correctly counted.”
  - Note: “identifiability not inherent” -> Principle of data minimization …

Case Study 1: e-petitions (Diaz et al. 2009)



Information Privacy Requirements and Guidelines

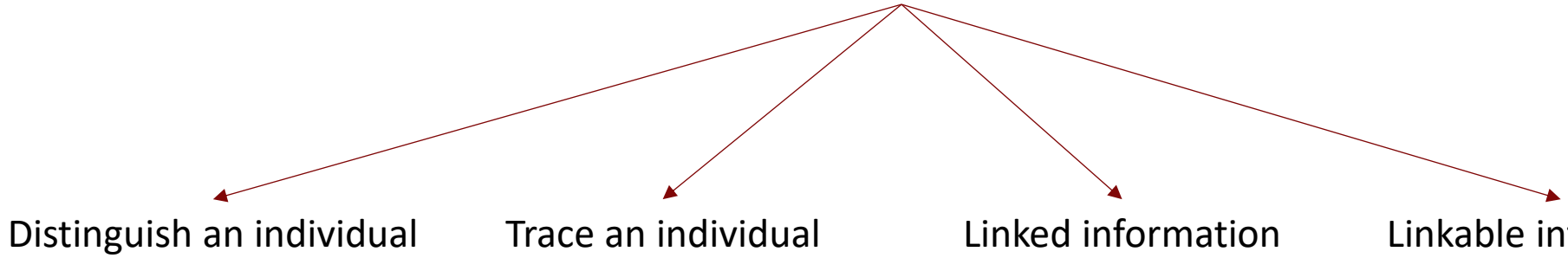
Spesifikasi Privasi Informasi



Data Pribadi

Setiap informasi tentang individu yang disimpan oleh lembaga, termasuk informasi yang dapat digunakan untuk membedakan atau menelusuri identitas individu, seperti nama, nomor jaminan sosial, tanggal dan tempat lahir, nama gadis ibu, atau catatan biometrik; serta informasi lain yang terkait atau dapat dihubungkan dengan individu, seperti informasi medis, pendidikan, keuangan, dan pekerjaan.

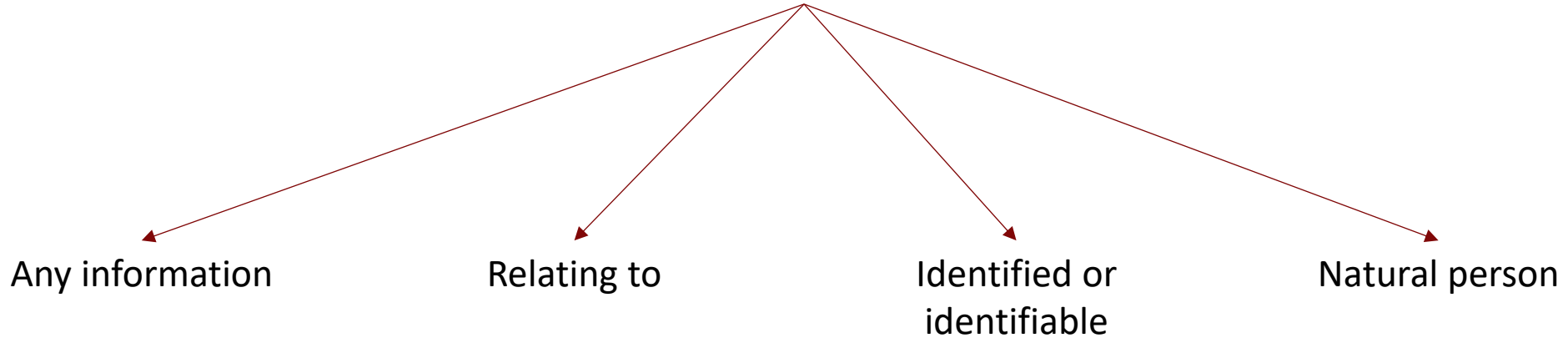
NIST SP 800-122



Data Pribadi

Setiap informasi terkait individu yang dapat diidentifikasi, baik secara langsung maupun tidak langsung, termasuk nama, nomor identifikasi, lokasi, pengenal daring, atau faktor lain yang terkait dengan fisik, fisiologis, genetik, mental, ekonomi, budaya, atau identitas sosial seseorang.

Regulasi Uni Eropa (GDPR)



Sumber Informasi Identitas Pribadi (PII)

1. **Identifikasi yang Dikeluarkan Pemerintah:**
   Contoh: SIM, paspor, akta kelahiran, dan pengidentifikasi manfaat pensiun serta medis (misalnya, di Amerika Serikat: nomor Jaminan Sosial dan nomor Medicare).
2. **Informasi Kontak:**
   Contoh: Alamat email, alamat fisik, dan nomor telepon.
3. **Informasi Daring:**
   Contoh: Akun Facebook dan media sosial lainnya, kata sandi, dan PIN (nomor identifikasi pribadi).
4. **Data Geolokasi:**
   Contoh: Dari ponsel cerdas, perangkat GPS, dan kamera.
5. **Alamat Perangkat:**
   Contoh: Alamat IP dari perangkat yang terhubung ke Internet atau alamat kontrol akses media (MAC) perangkat yang terhubung ke jaringan lokal.
6. **Data Verifikasi:**
   Contoh: Nama gadis ibu, nama hewan peliharaan atau anak, dan nama sekolah menengah.
7. **Informasi Catatan Medis:**
   Contoh: Resep obat, catatan medis, hasil pemeriksaan, dan gambar medis.
8. **Informasi Biometrik dan Genetik:**
   Contoh: Sidik jari, pemindaian retina, dan DNA.
9. **Nomor Akun:**
   Contoh: Nomor rekening bank, asuransi, investasi, dan kartu debit/kredit.

Sensitivitas Informasi Identitas Pribadi (PII)

PII sensitive ➔ PII yang jika hilang, dikompromikan, atau diungkapkan tanpa izin dapat menyebabkan kerugian, ketidaknyamanan, rasa malu, atau ketidakadilan kepada individu.

Contoh PII Sensitif:

1. Nomor Jaminan Sosial.
2. Tempat/tanggal lahir.
3. Nama gadis ibu.
4. Informasi biometrik.
5. Data medis (kecuali referensi singkat).
6. Informasi keuangan pribadi.
7. Nomor kartu kredit/debit.
8. Nomor paspor.
9. Informasi pekerjaan sensitif (misalnya, hasil investigasi latar belakang).
10. Riwayat kriminal.
11. Informasi yang dapat menstigmatisasi atau berdampak buruk pada individu.

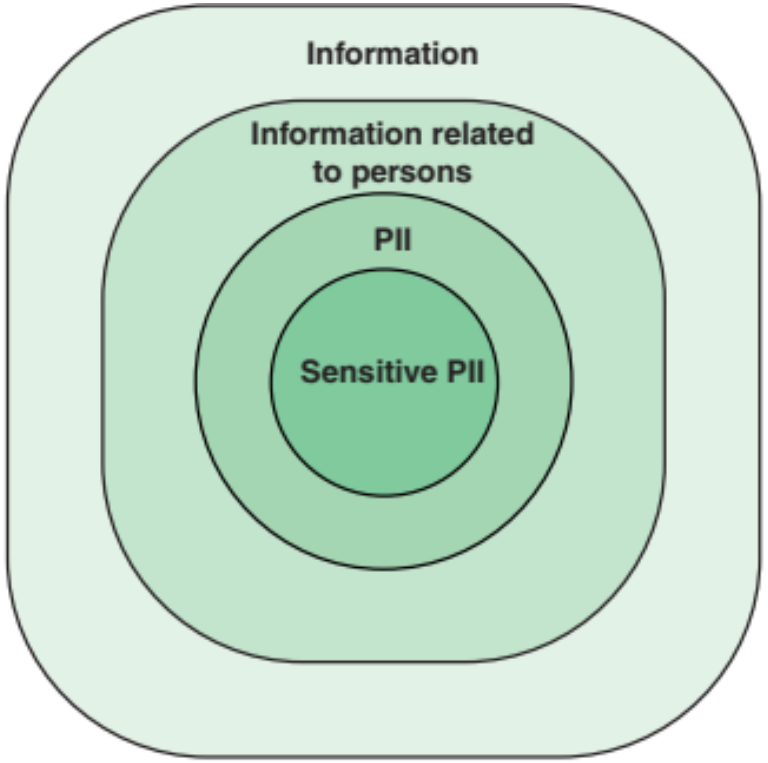
Contoh PII Tidak Sensitif:

1. Nama individu.
2. Alamat email kantor.
3. Alamat kerja.
4. Nomor telepon kerja.

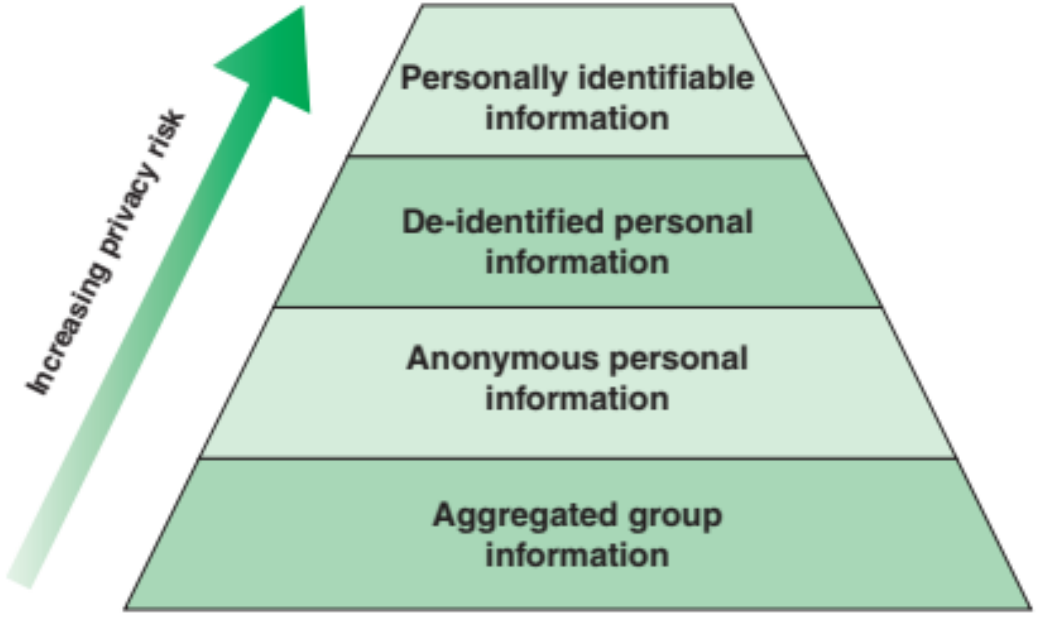
Konteks dan Sensitivitas:

Daftar nama pegawai biasa tidak dianggap sensitif, tetapi daftar pegawai penegak hukum

Sensitivitas Informasi Identitas Pribadi (PII)



Information and PII

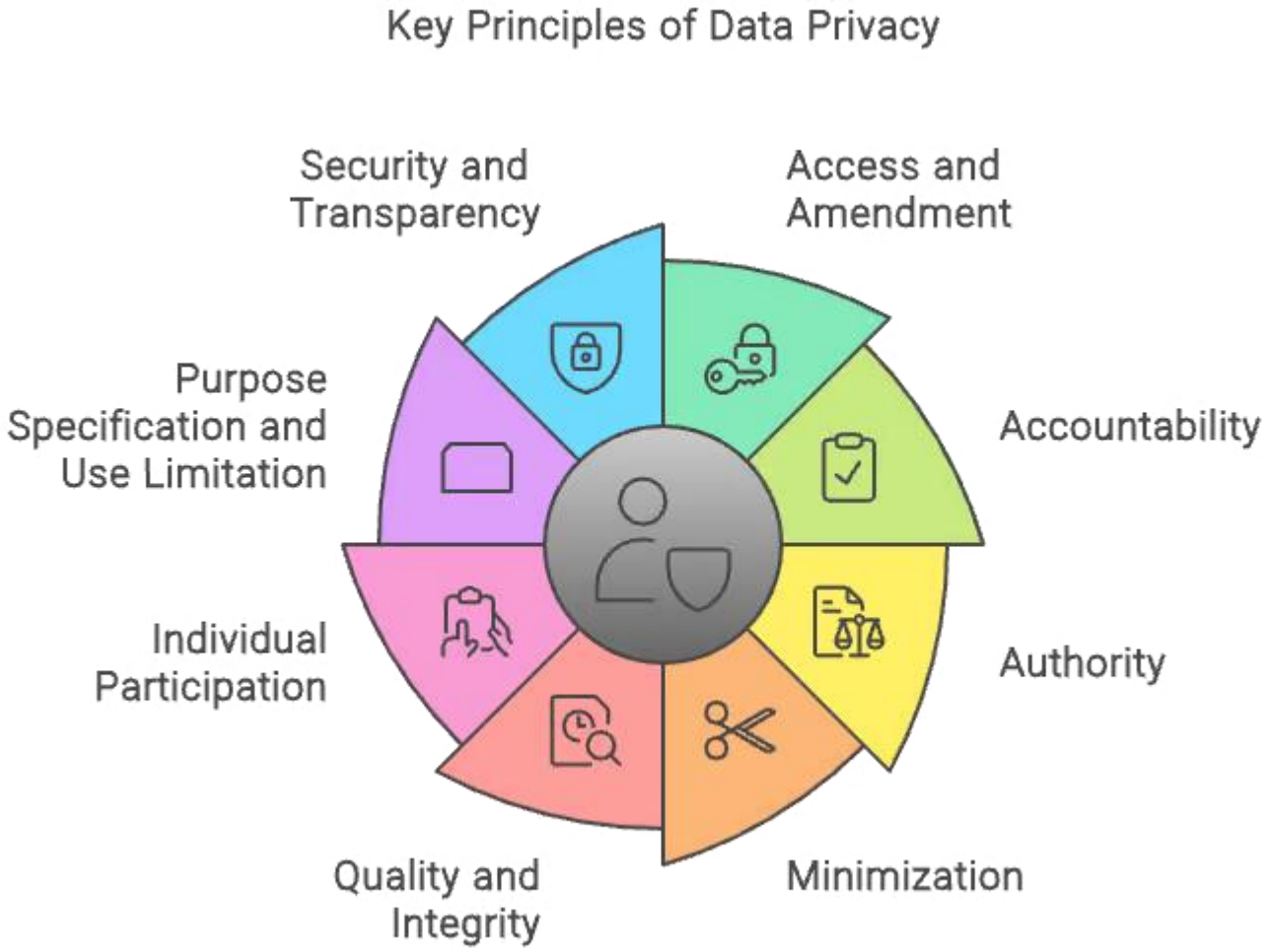


Degrees of Privacy Risk

Fair Information Practice Principles

Individu memiliki hak untuk berpartisipasi dalam pengelolaan informasi pribadi yang dapat diidentifikasi, termasuk menentukan isi dan penggunaannya.
Laporan tahun 1973 dari Departemen Kesehatan, Pendidikan, dan Kesejahteraan AS (HEW) yang berjudul Records, Computers, and the Rights of Citizens.

Pada tahun 1980, Organisasi untuk Kerja Sama dan Pembangunan Ekonomi (OECD) memperluas prinsip ini menjadi delapan prinsip yang dikenal sebagai OECD Fair Information Practice Principles



OECD Fair Information Practice Principles

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

Terima Kasih
Tuhan Memberkati