UNIVERSITAS AMIKOM YOGYAKARTA
Creative Economy Park

MATA KULIAH CYBER SECURITY

Program Studi Magister Informatika

Universitas AMIKOM Yogyakarta
Tahun 2025

Creative Economy Park

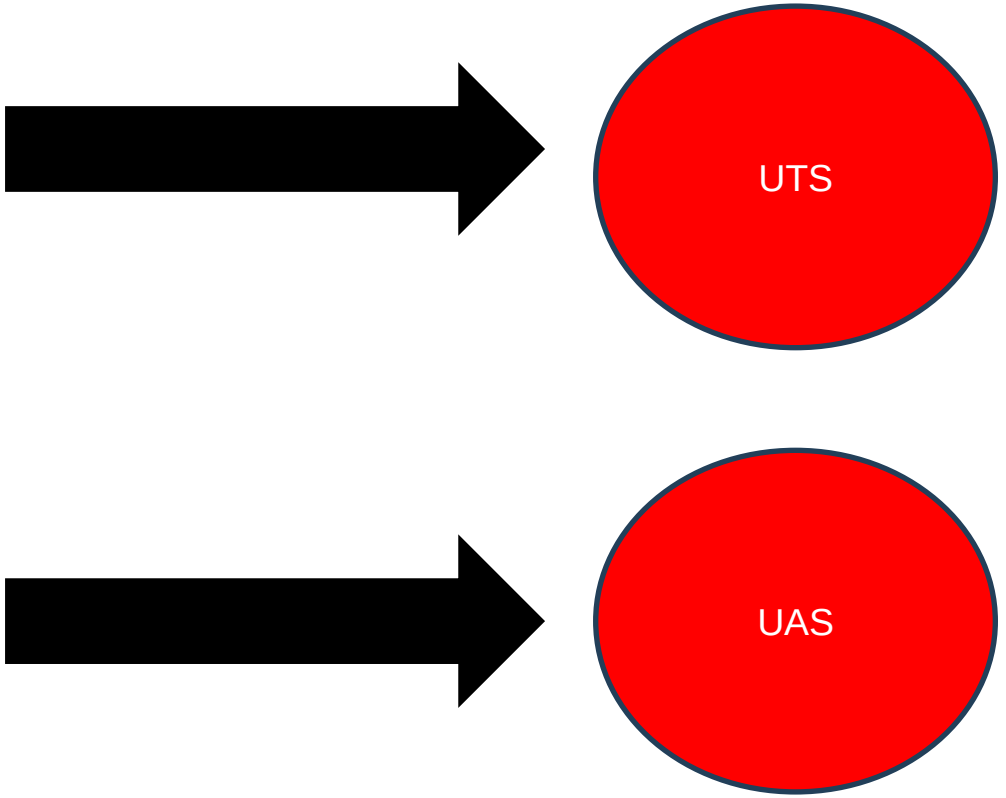
Dr. Ir. Yoga Sahria, S.Kom., M.Kom.

Fakultas Ilmu Komputer

Universitas AMIKOM Yogyakarta
Jln RingRoad Utara, Depok, Condongcatur
Yogyakarta

Outline Mata Kuliah Selama 1 Semester

1. Ruang lingkup keamanan cyber menurut framework Cyber Security Body of Knowledge (CyBoK)
2. Serangan infrastruktur jaringan
3. Malware
4. Serangan aplikasi desktop dan web
5. Social engineering
6. Solusi pengamanan data dan sistem modern
7. Regulasi dan kebijakan cyber law di Indonesia
8. Implementasi kebijakan keamanan TI
9. Penetration testing
10. Digital Forensic



UNIVERSITAS AMIKOM YOGYAKARTA
Creative Economy Park

Kebijakan dan Standar Keamanan Informasi

PERTEMUAN 6

Universitas AMIKOM Yogyakarta
Tahun 2025

Creative Economy Park

Dr. Ir. Yoga Sahria, S.Kom., M.Kom.

Fakultas Ilmu Komputer

Universitas AMIKOM Yogyakarta
Jln RingRoad Utara, Depok, Condongcatur
Yogyakarta

Kebijakan dan Standar Keamanan Informasi

Minggu 6

Dr. Ir. Yoga Sahria, S.Kom., M.Kom.

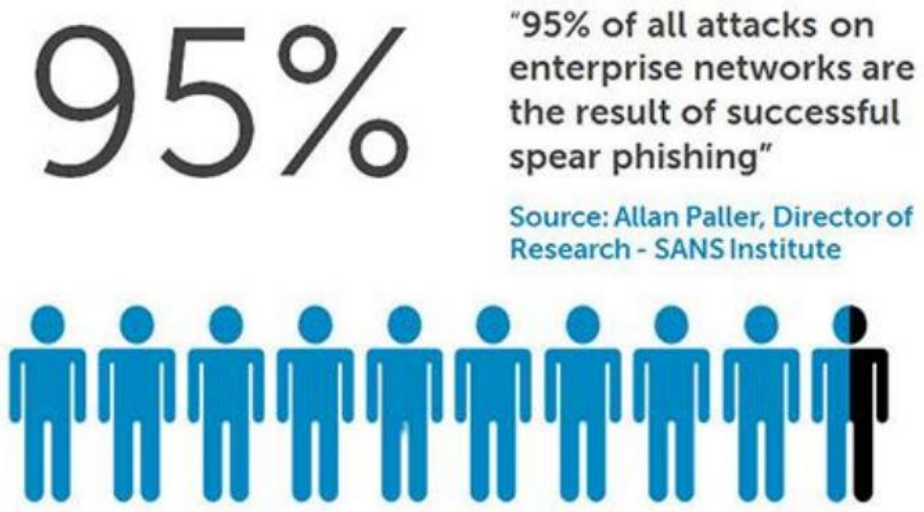
Capaian Pembelajaran

- Mahasiswa dapat menjelaskan pentingnya kebijakan dan prosedur keamanan TI pada perusahaan
- Mahasiswa dapat menulis konsep-konsep kebijakan dan prosedur keamanan yang yang baik sesuai dengan kebutuhan perusahaan

Warning

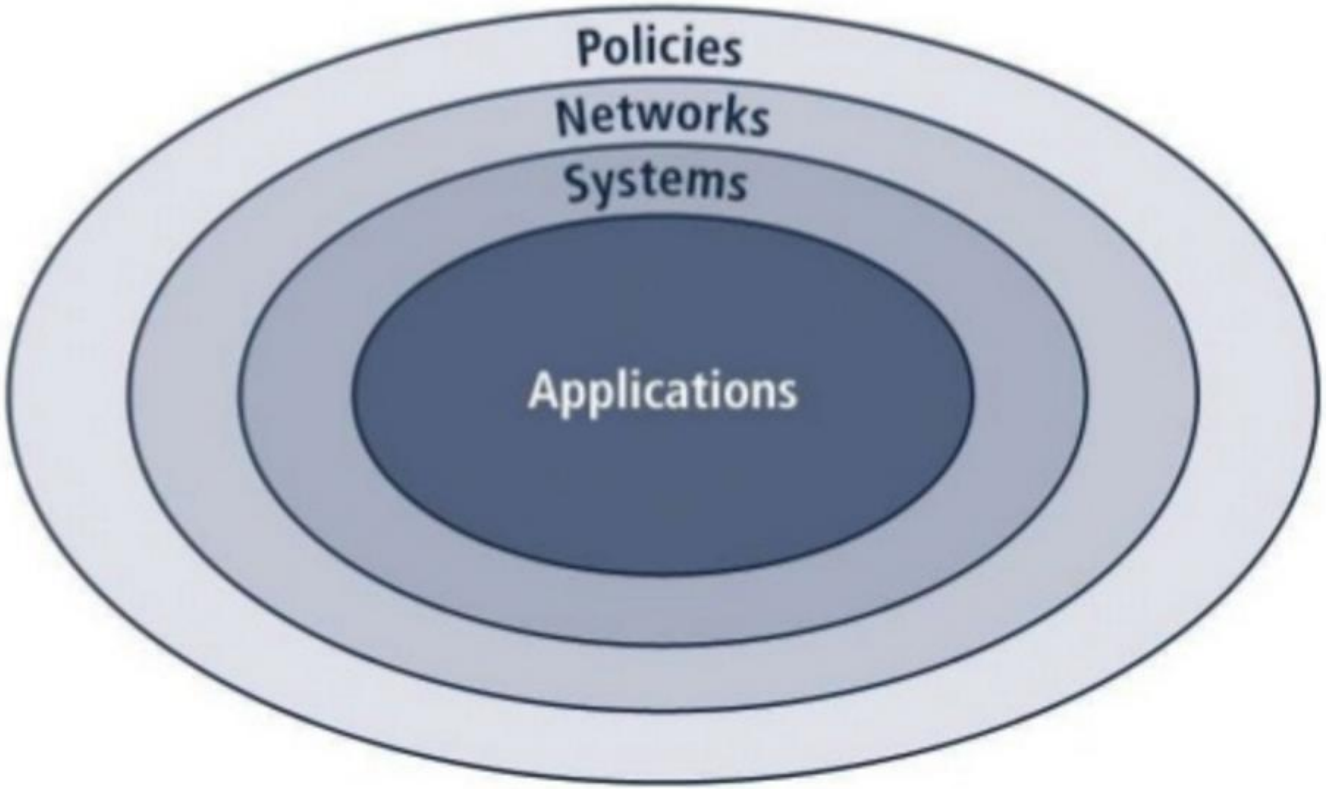
“The weakest link in the security chain is the human element”

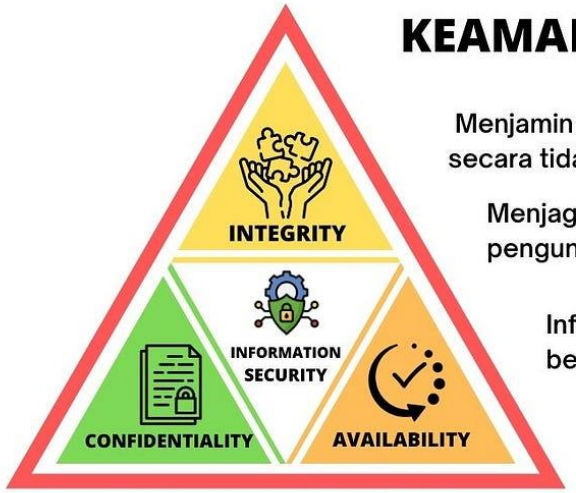
Mata Rantai Terlemah Dalam Rantai Keamanan Adalah Unsur Manusia

- 

Lapis model Bulls-eye

- 1. **Kebijakan (Policies)** : Lapis luar dalam diagram bull's-eye
- 2. **Jaringan (Networks)** : Tempat dimana ancaman dari jaringan publik bertemu dengan jaringan organisasi
- 3. **Sistem (Systems)** : Komputer yang digunakan sebagai server, desktop, dan sistem digunakan untuk kontrol proses dan sistem manufacturing
- 4. **Aplikasi (Applications)** : Semua sistem aplikasi, mulai dari aplikasi otomatisasi kantor, email, ERP, aplikasi khusus





KEAMANAN INFORMASI

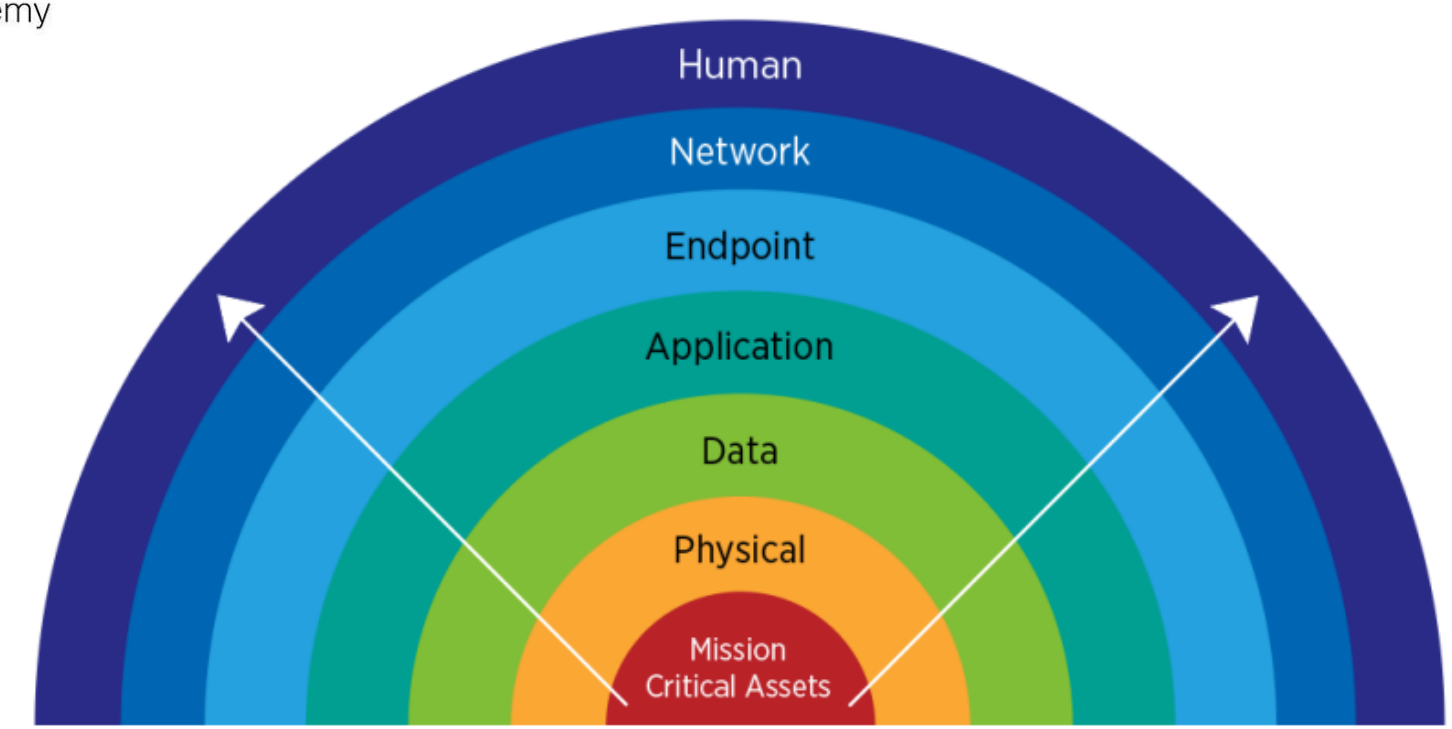
Menjamin keamanan bahwa data tidak dapat dimodifikasi secara tidak sah tata krama .

Menjaga kerahasiaan dalam aktivitas pengungkapan informasi ilegal

Informasi mudah di akses pengguna yang berwenang.

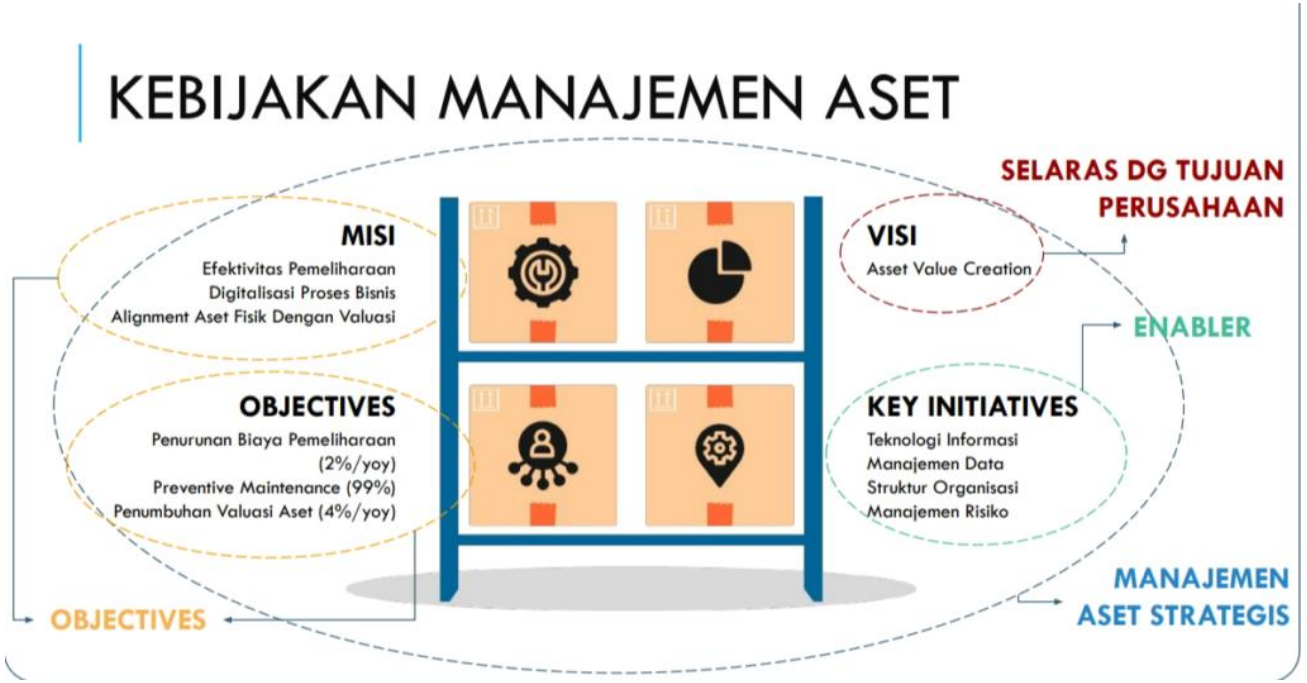
KOMINFO

Networking Academy
CISCO



Informasi Adalah Aset Bagi Organisasi.

- **Informasi adalah aset bagi organisasi**. Karena itu organisasi berkewajiban dan bertanggung jawab untuk melindunginya. Ketersediaan informasi yang lengkap dan akurat merupakan hal yang sangat penting untuk mendukung fungsi organisasi yang terkait dengan penyediaan kebutuhan informasi bagi pihak internal maupun eksternal organisasi.
- Dalam kaitannya memroses informasi, organisasi memiliki tanggung jawab untuk mengamankan informasi dan mencegah penyalahgunaan informasi. Hal penting yang patut dilakukan adalah menselaraskan antara risiko keamanan informasi dengan risiko bisnis perusahaan secara keseluruhan.
- Karena itu dengan penyerasian sistem keamanan informasi dengan strategi penanganan risiko bisnis, dapat menunjang keefektifan manajemen risiko perusahaan.



Keterkaitan Cyber Security(Keamanan Siber)

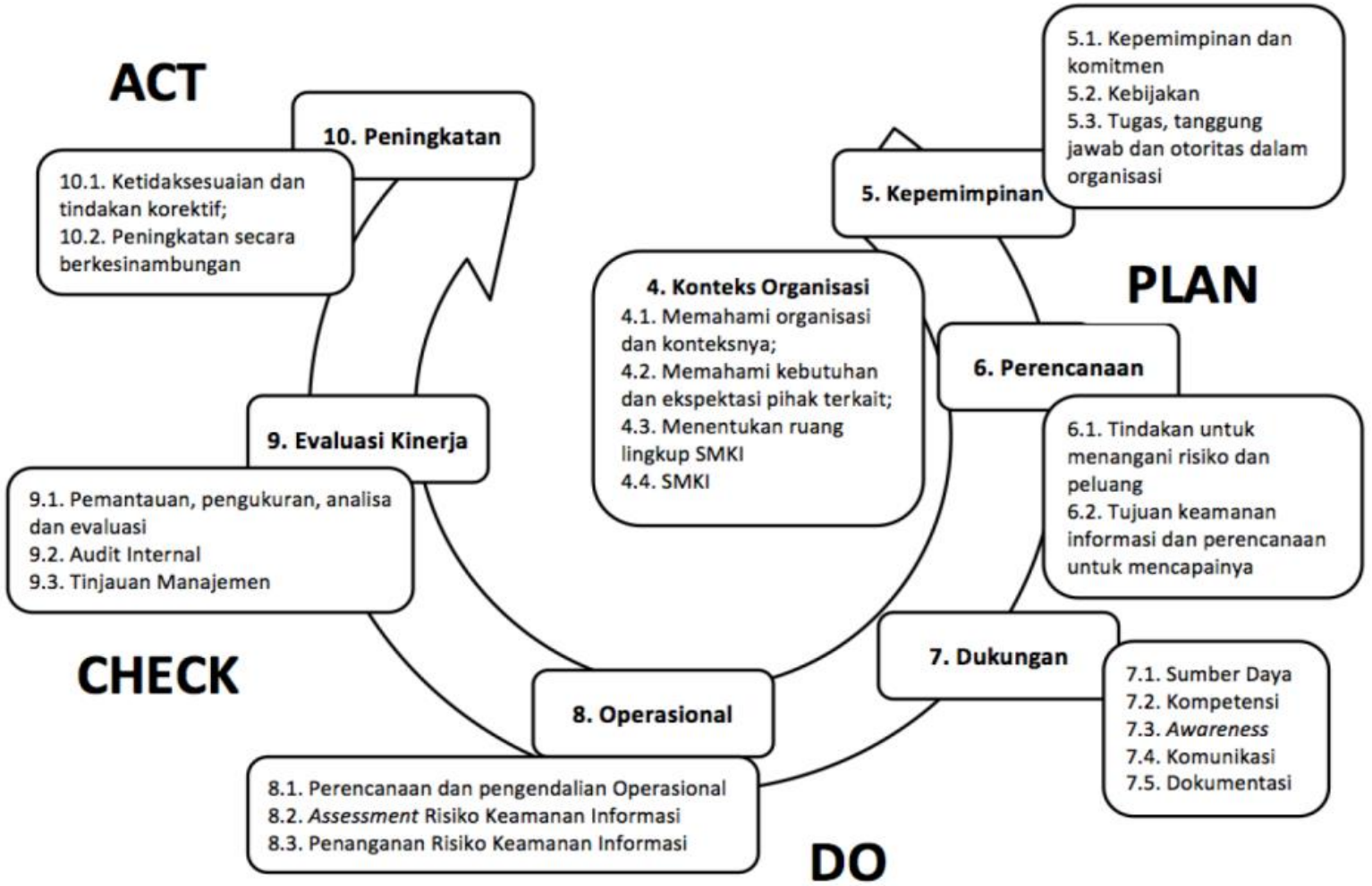
- Keamanan Siber dan Pertahanan Siber memiliki setidaknya satu keterkaitan erat, yaitu bahwa keduanya diterapkan untuk menjaga dan mempertahankan
- kerahasiaan (***confidentiality***), integritas (***integrity***), dan ketersediaan (***availability***) informasi elektronik atau Sistem Elektronik.
- **UU No.11 Tahun 2008** tentang Informasi dan **Transaksi Elektronik (UU ITE)** dan Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik merupakan pondasi membangun Keamanan Siber dan Pertahanan Siber nasional secara organik. Secara organik maksudnya keamanan dan pertahanan nasional dibangun oleh Penyelenggara Sistem Elektronik secara semesta dan berkesinambungan.

ISO 27001 untuk Cyber Security

- ISO 27001 sendiri merupakan suatu standar sistem manajemen keamanan informasi yang diterbitkan oleh ISO dan IEC pada tahun 2005.
- Standar ini sudah mengalami beberapa kali pembaruan, dan dirancang untuk meningkatkan keamanan informasi, praktek keamanan informasi yang baik, dan kebijakan untuk membantu mencegah penyalahgunaan dan pengubahan informasi dan komputasi sistem yang sensitif.
- Sertifikasi ISO 27001 juga bisa membantu organisasi untuk mendapatkan kepercayaan pelanggan yang lebih baik.
- Penerapan ISO 27001 sebagai Information Security Management System atau ISMS akan membantu organisasi dalam membangun dan memelihara sistem manajemen keamanan informasi atau ISMS.
- Information Security Management System atau ISMS sendiri adalah seperangkat unsur yang saling terkait dengan organisasi, yang digunakan dalam pengelolaan dan pengendalian risiko keamanan. Selain itu, ISMS juga digunakan untuk melindungi dan menjaga kerahasiaan (confidentiality) integritas (integrity) dan ketersediaan (availability) informasi.

Klik Disini

Struktur SNI ISO 27001:2013



Aset utama dalam cyber security

- Aset utama dalam cyber security adalah **personel atau SDM** yang memainkan peran sangat penting dalam pertahanan siber.
- Tantangan terbesar dalam implementasi pertahanan siber adalah menyediakan SDM yang kompeten dan senantiasa cepat dan sigap mengikuti dinamika lingkungan siber yang terus berkembang seiring berkembangnya teknologi dan kondisi sosial masyarakat.
- Untuk itu strategi pengembangan SDM harus didukung dengan program peningkatan kompetensi yang berkesinambungan.
- Sumber: Klik Disini

Strategi Nasional Keamanan Siber dan Pertahanan Siber

1. Penentuan dan evaluasi ancaman (threat) dan kelemahan (vulnerabilities) Sistem Elektronik Infrastruktur Strategis di Indonesia
2. Pengelolaan sumber daya (khususnya manusia, teknologi, serta Penelitian dan Pengembangan – R&D) dan untuk penguatan Keamanan Siber dan Pertahanan Siber
3. Pembangunan dan pengembangan sistem Keamanan Siber dan Pertahanan Siber semesta
4. Penentuan prioritas penguatan Sistem Elektronik Infrastruktur Strategis

Sumber National Cyber Defense: https://www.kemhan.go.id/pothan/wp-content/uploads/migrasi/admin/Cyber%20Defence.pdf

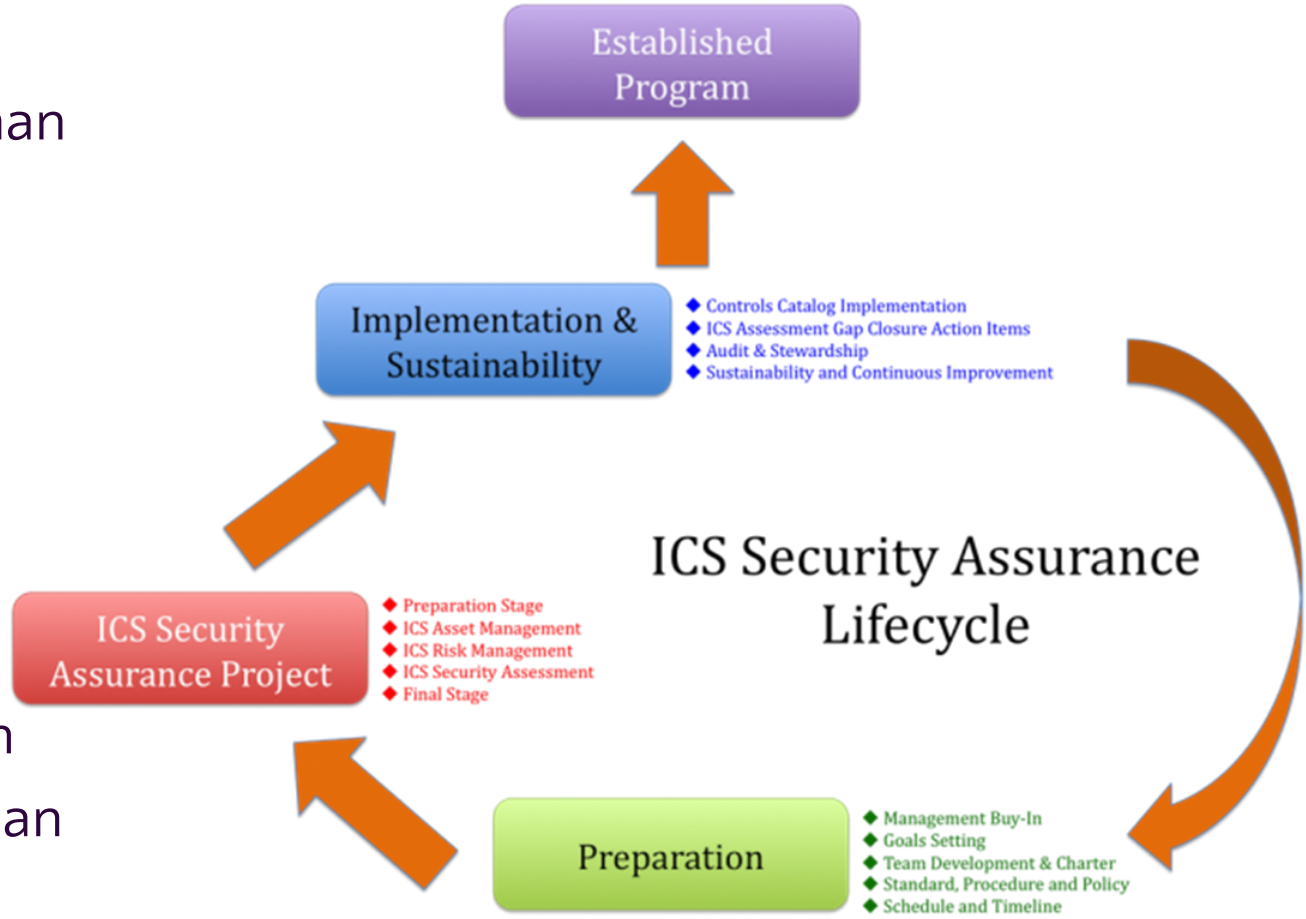
Kebijakan Keamanan Informasi Perusahaan / *Enterprise Infonformation Security Policy (EISP)*

- Menetapkan arah, ruang lingkup, dan rencana strategis untuk upaya keamanan organisasi

1. Menetapkan tanggung jawab untuk berbagai bidang keamanan informasi
2. Memandu pengembangan, implementasi, dan persyaratan manajemen program keamanan informasi

- **Elemen:**

1. Filosofi perusahaan tentang keamanan
2. Struktur organisasi dan peran keamanan informasi

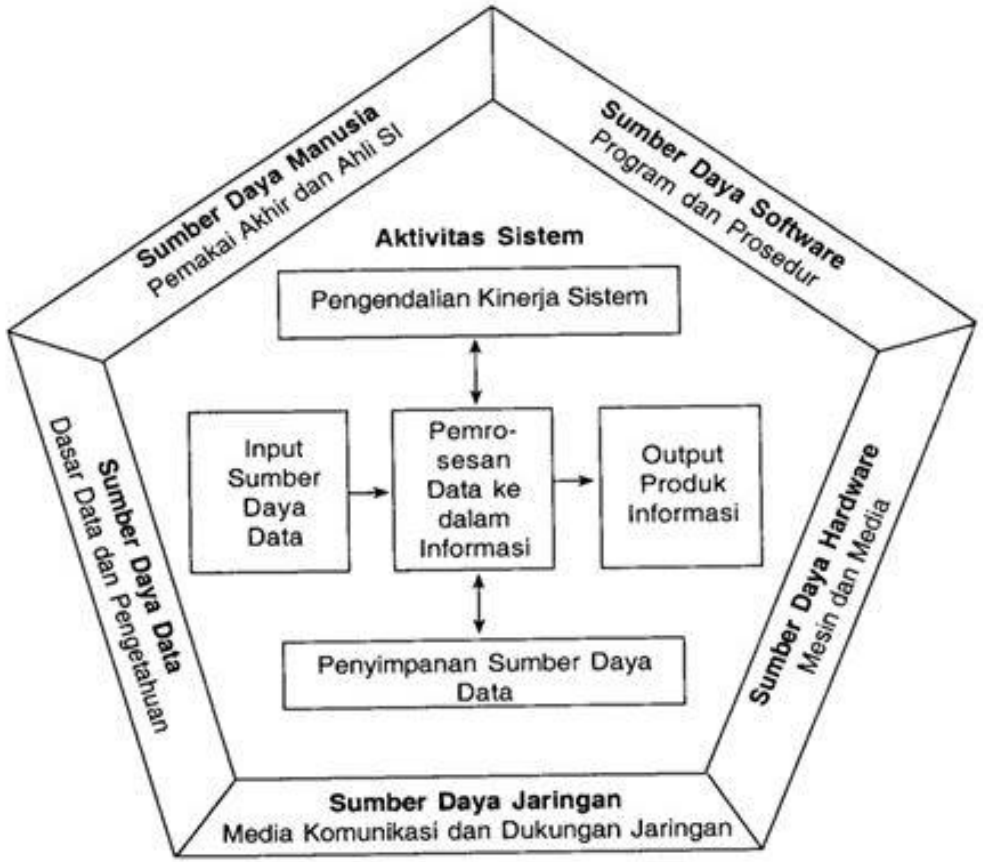


Siklus hidup Keamanan Informasi

- Menurut NIST (*National Institute of Standards and Technology*) Special Publication 80014, "*Generally Accepted Principles and Practices for Securing Information Technology Systems.*". Siklus hidup keamanan informasi merupakan tahapan atau fase yang harus dilalui pada pengembangan keamanan computer.
- Siklus hidup keamanan informasi dibagi menjadi lima fase dasar yaitu **inisiasi, pengembangan/akusisi, impelementasi, operasi dan pembuangan.**

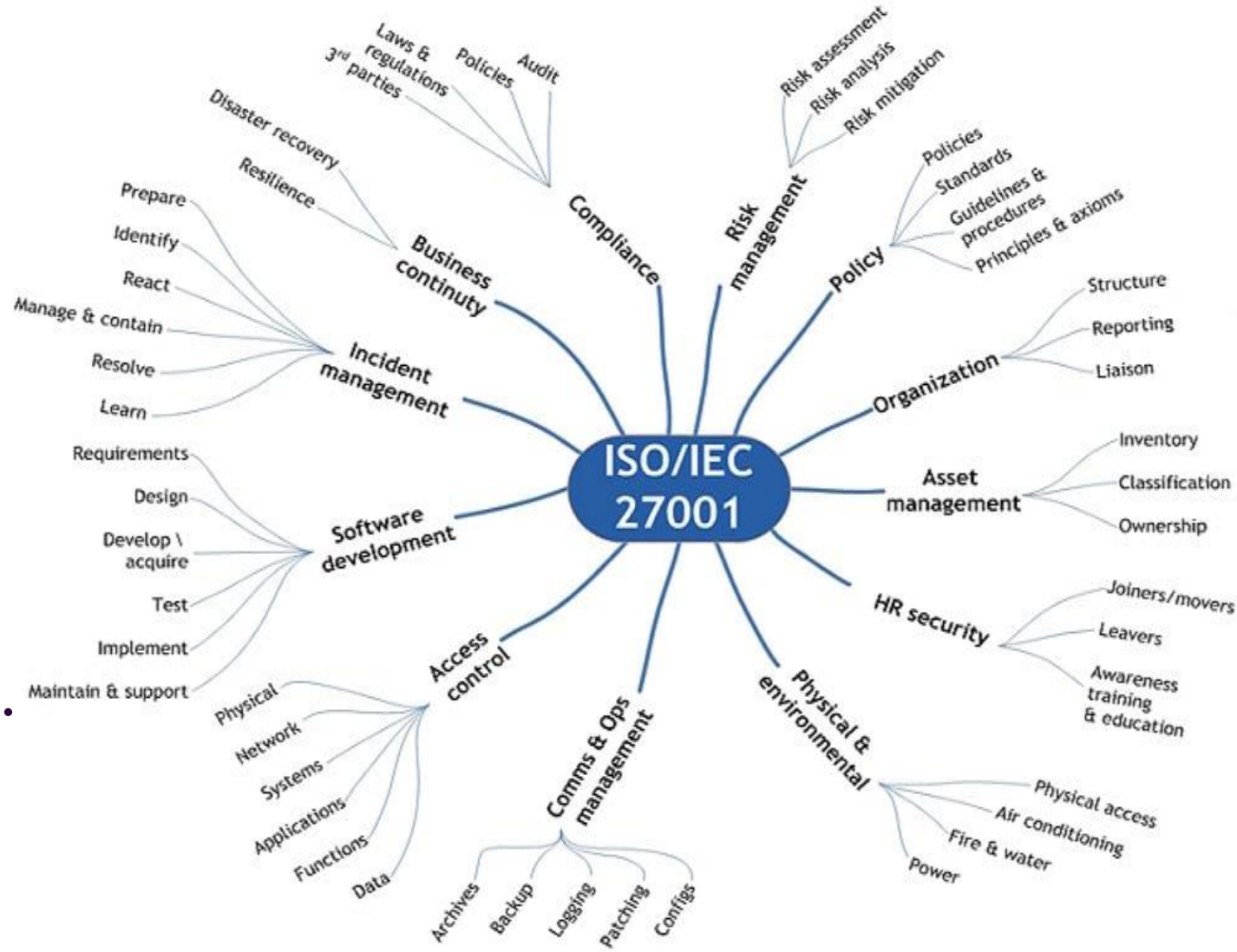
Aset yang dicakup meliputi, tetapi tidak terbatas pada:

- Data dan Informasi
- Software
- Hardware
- Perangkat Jaringan Komunikasi
- Fasilitas Pendukung
- Sumber Daya Manusia



Menurut ISO 27001 Aset Meliputi

- Informasi (information);
- Perangkat lunak (software);
- Perangkat keras (hardware);
- Perlengkapan umum (services);
- Sumber daya manusia (people); dan
- Aset tak berwujud (intangible assets).



Tabel nilai risiko

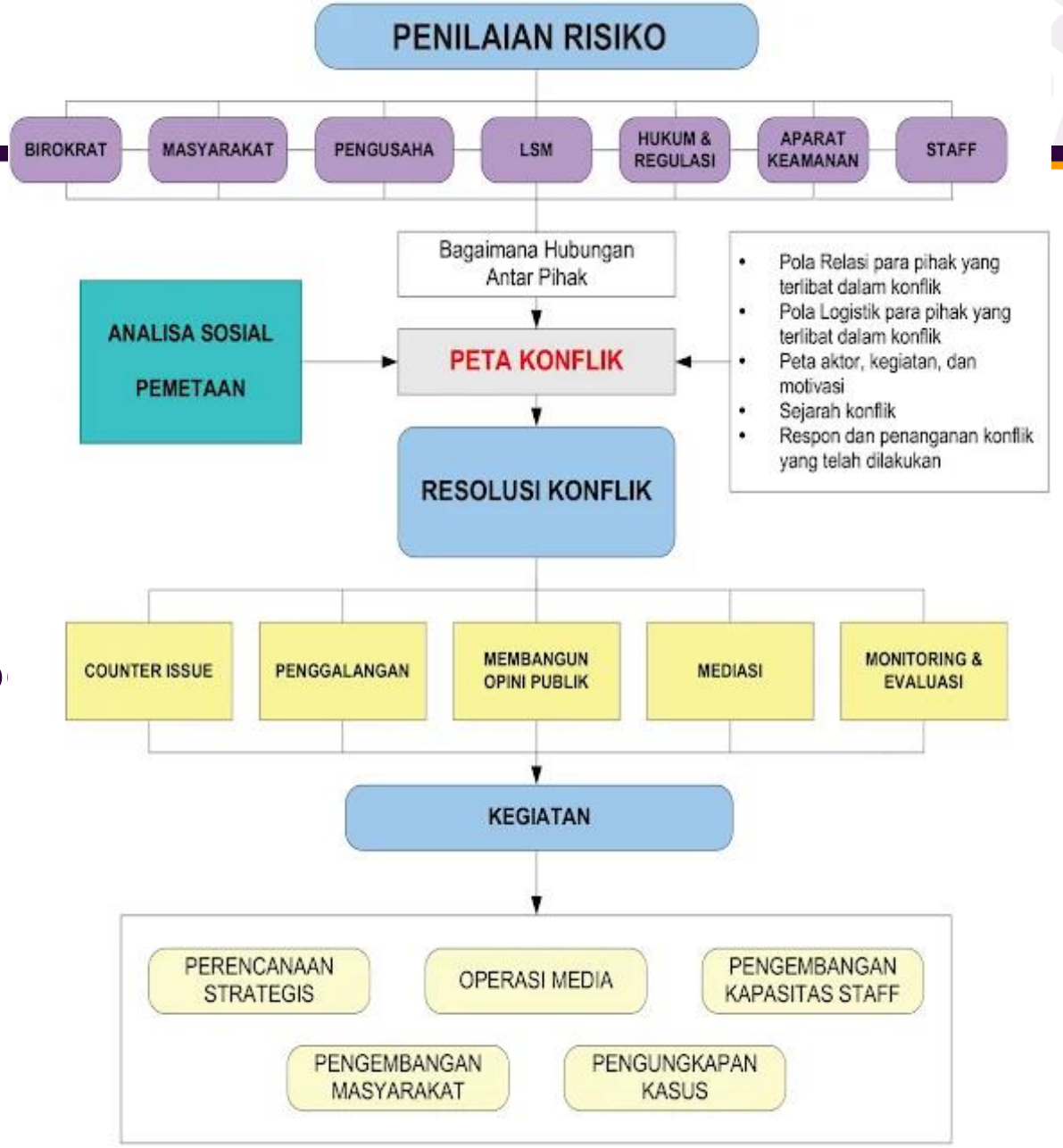
Skoring		Likelihood
1	Sangat kecil	Dapat diabaikan
2	Kecil	Kemungkinan keterjadiannya kecil
3	Sedang	Kemungkinan keterjadiannya sedang
4	Besar	Kemungkinan keterjadiannya besar
5	Sangat besar	Kemungkinan keterjadiannya sangat besar dalam segala situasi

Kepemilikan dan Pemeliharaan Kebijakan

- Kebijakan ini dimiliki oleh divisi teknologi informasi, dipelihara, direview dan diubah oleh divisi teknologi informasi bersama dengan internal audit sesuai dengan kebijakan perusahaan, prosedur, dan panduan.
- Kebijakan ini akan dilakukan review secara periodik (tahunan) dan diajukan kemana komite audit bila terjadi perubahan substansial atau melakukan pemodifikasian konsep kebijakan agar sesuai dengan kebutuhan yang relevan maupun pengelolaan yang efektif.

Elemen utama dari manajemen risiko

- Pengidentifikasian aset informasi
- Analisis kerentanan (vulnerability)
- Pengidentifikasian ancaman (threat)
- Penentuan kemungkinan keterjadian (likelihoo
- Penentuan nilai risiko
- Pemilihan kontrol untuk memitigasi risiko
- Rencana kegiatan saat genting



Security Roles

Senior Management	• Bertanggung jawab secara keselurahan terhadap keamanan • Pengambil kebijakan tertinggi, berpengaruh terhadap keberhasilan/kegagalan
Security Professional	• Menjalankan fungsi tertentu sesuai mandat • Bukan pengambil keputusan
Data Owner	• Bertanggung jawab terhadap data yang mereka miliki • Berisi perwakilan top level management
User	• Memiliki akses ke system • Bertanggung jawab untuk memahami kebijakan keamanan
Auditor	• Bertanggung jawab mereview penerapan kebijakan keamanan • Menghasilakan laporan kepatuhan dan efektifitasnya

Kesimpulan

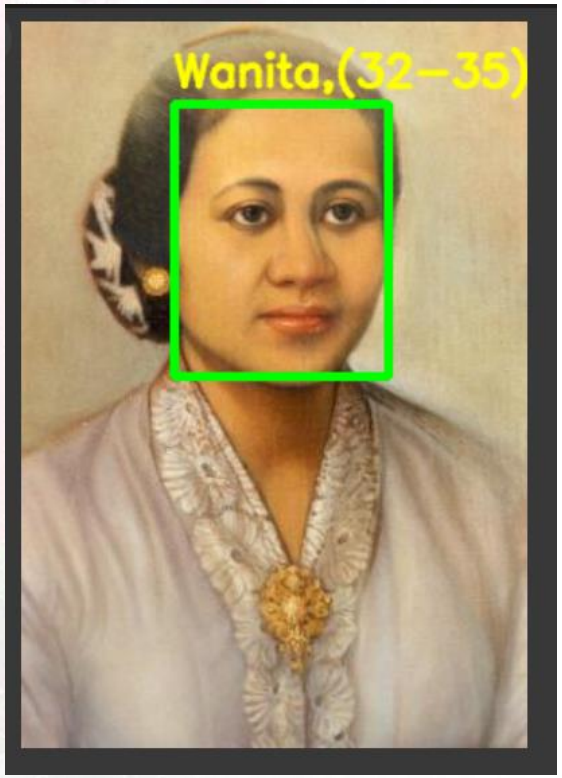
- Bagian terpenting setelah penetapan kebijakan adalah sosialisasi

1. Jika diperlukan melalui pelatihan atau training
2. Menghindari kesalahan penerapan kebijakan secara spesifik
3. Setelah itu perlu dilakukan evaluasi secara berkala

- Kebijakan keamanan yang baik diperlukan untuk mencegah risiko yang mungkin muncul dari manusia
- Kebijakan penting untuk menginformasikan karyawan hal apa yang bisa & tidak bisa diterima perilaku di dalam organisasi
- Kebijakan membantu meningkatkan produktivitas karyawan & mencegah potensi konflik di organisasi

PRAKTEK PENGENALAN WAJAH DAN UMUR

https://colab.research.google.com/drive/1DI_muqHUGlHKilG1zMoK9_N8TntV-iL7?authuser=1



Quotes

"Kechilafan Satu Orang Sahaja Tjukup Sudah Menjebabkan Keruntuhan Negara"

Mayjen TNI Dr. Roebiono Kertopati
(1914 - 1984)
Bapak Persandian Republik Indonesia

	Human, Organisational and Regulatory Aspects
Risk Management & Governance	Security management systems and organisational security controls, including standards, best practices, and approaches to risk assessment and mitigation.
Law & Regulation	International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare.
Human Factors	Usable security, social & behavioural factors impacting security, security culture and awareness as well as the impact of security controls on user behaviours.
Privacy & Online Rights	Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems.
	Attacks and Defences
Malware & Attack Technologies	Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches.
Adversarial Behaviours	The motivations, behaviours, & methods used by attackers, including malware supply chains, attack vectors, and money transfers.
Security Operations & Incident Management	The configuration, operation and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence.
Forensics	The collection, analysis, & reporting of digital evidence in support of incidents or criminal events.
	Systems Security
Cryptography	Core primitives of cryptography as presently practised & emerging algorithms, techniques for analysis of these, and the protocols that use them.
Operating Systems & Virtualisation Security	Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualisation, and security in database systems.
Distributed Systems Security	Security mechanisms relating to larger-scale coordinated distributed systems, including aspects of secure consensus, time, event systems, peer-to-peer systems, clouds, multitenant data centres, & distributed ledgers.
Formal Methods for Security	Formal specification, modelling and reasoning about the security of systems, software and protocols, covering the fundamental approaches, techniques and tool support.
Authentication, Authorisation & Accountability	All aspects of identity management and authentication technologies, and architectures and tools to support authorisation and accountability in both isolated and distributed systems.

TUGAS

	Software and Platform Security
Software Security	Known categories of programming errors resulting in security bugs, & techniques for avoiding these errors—both through coding practice and improved language design—and tools, techniques, and methods for detection of such errors in existing systems.
Web & Mobile Security	Issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models.
Secure Software Lifecycle	The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default.
	Infrastructure Security
Applied Cryptography	The application of cryptographic algorithms, schemes, and protocols, including issues around implementation, key management, and their use within protocols and systems.
Network Security	Security aspects of networking & telecommunication protocols, including the security of routing, network security elements, and specific cryptographic protocols used for network security.
Hardware Security	Security in the design, implementation, & deployment of general-purpose and specialist hardware, including trusted computing technologies and sources of randomness.
Cyber-Physical Systems Security	Security challenges in cyber-physical systems, such as the Internet of Things & industrial control systems, attacker models, safe-secure designs, and security of large-scale infrastructures.
Physical Layer & Telecommunications Security	Security concerns and limitations of the physical layer including aspects of radio frequency encodings and transmission techniques, unintended radiation, and interference.

Any Questions..?

UNIVERSITAS
AMIKOM
YOGYAKARTA