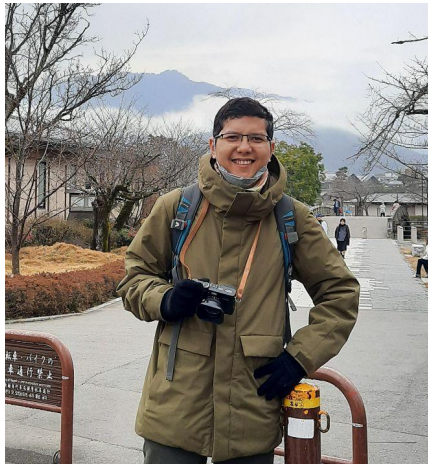
UNIVERSITAS GUNADARMA

Audit Teknologi Sistem Informasi

Risiko dan Pengendalian dalam Audit Teknologi Informasi

Evans Winanda Wirga
Universitas Gunadarma - 24 Maret 2025



Evans Winanda Wirga

evanswinanda@gmail.com
evansww@staff.gunadarma.ac.id
@kacamatadosen

- Roadmap Interoperabilitas Sistem pada Kementerian Kesehatan dan BPJS Kesehatan
- Project Lead Treaty Room System for Ministry of Foreign Affairs RI
- Project Lead Treaty Monitor System for Ministry of Foreign Affairs RI
- Senior Programming and UI/UX in Mhealth Application Kementerian Kesehatan Senior UI/UX in Sistem Informasi Aparatur Sipil Negara (SIASN) - BKN
- etc

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Outline

- Risiko dalam Audit TI
- Pengendalian dalam Audit TI
- Framework dan Regulasi

Mengapa Risiko dan Pengendalian Penting dalam Audit TI?

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Risiko dan Pengendalian

- Teknologi informasi membawa manfaat besar, tetapi juga risiko tinggi
- Risiko dapat menyebabkan kerugian finansial, reputasi, dan operasional
- Pengendalian yang efektif membantu mengurangi dampak risiko

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Risiko

Risiko dalam audit TI adalah potensi kerugian akibat kegagalan sistem, ancaman keamanan, atau kesalahan manusia

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Jenis Risiko

- Risiko Keamanan Informasi
- Risiko Operasional TI
- Risiko Kepatuhan Regulasi
- Risiko Strategis TI

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Faktor Penyebab Risiko

- Ancaman eksternal (serangan siber, malware)
- Ancaman internal (human error, fraud)
- Kegagalan teknologi (sistem crash, data corruption)
- Perubahan regulasi

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Contoh Kasus Risiko

- Kebocoran data pelanggan akibat serangan ransomware
- Gangguan layanan akibat kesalahan konfigurasi sistem
- Denda besar karena ketidakpatuhan terhadap regulasi

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Pengendalian TI

Proses, kebijakan, dan prosedur untuk mengurangi risiko TI

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Jenis Pengendalian

- **Preventif**: Mencegah risiko sebelum terjadi (firewall, enkripsi)
- **Detektif**: Mendeteksi kejadian risiko (log monitoring, audit log)
- **Korektif**: Memperbaiki masalah setelah terjadi (disaster recovery, backup sistem)

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Contoh Implementasi Pengendalian

- Multi-Factor Authentication (MFA) untuk mencegah akses tidak sah
- Monitoring aktivitas sistem untuk mendeteksi anomali
- Backup harian untuk memulihkan data yang hilang

Framework Manajemen Risiko dalam Audit

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Manajemen Risiko

Proses mengidentifikasi, menilai, dan mengurangi risiko TI dalam organisasi

Framework membantu organisasi menerapkan pendekatan sistematis dalam pengelolaan risiko

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Framework Manajemen Risiko

- **COBIT (ISACA)** – Tata kelola dan manajemen risiko TI
- **ISO 27005** – Manajemen risiko keamanan informasi
- **NIST Cybersecurity Framework** – Panduan untuk mengelola keamanan siber
- **COSO ERM** – Enterprise Risk Management untuk tata kelola risiko secara menyeluruh

- **ISO 31000** – Panduan manajemen risiko yang dapat diterapkan pada berbagai sektor

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Siklus Manajemen Risiko TI

- Identifikasi risiko
- Analisis dan evaluasi risiko
- Implementasi pengendalian
- Monitoring dan review

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

COSO Enterprise Risk Management (ERM)

Dikembangkan oleh **Committee of Sponsoring Organizations of the Treadway Commission (COSO)**

Berfokus pada pendekatan menyeluruh dalam pengelolaan risiko perusahaan

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

COSO Enterprise Risk Management (ERM)

Mencakup **8 komponen utama**:

1. Lingkungan internal
2. Penetapan tujuan
3. Identifikasi risiko
4. Penilaian risiko
5. Respon risiko
6. Aktivitas pengendalian
7. Informasi & komunikasi
8. Pemantauan

Kelebihan COSO ERM:

- Fokus pada tata kelola risiko di seluruh organisasi
- Terintegrasi dengan strategi bisnis dan operasional

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

NIST Cybersecurity Framework

Dikembangkan oleh **National Institute of Standards and Technology (NIST)**

Digunakan untuk meningkatkan ketahanan keamanan siber organisasi

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

NIST Cybersecurity Framework

5 Fungsi Utama dalam Framework NIST:

1. **Identify** – Mengidentifikasi aset dan risiko
2. **Protect** – Melindungi sistem dari ancaman
3. **Detect** – Mendeteksi ancaman dan insiden
4. **Respond** – Merespons serangan atau insiden siber
5. **Recover** – Memulihkan sistem setelah insiden

Kelebihan NIST Framework:

- Fokus pada keamanan siber dan risiko TI
- Digunakan secara luas dalam berbagai industri

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

ISO 31000 – Manajemen Risiko

Standar internasional untuk manajemen risiko yang diterbitkan oleh **International Organization for Standardization (ISO)**

Dapat diterapkan di berbagai industri dan sektor, termasuk teknologi informasi

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

ISO 31000 – Manajemen Risiko

3 Prinsip Utama ISO 31000:

1. **Prinsip Manajemen Risiko** – Panduan untuk menerapkan manajemen risiko yang efektif
2. **Kerangka Kerja (Framework)** – Struktur untuk integrasi manajemen risiko dalam organisasi
3. **Proses Manajemen Risiko** – Langkah-langkah sistematis dalam mengelola risiko

Kelebihan ISO 31000:

- Fleksibel dan dapat diterapkan di berbagai sektor
- Berfokus pada pendekatan sistematis dalam pengelolaan risiko

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Mengapa Framework Ini Penting untuk Auditor TI?

Framework	Fokus Utama	Digunakan Oleh	Keunggulan
COSO ERM	Manajemen risiko organisasi	Perusahaan & institusi finansial	Tata kelola menyeluruh
NIST CSF	Keamanan siber & TI	Organisasi teknologi & pemerintahan	Spesifik untuk risiko siber
ISO 31000	Manajemen risiko umum	Berbagai industri	Standar internasional fleksibel

- Membantu auditor TI dalam menilai risiko secara sistematis
- Menyediakan pedoman dalam menerapkan pengendalian risiko
- Memastikan kepatuhan terhadap regulasi dan standar industri

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Contoh Penerapan Manajemen Risiko dalam Perusahaan

- Bank menggunakan monitoring transaksi untuk mendeteksi fraud
- Rumah sakit menerapkan enkripsi data pasien untuk keamanan

Hubungan Risiko, Pengendalian, dan Audit TI

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Bagaimana Auditor TI Mengelola Risiko?

- Menilai efektivitas kontrol yang ada
- Mengidentifikasi kelemahan keamanan sistem
- Merekomendasikan perbaikan pengendalian

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Audit Berbasis Risiko

- Audit TI harus fokus pada area dengan risiko tinggi
- Menilai apakah pengendalian yang diterapkan cukup efektif

Regulasi dan Standar Manajemen Risiko TSI di Indonesia

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Peraturan Otoritas Jasa Keuangan (OJK) – Manajemen Risiko dalam TI

📜 **POJK No. 38/POJK.03/2016 – Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum**

- Mengatur bagaimana perbankan menerapkan manajemen risiko dalam TI
- Menekankan aspek keamanan, pengelolaan data, dan mitigasi risiko TI

📜 **SEOJK No. 21/SEOJK.03/2017 – Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum**

- Merinci POJK 38/2016 dan memberikan panduan implementasi
- Mencakup pengelolaan keamanan siber dan risiko teknologi perbankan

📜 **POJK No. 13/POJK.03/2020 – Tata Kelola Risiko TI dalam Layanan Perbankan Digital**

- Regulasi bagi bank digital dan fintech yang menggunakan layanan digital
- Menekankan **Cyber Resilience, Data Privacy, dan Business Continuity Plan (BCP)**

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Bank Indonesia (BI) – Keamanan dan Manajemen Risiko TI

📜 **PBI No. 9/15/PBI/2007 – Penerapan Manajemen Risiko bagi Bank Umum**

- Mengatur tata kelola risiko TI dalam industri perbankan
- Menyelaraskan dengan standar **Basel II**

📜 **SEBI No. 14/17/DPNP/2012 – Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum**

- Menyediakan pedoman spesifik mengenai pengendalian risiko TI
- Menekankan pada **Business Continuity Management (BCM) dan Information Securit**

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Badan Siber dan Sandi Negara (BSSN) – Keamanan Informasi & Risiko Siber

📜 Peraturan BSSN No. 8 Tahun 2020 – Pedoman Manajemen Risiko Keamanan Siber

- Mengadopsi konsep dari **NIST Cybersecurity Framework**
- Berisi panduan bagi sektor publik dan swasta dalam menangani risiko keamanan siber

📜 Peraturan BSSN No. 4 Tahun 2021 – Manajemen Risiko Keamanan Informasi Berbasis ISO 27005

- Mengatur strategi keamanan informasi berbasis standar **ISO 27005**
- Fokus pada perlindungan data sensitif dalam sistem TI

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Standar Nasional Indonesia (SNI) – Manajemen Risiko dan Keamanan Informasi

📜 **SNI ISO 31000:2018 – Manajemen Risiko – Pedoman Umum**

- Standar resmi dari ISO 31000 yang diterapkan di Indonesia
- Digunakan dalam berbagai sektor termasuk teknologi informasi

📜 **SNI ISO/IEC 27001:2013 – Sistem Manajemen Keamanan Informasi (ISMS)**

- Mengacu pada ISO 27001 yang mengatur tentang **manajemen risiko keamanan informasi**
- Digunakan dalam industri perbankan, pemerintahan, dan perusahaan teknologi

📜 **SNI 8799:2019 – Keamanan Sistem Elektronik**

- Menetapkan standar keamanan untuk sistem elektronik di Indonesia
- Berlaku untuk penyelenggara sistem elektronik (PSE), termasuk perusahaan TI dan layanan cloud

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Undang-Undang dan Regulasi Terkait

📜 **UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)**

- Mengatur aspek keamanan data, transaksi elektronik, dan risiko siber

📜 **UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP)**

- Menetapkan kewajiban bagi organisasi dalam mengelola risiko kebocoran data
- Sejalan dengan standar **ISO 27001 dan GDPR**

📜 **PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE)**

- Mewajibkan perusahaan digital dan layanan TI memiliki sistem manajemen risiko

Studi Kasus – 1

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Serangan Siber terhadap Bank XYZ

Latar Belakang

Bank XYZ adalah salah satu bank digital di Indonesia yang menyediakan layanan perbankan berbasis aplikasi mobile dan internet banking. Bank ini mengalami **serangan siber** yang menyebabkan kebocoran data nasabah dan gangguan operasional.

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Kronologi Insiden

1. **Tahap 1 – Eksploitasi Celah Keamanan**
   - Peretas menemukan **kerentanan dalam API perbankan** yang memungkinkan mereka mengakses data pelanggan tanpa otentikasi yang benar.
   - Mereka melakukan **injeksi kode berbahaya** melalui API yang tidak dilindungi dengan baik.

2. **Tahap 2 – Akses Tidak Sah & Eksfiltrasi Data**
   - Peretas berhasil masuk ke sistem dan mencuri **data rekening nasabah** termasuk saldo, transaksi, dan informasi kartu kredit.
   - Bank XYZ tidak memiliki **monitoring real-time** yang cukup untuk mendeteksi anomali aktivitas pengguna.

3. **Tahap 3 – Dampak dan Krisis Kepercayaan**
   - 50.000 nasabah melaporkan transaksi tidak sah di rekening mereka.
   - Bank XYZ kehilangan reputasi dan mengalami **kerugian finansial** akibat kompensasi ke nasabah.
   - OJK memberikan teguran dan meminta audit menyeluruh atas sistem keamanan TI.

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Analisis Risiko dengan Framework Manajemen Risiko

Framework	Penerapan dalam Kasus Ini
COSO ERM	- Identifikasi risiko: Risiko serangan siber tidak dimitigasi dengan baik. - Respons risiko: Tidak ada strategi mitigasi yang kuat. - Kontrol internal: Sistem tidak memiliki pemantauan real-time dan otentikasi API yang kuat.
NIST Cybersecurity Framework	- **Identify**: Bank tidak melakukan **Risk Assessment** yang memadai terhadap API. - **Protect**: Tidak ada enkripsi data yang kuat. - **Detect**: Tidak ada SIEM (Security Information & Event Management) untuk mendeteksi anomali. - **Respond**: Tanggapan terhadap insiden lambat. - **Recover**: Pemulihan sistem memakan waktu lama dan menyebabkan kerugian finansial.
ISO 31000	- **Risk Identification**: Serangan API Injection tidak dipertimbangkan sebagai ancaman utama. - **Risk Evaluation**: Tidak ada mitigasi terhadap serangan siber melalui API. - **Risk Treatment**: Tidak ada pengamanan tambahan seperti **Multi-Factor Authentication (MFA)** atau enkripsi tambahan.

Pengendalian yang Dapat Diterapkan

- **Menerapkan Zero Trust Security**: Setiap akses ke API harus diverifikasi.
- **Menggunakan Web Application Firewall (WAF)**: Mencegah eksploitasi celah keamanan API.
- **Meningkatkan Enkripsi dan Tokenisasi Data**: Agar data tetap aman meskipun dicuri.
- **Menjalankan Penetration Testing Berkala**: Untuk mengidentifikasi celah keamanan sebelum diretas.
- **Menggunakan SIEM untuk Monitoring Real-Time**: Agar serangan bisa dideteksi sebelum menyebabkan kerusakan besar.

Studi Kasus – 2

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Insiden Keamanan pada Pusat Data Nasional Sementara (PDNS)

Latar Belakang

Pemerintah Indonesia melalui **Kementerian Komunikasi dan Informatika (Kominfo)** membangun **Pusat Data Nasional Sementara (PDNS)** untuk mendukung transformasi digital di sektor pemerintahan. PDNS digunakan oleh berbagai instansi pemerintah untuk menyimpan dan mengelola data, termasuk data kependudukan, keuangan, dan layanan publik.

Pada tahun 2024, PDNS mengalami **serangan siber yang menyebabkan gangguan layanan publik**, seperti layanan kependudukan, pajak, dan perizinan online. Insiden ini menimbulkan **pertanyaan mengenai pengelolaan risiko dan pengendalian dalam infrastruktur TI pemerintah.**

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Kronologi Insiden

1. **Tahap 1 – Eksploitasi Celah Keamanan**
   - Peretas menemukan **kerentanan pada sistem remote access** yang digunakan oleh administrator PDNS.
   - Mereka menggunakan teknik **brute force attack** untuk mendapatkan akses ke akun administrator dengan kredensial lemah.

2. **Tahap 2 – Penyebaran Ransomware**
   - Setelah masuk ke sistem, peretas menyebarkan **ransomware** yang mengenkripsi data di beberapa server PDNS.
   - Sistem layanan kependudukan dan perizinan tidak dapat diakses selama lebih dari **48 jam**.

3. **Tahap 3 – Dampak terhadap Layanan Publik**
   - Masyarakat tidak bisa mengakses layanan administrasi kependudukan seperti **KTP elektronik (e-KTP)** dan **pembuatan paspor**.
   - Layanan keuangan daerah mengalami keterlambatan karena data transaksi tidak bisa diproses.
   - Gangguan ini menyebabkan **kerugian reputasi bagi pemerintah dan kepercayaan masyarakat terhadap sistem digital menurun**.

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Analisis Risiko dengan Framework Manajemen Risiko

Framework	Penerapan dalam Kasus PDNS
COSO ERM	- **Identifikasi risiko**: Risiko serangan ransomware tidak dimitigasi dengan baik. - **Respons risiko**: Tidak ada sistem pemulihan bencana yang cepat. - **Kontrol internal**: Tidak ada pemantauan ketat terhadap akses administrator.
NIST Cybersecurity Framework	- **Identify**: PDNS tidak melakukan **vulnerability assessment** secara rutin. - **Protect**: Tidak ada implementasi **multi-factor authentication (MFA)** untuk akses administrator. - **Detect**: Tidak ada deteksi dini terhadap akses mencurigakan. - **Respond**: Tim IT lambat dalam menanggapi serangan ransomware. - **Recover**: Pemulihan data memakan waktu lebih dari 48 jam.
ISO 31000	- **Risk Identification**: Tidak ada mitigasi khusus untuk risiko ransomware. - **Risk Evaluation**: Risiko keamanan siber tidak dikategorikan sebagai prioritas utama. - **Risk Treatment**: Tidak ada mekanisme backup yang cukup cepat untuk pemulihan data.

Pengendalian yang Dapat Diterapkan

- **Menerapkan Zero Trust Security**: Semua akses administrator harus melalui otentikasi ketat.
- **Menggunakan Endpoint Detection and Response (EDR)**: Untuk mendeteksi anomali dan serangan secara real-time.
- **Mewajibkan Multi-Factor Authentication (MFA)**: Agar tidak ada akses ilegal ke sistem.
- **Melakukan Backup Data Berkala dengan Air-Gap Storage**: Untuk mencegah data dikunci oleh ransomware.
- **Mengadakan Simulasi Serangan Siber (Red Team Exercise)**: Untuk menguji ketahanan sistem terhadap serangan nyata.

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Regulasi dan Standar yang Berlaku di Indonesia

Indonesia memiliki beberapa regulasi yang terkait dengan keamanan Pusat Data Nasional, antara lain:

1. **Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)**
   - Mengatur kewajiban **pengendali data** dalam mengamankan data pribadi di PDNS.
   - Pemerintah harus memastikan bahwa data pribadi tidak bocor akibat serangan siber.

2. **Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE)**
   - Mengatur pengelolaan sistem elektronik pemerintah agar lebih aman dan terintegrasi.

3. **Peraturan Menteri Kominfo No. 4 Tahun 2016 tentang Manajemen Keamanan Informasi**
   - Menetapkan **standar keamanan informasi**, termasuk mitigasi risiko serangan siber.

4. **Keputusan Menteri Kominfo No. 174 Tahun 2023 tentang Pengelolaan Pusat Data Nasional**
   - Mengatur aspek teknis dan operasional Pusat Data Nasional, termasuk aspek keamanan.

Tugas

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Tugas

Pada 11 September 2024, platform perdagangan kripto terbesar di Indonesia, **Indodax**, mengalami serangan siber yang signifikan, mengakibatkan kerugian sekitar Rp 300 miliar. Insiden ini bermula ketika seorang karyawan di bagian pengembangan operasi (dev ops) menerima tawaran pekerjaan sampingan dengan imbalan besar. Tanpa disadari, laptop karyawan tersebut terinfeksi malware yang kemudian menyebar ke server non-kritis perusahaan. Malware ini mengeksploitasi celah keamanan, memungkinkan peretas mengakses sistem internal Indodax.

Investigasi lebih lanjut mengindikasikan bahwa serangan tersebut diduga berasal dari peretas yang terkait dengan Korea Utara. Meskipun demikian, Indodax berhasil memulihkan sistemnya dalam waktu sekitar 80 jam, menjadikannya salah satu pemulihan tercepat dalam industri kripto.

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

- **Analisis Risiko**

  Identifikasilah **lima risiko utama** yang berkontribusi terhadap insiden peretasan ini. Jelaskan bagaimana setiap risiko tersebut dapat terjadi dan dampaknya terhadap operasional serta reputasi Indodax.

- **Evaluasi Framework Manajemen Risiko**

  Pilih **satu framework manajemen risiko** dari **COSO ERM, NIST Cybersecurity Framework, atau ISO 31000**, lalu jelaskan bagaimana framework tersebut dapat diterapkan untuk mengelola dan memitigasi risiko yang ada dalam studi kasus ini. Berikan contoh langkah konkret yang dapat diambil oleh Indodax.

- **Pengendalian Keamanan TI**

  Sebagai auditor TI, rekomendasikan **lima pengendalian keamanan** yang harus diterapkan oleh Indodax untuk mencegah kejadian serupa di masa depan. Jelaskan bagaimana setiap pengendalian ini bekerja dan dampaknya dalam meningkatkan keamanan sistem.

- **Kepatuhan terhadap Regulasi di Indonesia**

  Berdasarkan regulasi keamanan siber dan perlindungan data di Indonesia, seperti **Peraturan Otoritas Jasa Keuangan (POJK) No. 13/POJK.02/2018 tentang Inovasi Keuangan Digital** dan **Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)**, analisis bagaimana regulasi ini dapat membantu dalam pencegahan dan mitigasi insiden seperti yang dialami oleh Indodax.

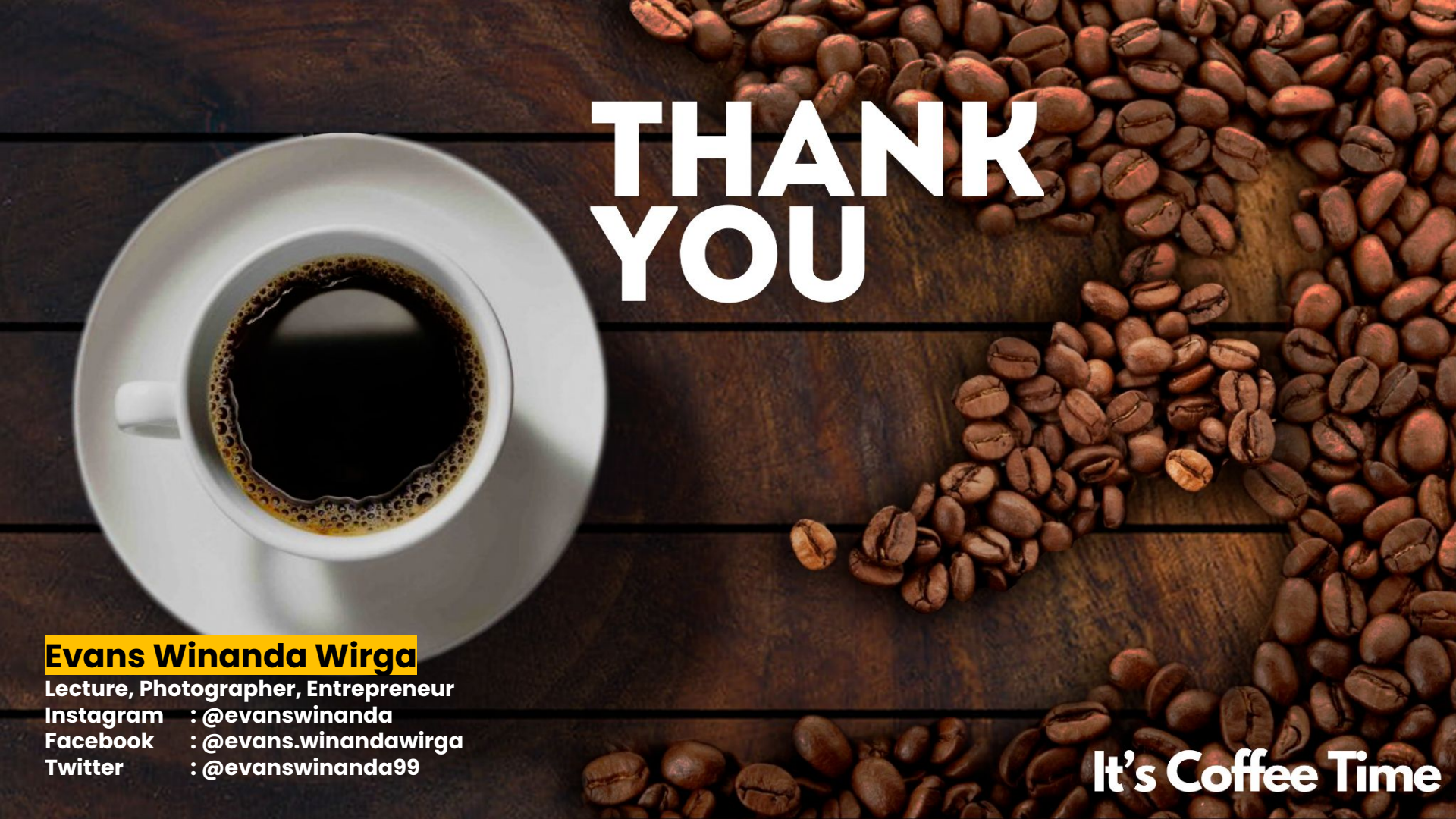
- **Simulasi Audit Keamanan**

  Bayangkan Anda adalah bagian dari tim audit TI yang ditugaskan untuk menilai keamanan Indodax pasca-serangan. Buatlah **tiga pertanyaan audit** yang akan Anda gunakan untuk mengevaluasi keamanan sistem Indodax. Jelaskan juga **mengapa** pertanyaan tersebut penting.

Evans Winanda Wirga
evansww@staff.gunadarma.ac.id

Tugas

- Tugas dikumpulkan 30 April 2025
- Tugas dikerjakan Kelompok
- Menggunakan template yang sudah disediakan.
- Presentasi tugas pada pertemuan berikutnya.



Evans Winanda Wirga
Lecture, Photographer, Entrepreneur
Instagram : @evanswinanda
Facebook : @evans.winandawirga
Twitter : @evanswinanda99

It's Coffee Time