BAB 3
PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Organisasi

Penempatan kerja magang Penulis di Bank Indonesia pada harus sesuai dengan *major* yang telah diambil oleh Penulis di Universitas Multimedia Nusantara sebagai persyaratan kelulusan yaitu pada Departemen Layanan Digital dan Keamanan Siber. Dalam praktik kerja magang di Bank Indonesia selama 4 bulan, Penulis ditempatkan di Grup Ketahanan dan Keamanan Siber Kelompok Pengelolaan, Pengaturan, Koordinasi, dan Edukasi Keamanan Siber. Departemen Layanan Digital dan Keamanan Siber, khususnya Kelompok Pengelolaan, Pengaturan, Koordinasi, dan Edukasi Keamanan Siber bertanggung jawab tehadap memastikan kepatuhan terhadap kebijakan, pedoman, dan standar ketahanan dan keamanan siber (KKS) internal. Adapun Penulis membantu tugas-tugas yang berada di Kelompok Pengelolaan, Pengaturan, Koordinasi, dan Edukasi Keamanan Siber, Penulis menyusun pedoman kebijakan keamanan siber bagi pegawai Bank Indonesia.

Selama Penulis melakukan kegiatan kerja magang dalam *project* penyusunan kebijakan keamanan siber bagi pegawai Bank Indonesia, dikoordinasikan oleh Bapak Diki Tedriana selaku *Assistant Director - Digital Services and Cybersecurity Department* dan Bapak Paskalis Afrian Purba selaku *Assistant Manager - Digital Services and Cybersecurity Department*. Waktu meeting tidak memiliki jadwal yang pasti, namun rapat biasanya dilakukan setiap minggunya untuk melakukan evaluasi terkait perkembangan progress yang telah dilakukan, kendaladan kesulitan yang ditemui.

3.2 Tugas yang Dilakukan

Kegiatan magang di Bank Indonesia dilakukan dengan fokus dalam tiga kegiatan utama dalam atau sesusai dengan *Personal Development Journey* (PDJ) yang telah dibuat dan disepakati oleh mentor didalam satuan kerja penempatan. Berikut adalah rincian kegiatannya:

Tabel 3.1. Learning

Learning	
No	Topik Pembelajaran
1	Kebanksentralan 1
2	Digital Economy and Indonesia Payment System Blueprint 2025
3	Cyber Security and Cyber Resilient on Payment System
4	Transformational Leadership - Basic

Tabel 3.2. Proyek

Proyek / Riset	
No	Target / Output
1	Penyusunan Pedoman Keamanan Siber bagi Pegawai

Tabel 3.3. Working Experience

Working Experience	
No	Uraian Tugas
1	Monitoring keamanan siber di Security Operation Center (SOC)

3.3 Uraian Pelaksanaan Magang

Program magang dilakukan dari 28 Februari sampai 27 Juni 2023 dan berikut adalah *timeline* yang dilakukan selama magang.

Tabel 3.4: Uraian pelaksanaan magang

Minggu ke -	**Pekerjaan yang dilakukan**

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

1	• Gladi Resik Inagurasi dan Pembukaan KMBI • Inaugurasi KMBI V serta Pembukaan KMBI VI dan KMBI Tematik • Program Induksi Hari ke-2 • Program Induksi Hari ke-3

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

2	• Membaca materi tentang Peraturan Anggota Dewan Gubernur (PADG) Nomor 24/51/PADG INTERN/2022 tentang Pengamanan Siber Bank Indonesia • Membaca materi tentang Peraturan Dewan Gubernur (PDG) Nomor 8/17/PDG/2006 tentang Kewajiban Menjaga Informasi Rahasia • Membaca materi tentang PDG Nomor 20/3/PDG/2018 tentang Peraturan Disiplin Bank Indonesia • Membaca materi tentang Pedoman Penggunaan Aset Sistem Informasi yang Aman • Membaca materi tentang Pedoman Penggunaan Email yang Aman • Membaca materi tentang Pedoman Penggunaan Internet yang Aman • Membaca materi tentang Bekerja Secara Aman saat Teleworking • Membaca materi tentang Pedoman Pembentukan Kebijakan Pendukung Operasional Sistem Informasi • Membuat rencana pengerjaan penyusunan pedoman Sistem Informasi • Menyelesaikan administrasi KMBI • Membahas rencana kerja penyusunan Sistem Informasi yang telah dibuat • Membaca materi tentang PADG Nomor 24/51/PADG INTERN/2022 tentang Pengamanan Siber Bank Indonesia • Mengeksplorasi ruang lingkup pengamanan yang belum ada di Bank Indonesia • Membaca materi tentang Prosedur Pengelolaan Insiden Keamanan SI di Bank Indonesia • Membahas Personalised Development Journey • Membaca materi tentang Pedoman Penggunaan Password • Membaca materi tentang Pedoman Non-Disclosure Agreement (NDA) • Melakukan perbandingan pedoman-pedoman yang ada di Bank Indonesia dengan institusi lain terkait Sistem Informasi

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

3	• Melakukan perbandingan pedoman EUD aset sistem informasi yang ada di Bank Indonesia dengan yang ada di institusi lain • Mengeksplorasi pedoman tentang enkripsi • Membaca materi tentang Pedoman Sistem Manajemen Keamanan Informasi berbasis ISO 27001:2013 • Membaca materi tentang pemaparan fungsi dan SDM Satuan Kerja Pengelolaan Inovasi Digital Bank Indonesia • Membaca materi tentang PADG tentang Organisasi Departemen Layanan Digital dan Keamanan Siber • Membuat daftar rangkuman materi pedoman-pedoman pokok terkait keamanan sistem informasi di Bank Indonesia • Melakukan revisi ketiga terhadap rencana pengerjaan pedoman • Memetakan daftar rangkuman materi pedoman-pedoman pokok terkait keamanan sistem informasi di Bank Indonesia • Mempelajari modul learning wajib kebanksentralan 1 sesi 1 • Melakukan revisi keempat terhadap rencana pengerjaan pedoman • Membaca materi tentang pedoman Clear Desk dan Clear Screen • Mempelajari modul pendalaman materi kebanksentralan sesi 1 • Melakukan eksplorasi referensi materi pedoman penggunaan password di luar Bank Indonesia • Membaca materi tentang Information Security Awareness oleh Kementerian Keuangan • Membaca materi tentang Standar Katalog Teknologi Informasi Bank Indonesia Tahun 2022 • Memetakan daftar rangkuman materi pedoman terkait keamanan sistem informasi di luar Bank Indonesia • Mengikuti webinar pendalaman kebanksentralan topik Pengantar Kebanksentralan

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

4	• Membaca materi tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan • Membaca materi tentang Pedoman Keamanan Siber untuk Pegawai Pemerintah Kementerian Elektronik dan Teknologi Informasi India • Melakukan eksplorasi referensi materi pedoman penggunaan password di luar Bank Indonesia • Melanjutkan memetakan daftar rangkuman materi pedoman terkait keamanan sistem informasi di luar Bank Indonesia • Mempelajari modul pendalaman materi kebanksentralan sesi 2 • Membaca materi tentang Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber • Membaca materi tentang Pedoman Pembentukan Kebijakan Pendukung Operasional Sistem Informasi • Membuat draft pedoman berdasarkan kebijakan keamanan sistem informasi yang telah dipetakan • Melanjutkan membuat draft pedoman berdasarkan kebijakan keamanan sistem informasi yang telah dipetakan • Mengikuti webinar pendalaman kebanksentralan topik Moneter
5	• Membaca materi Surat Edaran Direktur Jenderal Pajak No. SE-45/PJ/2020 tentang Pedoman Pengamanan Perangkat dan Fasilitas Pengolahan Data dan Informasi • Melanjutkan membuat draft pedoman berdasarkan kebijakan keamanan sistem informasi yang telah dipetakan • Mempelajari modul learning wajib kebanksentralan 1 sesi 2 • Menyusun latar belakang pedoman kebijakan keamanan sistem informasi • Mempelajari modul learning wajib kebanksentralan 1 sesi 3 • Mempelajari modul pendalaman materi kebanksentralan sesi 3 • Menyusun tujuan pedoman kebijakan keamanan sistem informasi • Mempelajari modul learning wajib kebanksentralan 1 sesi 4 • Mempelajari modul learning wajib kebanksentralan 1 sesi 5 • Mengikuti webinar pendalaman kebanksentralan topik Stabilitas Sistem Keuangan

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

6	• Membuat presentasi berdasarkan materi paparan inisiatif peningkatan cybersecurity awareness Bank Indonesia • Mempelajari modul pendalaman materi kebanksentralan sesi 4 • Mengikuti webinar pendalaman kebanksentralan topik Sistem Pembayaran • Mempelajari modul learning wajib kebanksentralan 1 sesi 6 • Mempelajari modul learning wajib kebanksentralan 1 sesi 7
7	• Membuat presentasi berdasarkan materi paparan inisiatif peningkatan cybersecurity awareness Bank Indonesia • Mempelajari modul pendalaman materi kebanksentralan sesi 5 • Mempelajari modul learning wajib kebanksentralan 1 sesi 8 • Mengikuti pembahasan materi presentasi pop-up quiz untuk CRISP meeting • Mempelajari modul pendalaman materi kebanksentralan sesi 6 • Mempelajari modul pelengkap Transformational Leadership - Basic sesi 1 • Mengikuti webinar pendalaman kebanksentralan topik pengelolaan uang Rupiah • Membaca materi Cybersecurity Resilience and Information Sharing Platform (CRISP) ASEAN • Menyusun laporan akhir magang Bank Indonesia • Mengikuti webinar pendalaman kebanksentralan topik ekonomi digital • Membaca materi Opening Remarks Speech terkait cyber resilience

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

8	• Mengikuti 7th ASEAN DTN-CRISP Meeting - 2023 • Membahas draft pedoman kebijakan keamanan sistem informasi yang telah dibuat • Melakukan revisi terhadap draft pedoman berdasarkan kebijakan keamanan sistem informasi yang telah dipetakan • Mempelajari modul pelengkap Transformational Leadership - Basic sesi 2 • Melanjutkan membuat draft pedoman berdasarkan kebijakan keamanan sistem informasi yang telah dipetakan • Membaca materi tentang pedoman pengamanan penggunaan software Zoom • Mempelajari modul pelengkap Transformational Leadership - Basic sesi 3 • Mempelajari modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System sesi 1 • Mempelajari modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System sesi 2 • Mempelajari modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System sesi 3 • Mempelajari modul learning wajib kebanksentralan 1 sesi 9 • Mempelajari modul learning wajib kebanksentralan 1 sesi 10 • Mempelajari modul pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 sesi 1 • Mempelajari modul pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 sesi 2 • Mempelajari modul learning wajib kebanksentralan 1 sesi 11 • Mempelajari modul learning wajib kebanksentralan 1 sesi 12 • Membaca materi tentang pedoman pengamanan dan penanganan informasi • Membaca materi tentang PDG Nomor 22/1/PDG/2020 Tentang Kode Etik dan Pedoman Perilaku Bank Indonesia • Mempelajari modul pelengkap Transformational Leadership - Basic sesi 4

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

9	• Membuat materi presentasi berdasarkan draft pedoman kebijakan keamanan sistem informasi yang telah dipetakan • Melakukan eksplorasi referensi materi sanksi pelanggaran terhadap kebijakan keamanan Siber di luar Bank Indonesia • Mempelajari modul pelengkap Transformational Leadership - Basic sesi 5 • Menyusun laporan akhir magang Bank Indonesia • Melanjutkan membuat draft pedoman berdasarkan kebijakan keamanan sistem informasi yang telah dipetakan • Melanjutkan membuat materi presentasi berdasarkan draft pedoman kebijakan keamanan sistem informasi yang telah dipetakan • Mempelajari modul pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 sesi 3 • Mempelajari modul pelengkap Transformational Leadership - Basic sesi 6 • Mempelajari modul pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 sesi 4 • Mempelajari modul pelengkap Transformational Leadership - Basic sesi 7 • Mempelajari modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System sesi 4 • Mempelajari modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System sesi 5 • Mempelajari modul pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 sesi 5

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

10	• Menyusun laporan akhir magang Bank Indonesia • Melakukan eksplorasi referensi materi sanksi pelanggaran terhadap kebijakan keamanan Siber di luar Bank Indonesia • Membahas draft materi presentasi pedoman kebijakan keamanan sistem informasi yang telah dipetakan • Melanjutkan membuat materi presentasi berdasarkan draft pedoman kebijakan keamanan sistem informasi yang telah dipetakan • Mengerjakan assignment modul pelengkap Transformational Leadership - Basic • Mempelajari modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System sesi 6 • Mempelajari modul pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 sesi 6 • Melanjutkan membuat draft pedoman berdasarkan kebijakan keamanan sistem informasi yang telah dipetakan • Mempelajari modul pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 sesi 7 • Mempelajari modul pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 sesi 8 • Mengikuti webinar Engagement Enrichment Series KMBI VI Agility, Comfortable in Being Uncomfortable • Mempelajari modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System sesi 7 • Mempelajari modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System sesi 8 • Mempelajari modul pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 sesi 9

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

11	• Melanjutkan membuat materi presentasi berdasarkan draft pedoman kebijakan keamanan sistem informasi yang telah dipetakan • Membaca materi Keputusan Menteri Keuangan RI Nomor 695/KMK.01/2017 tentang kebijakan sistem manajemen keamanan informasi di lingkungan Kementerian Keuangan • Membaca materi Kementerian Keuangan RI Peraturan Direktorat Jenderal Perbendaharaan Nomor PER-1/PB/2021 tentang kebijakan sistem manajemen keamanan informasi di lingkungan Direktorat Jenderal Perbendaharaan • Membaca materi kebijakan dan standar sistem manajemen keamanan informasi di lingkungan Kementerian Keuangan • Mempelajari modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System sesi 9 • Mempelajari modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System sesi 10 • Mengikuti Threat Intelligence Workshop for Bank Indonesia • Membahas draft materi presentasi pedoman kebijakan keamanan sistem informasi yang telah dipetakan • Mempelajari modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System sesi 11 • Mengerjakan assignment modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System • Mengerjakan assignment modul wajib Kebanksentralan 1 menyusun materi short video topik ekonomi digital • Mempelajari modul pilihan SPPUR Cyber Security and Cyber Resilient on Payment System sesi 12 • Mengerjakan assignment modul pelengkap Transformational Leadership - Basic • Mempelajari modul pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 sesi 10 • Membaca materi Cybersecurity Framework Implementation Guidance by CISA • Mempelajari modul pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 sesi 11

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

12	• Menyusun laporan akhir magang Bank Indonesia • Mempelajari modul pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 sesi 12 • Mengerjakan assignment pilihan BI Wide Digital Economy and Indonesia Payment System Blueprint 2025 • Membahas draft materi presentasi pedoman kebijakan keamanan sistem informasi yang telah dipetakan • Melanjutkan membuat materi presentasi berdasarkan draft pedoman kebijakan keamanan sistem informasi yang telah dipetakan • Mengerjakan assignment modul wajib Kebanksentralan 1 menyusun materi short video topik ekonomi digital • Melanjutkan membuat draft pedoman berdasarkan kebijakan keamanan sistem informasi yang telah dipetakan • Mengerjakan tugas video campaign KMBI VI • Mengikuti talkshow dan bedah buku: You Do You penutupan World Book and Copyright Day 2023 • Membaca jurnal Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce • Membaca International Standard ISO/IEC 27001:2013 • Membaca International Standard ISO/IEC 27001:2022 • Mengikuti webinar Engagement Enrichment Series sesi Keeping On Track with Your Goals

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

13	• Menyusun laporan akhir magang Bank Indonesia • Mengerjakan modul learning wajib Kebanksentralan 1 (assessment) • Membaca International Standard ISO/IEC 27002:2013 • Melanjutkan membuat materi presentasi berdasarkan draft pedoman kebijakan keamanan sistem informasi yang telah dipetakan • Membaca NIST Special Publication 1800-21 Mobile Device Security: Corporate-Owned Personally-Enabled (COPE) • Membaca materi tentang pedoman pembentukan kebijakan pendukung operasional sistem informasi Nomor 20/9/DPSI/PDM/B • Mengikuti kegiatan konsinyering pembahasan KAK konsultan penguatan arsitektur siber lingkup teknis: 1. Latar belakang 2. Tujuan 3. Jenis kebutuhan 4. Ruang lingkup pekerjaan • Mengikuti kegiatan konsinyering pembahasan KAK konsultan penguatan arsitektur siber lanjutan lingkup teknis: 1. Latar belakang 2. Tujuan 3. Jenis kebutuhan 4. Ruang lingkup pekerjaan • Mengikuti kegiatan konsinyering pembahasan KAK konsultan penguatan arsitektur siber lingkup teknis: 5. Pendekatan dan metodologi 6. Laporan kemajuan pekerjaan 7. Lokasi pelaksanaan pekerjaan 8. Keluaran (deliverables) • Mengikuti kegiatan konsinyering pembahasan KAK konsultan penguatan arsitektur siber lingkup teknis lanjutan: 5. Pendekatan dan metodologi 6. Laporan kemajuan pekerjaan 7. Lokasi pelaksanaan pekerjaan 8. Keluaran (deliverables) • Mengikuti kegiatan konsinyering finalisasi draf KAK konsultan penguatan arsitektur siber dan SOC • Mengikuti kegiatan konsinyering pembahasan vulnerability management process • Mengikuti kegiatan konsinyering pembahasan vulnerability management process lanjutan • Wrap up hasil konsinyering GKKS

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

14	• Melanjutkan membuat materi presentasi berdasarkan draft pedoman kebijakan keamanan sistem informasi yang telah dipetakan • Membahas draft materi presentasi pedoman kebijakan keamanan sistem informasi yang telah dipetakan • Membaca materi tentang pedoman pembentukan kebijakan pendukung operasional sistem informasi Nomor 20/9/DPSI/PDM/B • Membuat swimlane diagram proses monitoring kepatuhan pedoman kebijakan keamanan siber pegawai • Mengikuti webinar Apple Developer Academy • Menyusun laporan akhir magang Bank Indonesia • Membaca NIST Special Publication 800-46 Revision 2 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security • Membaca jurnal BYOD Security: A Study of Human Dimensions Informatics • Membaca jurnal Bring Your Own Device (BYOD): Legal Protection of the Employee in Malaysia • Membaca jurnal Process for Security Policy and Requirements Development • Melanjutkan membuat draft pedoman berdasarkan kebijakan keamanan sistem informasi yang telah dipetakan • Membaca International Standard ISO/IEC 27001:2013

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

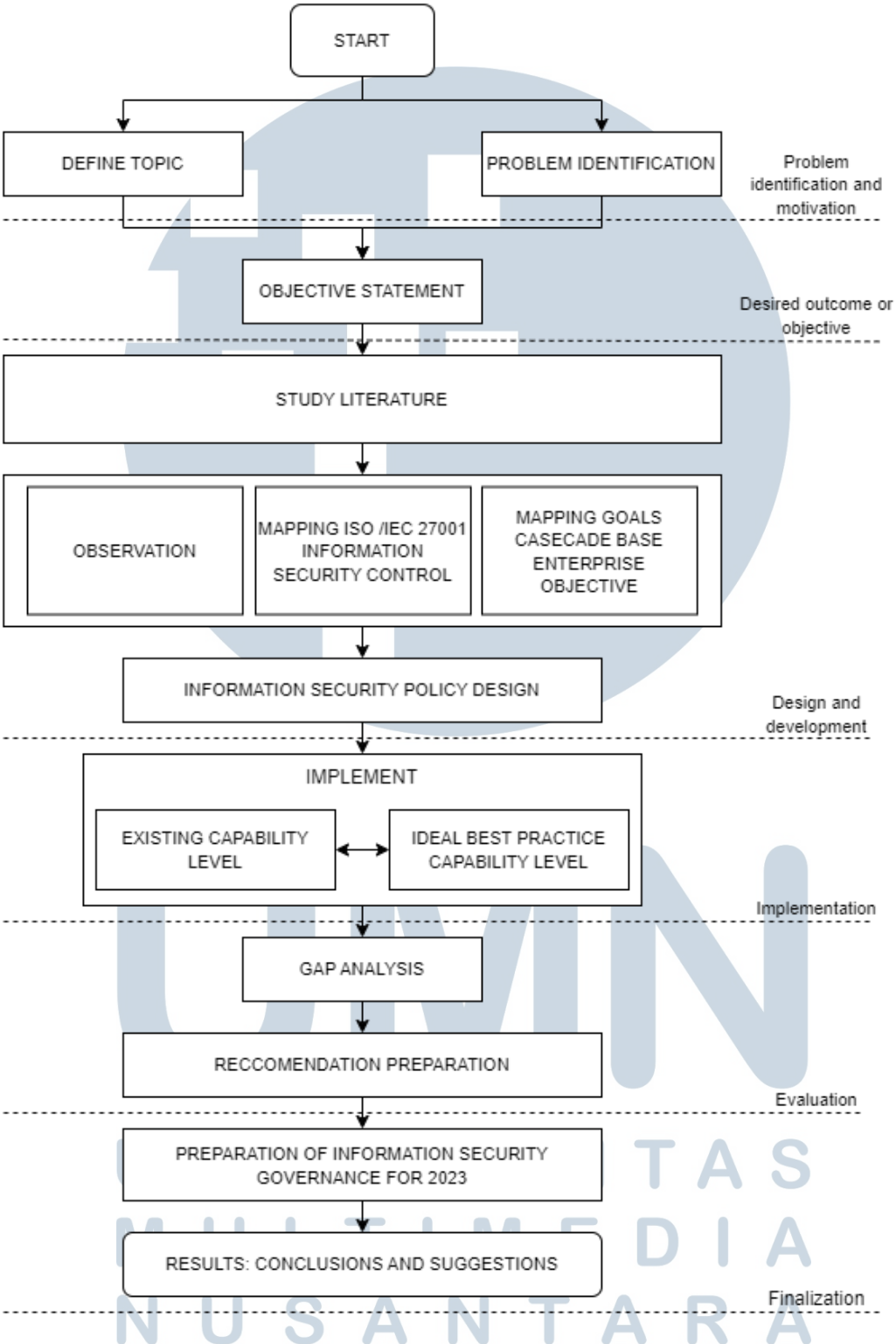
15	• Membaca International Standard ISO/IEC 27001:2022 • Melanjutkan membuat materi presentasi berdasarkan draft Pedoman Kebijakan Keamanan Sistem Informasi yang telah dipetakan • Membaca NIST Special Publication 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations • Membaca NIST Special Publication 800-63 Revision 3 Digital Identity Guidelines • Membaca International Standard ISO/IEC 27001:2013 • Membaca NIST Technical Note 1945 Email Authentication Mechanisms: DMARC, SPF, and DKIM • Membaca COBIT 2019 Framework Introduction and Methodology • Membaca Jurnal ”A Survey of Security Standards Applicable to Health Information Systems” • Membaca Jurnal ”The Organizational Principles of Information Protection Management System Realization” • Menyusun Laporan Akhir Magang Bank Indonesia • Membaca COBIT Focus Area: Information Security • Membaca Temenos Information Systems Security Policy • Membaca Carnegie Mellon Instant Messaging Security and Use Guidelines • Membaca Jurnal ”Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013” (Case Study Ditreskrimsus Polda XYZ)

Continued on next page

Tabel 3.4: Uraian pelaksanaan magang (Continued)

16	• Membahas draft materi presentasi Pedoman Kebijakan Keamanan Sistem Informasi yang telah dipetakan. • Melanjutkan membuat materi presentasi berdasarkan draft Pedoman Kebijakan Keamanan Sistem Informasi yang telah dipetakan. • Membaca pedoman pengelolaan Remote Access VPN. • Menyusun laporan akhir magang Bank Indonesia. • Membaca PDG Bank Indonesia Nomor 10/10/PDG/2008 tentang Manajemen Informasi Bank Indonesia. • Membaca PDG Bank Indonesia Nomor 18/10/PDG/2016 tentang Sistem Informasi Bank Indonesia. • Mengikuti meeting pembahasan draf materi Kickoff dan rencana simulasi Table Top ASEAN CRISP. • Membaca jurnal integrasi antara framework ISO 27001 dan COBIT 2019 pada keamanan informasi di PT. YoY Manajemen Internasional. • Membaca jurnal comparative study between the integration of ITIL and ISO / IEC 27001 with the integration of COBIT and ISO / IEC 27001. • Melanjutkan membuat draft pedoman berdasarkan Kebijakan Keamanan Sistem Informasi yang telah dipetakan. • Mengikuti webinar Engagement and Enrichment topik The Art of Communication/Personal Branding (CV).

Tugas utama yang dilakukan oleh Penulis selama magang di Bank Indonesia adalah menyusun pedoman keamanan siber yang komprehensif untuk pegawai Bank Indonesia. Pedoman kebijakan keamanan informasi yang jelas dan ringkas dalam kebijakan ini mencakup kontrol akses, manajemen insiden, klasifikasi data, dan topik-topik terkait lainnya. Pedoman ini mencerminkan tren dan standar saat ini sebagai hasil dari penelitian ekstensif Penulis mengenai *best practice* keamanan informasi nasional dan internasional. Gambar dibawah menunjukkan tahapan-tahapan yang dilakukan dalam penelitian proyek magang yang dilakukan Penulis.



Gambar 3.1. Skema metodologi penelitian

3.3.1 Identifikasi Masalah dan Motivasi

Mengamankan informasi sensitif merupakan perhatian utama bagi organisasi dari setiap industri. Terutama bagi lembaga keuangan seperti Bank Indonesia yang menyimpan data sensitif dalam jumlah besar. Untuk memastikan keamanan sistem informasinya, Bank Indonesia telah menerapkan serangkaian kebijakan yang komprehensif yang bertujuan untuk meningkatkan kesadaran dan kepatuhan pegawai. Namun, pedoman kebijakan di Bank Indonesia masih tersebar di berbagai dokumen dan sumber yang berbeda. Hal ini berpotensi menimbulkan ketidakkonsistenan dan kesulitan bagi pegawai untuk memahami dan mematuhi kebijakan tersebut. Oleh karena itu, diperlukan suatu pedoman yang terpadu, komprehensif, dan mudah diakses oleh semua pihak yang terlibat.

Selain itu, tidak ada tindak lanjut yang jelas bagi pegawai yang melanggar pedoman keamanan siber di Bank Indonesia. Hal ini menyebabkan kurangnya akuntabilitas dan menciptakan potensi risiko pelanggaran dan serangan siber. Untuk mengatasi masalah ini, kebijakan disipliner yang jelas dan konsisten untuk pelanggaran keamanan siber sangat penting. Bank Indonesia harus menerapkan kebijakan ini melalui pelatihan rutin dan kegiatan peningkatan kesadaran. Selain itu, Bank Indonesia disarankan untuk menerapkan sistem pemantauan untuk melacak dan melaporkan pelanggaran dan menegakkan kebijakan tersebut.

3.3.2 Hasil atau Tujuan yang Diinginkan

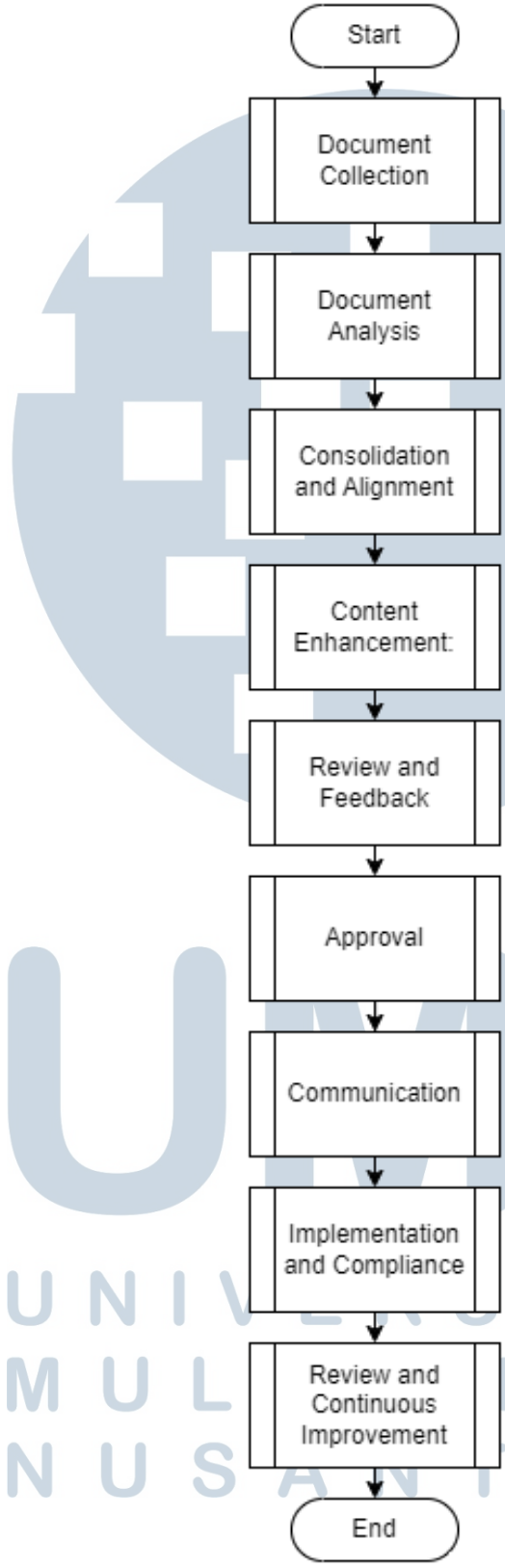
Tujuannya adalah untuk mengembangkan dan mengimplementasikan pedoman kebijakan keamanan siber yang terpadu dan komprehensif untuk Bank Indonesia. Pedoman keamanan siber ini harus mencakup seluruh tugas yang dilakukan di Bank Indonesia, termasuk standar dan manajemen *password*, perilaku yang diharapkan untuk semua pegawai yang mengakses jaringan Bank Indonesia atau menggunakan perangkat PC/*notebook* mereka untuk mengakses data Bank Indonesia di luar kantor, ekspektasi keamanan jaringan dan akses jarak jauh seperti autentikasi dua faktor dan *virtual private network*, serta kebijakan keamanan *end user device* untuk memitigasi risiko yang terkait dengan penggunaan perangkat pribadi untuk mengakses data Bank Indonesia. Kebijakan ini berlaku bagi seluruh pegawai Bank Indonesia, terlepas dari jabatan, peran dan lokasi mereka. Kebijakan ini juga berlaku bagi pihak ketiga yang mengakses sistem informasi atau data Bank Indonesia, seperti vendor, konsultan, atau auditor. Seluruh pegawai harus mematuhi

kebijakan ini dan prosedur terkait lainnya yang mungkin dikeluarkan oleh Bank Indonesia dari waktu ke waktu.

Selain itu, tujuannya adalah untuk menetapkan kebijakan disipliner yang kuat untuk pelanggaran pedoman keamanan siber di Bank Indonesia. Kebijakan ini harus secara jelas mendefinisikan konsekuensi tindak lanjut atas kegagalan dalam mematuhi kebijakan keamanan siber dengan mengembangkan dan mengimplementasikan sistem pemantauan untuk pelacakan dan pelaporan pelanggaran keamanan siber. Sistem ini harus memungkinkan deteksi proaktif terhadap perilaku yang tidak patuh, pelaporan insiden secara tepat waktu, dan penegakan disiplin yang efektif. Sistem ini harus memberikan visibilitas ke dalam aktivitas pegawai yang terkait dengan keamanan siber, seperti mengakses data sensitif atau mencoba melakukan tindakan yang tidak sah.

3.3.3 Perancangan dan Pengembangan

Penulis menggunakan tinjauan literatur kualitatif sebagai metode penelitian untuk memberikan analisis mendalam mengenai praktik keamanan siber Bank Indonesia saat ini dan mengidentifikasi potensi *gap* atau area yang perlu ditingkatkan. Kajian ini mencakup analisis komprehensif terhadap jurnal ilmiah, *white paper*, dan dokumen kebijakan. Untuk lebih memahami kebijakan keamanan siber yang ada dan kesulitan-kesulitan yang dihadapi organisasi, Penulis juga berkonsultasi dengan anggota tim keamanan siber Bank Indonesia. Berikut langkah-langkah yang dilakukan Penulis dalam tahap perancangan dan pengembangan pedoman Bank Indonesia untuk membangun budaya keamanan siber yang menekankan pentingnya keamanan informasi di semua aspek operasi organisasi untuk meningkatkan kesadaran dan kepatuhan pegawai.



Gambar 3.2. Langkah-langkah Tahap Perancangan dan Pengembangan

Mendapatkan dokumen pedoman keamanan siber terkini dari Bank Indonesia adalah proses pengumpulan dokumen. Dokumen-dokumen ini didapatkan dari *website* internal Bank Indonesia. Dokumen-dokumen ini memberikan *framework* tentang persyaratan dan saran spesifik dari regulator. Setelah mendapatkan bahan-bahan tersebut, langkah penting berikutnya adalah mengumpulkan semua dokumen kebijakan dan pedoman yang relevan terkait keamanan informasi. Hal ini akan membutuhkan pencarian menyeluruh terhadap kebijakan internal, *best practice*, dan materi relevan lainnya yang dapat membantu pembuatan *framework* keamanan siber yang kuat.

Dokumen-dokumen pedoman yang diperoleh oleh Penulis ditinjau dan dianalisis dengan hati-hati selama tahap analisis dokumen. Ada tiga jenis dokumen yang ada di Bank Indonesia, yaitu standar, pedoman, dan petunjuk teknis (juknis). Setiap dokumen harus diperiksa untuk memahami sepenuhnya konten dan implikasinya. Tujuannya adalah untuk menemukan tema-tema yang sama, tumpang tindih, dan *gap* dalam kebijakan yang ada saat ini. Analisis komparatif memungkinkan untuk mengidentifikasi area-area di mana kebijakan-kebijakan selaras dan saling menguatkan. Penulis juga mengidentifikasi kontradiksi atau *gap* dalam kebijakan, menyoroti area yang mungkin memerlukan pedoman tambahan. Untuk membangun gambaran menyeluruh tentang kondisi pedoman keamanan siber saat ini di Bank Indonesia, langkah ini sangat penting untuk mensintesis data yang dikumpulkan dari berbagai sumber.

Selama langkah konsolidasi dan penyelarasan, data dan bagian yang relevan dari dokumen yang ada khususnya dokumen pedoman diintegrasikan ke dokumen baru untuk membuat pedoman kebijakan keamanan siber yang terorganisir dan menyeluruh. Hal ini memastikan bahwa dokumen akhir mencerminkan kebutuhan dan persyaratan spesifik Bank Indonesia dengan memilih dan mengintegrasikan kebijakan yang paling relevan dari berbagai sumber secara hati-hati. Dengan menyelaraskan kebijakan, diharapkan juga dapat mendorong konsistensi dan keseragaman konten pedoman yang disusun. Proses ini melibatkan penyelarasan terminologi dan penghilangan ketidakkonsistenan serta pengulangan. Dengan menggabungkan dan menyelaraskan prinsip-prinsip tersebut, Penulis dapat membuat dokumen pedoman yang terpadu dan mudah diakses yang memberikan panduan yang jelas dan dapat ditindaklanjuti untuk mengimplementasikan tindakan keamanan siber yang efektif. Selama proses penyusunan, Penulis mengacu pada Pedoman Pembentukan Kebijakan Pendukung Operasional Sistem Informasi dari Bank Indonesia. Hal ini dilakukan untuk mengembangkan pedoman kebijakan

keamanan siber dengan menggunakan prosedur dan metodologi yang terstandarisasi oleh Bank Indonesia.

Selama menyusun pedoman keamanan siber Bank Indonesia, Penulis menyadari pentingnya menyelaraskan pedoman dengan standar dan *framework* internasional sebagai tahap peningkatan konten. Bank Indonesia dapat memperkuat postur keamanan sibernya dan memastikan kesesuaian dengan standar global dengan memanfaatkan *best practice* yang ada. Penulis secara ekstensif meneliti dan merujuk pada beberapa *framework* standar internasional, termasuk seri ISO/IEC 27000 dan *Framework* NIST Cybersecurity. Pedoman ini menawarkan *framework* untuk pengembangan dan penggunaan kontrol keamanan yang sesuai untuk menangani ancaman yang teridentifikasi dan melindungi aset penting berdasarkan *best practice* industri.

ISO adalah pemimpin global dalam menyediakan standar teknologi informasi, pedoman, dan solusi untuk membantu organisasi membangun dan memelihara sistem manajemen keamanan informasi yang efektif. ISO telah mengembangkan seri standar keamanan informasi ISO/IEC 27000, yang berfungsi sebagai *framework* untuk *best practice* Sistem Manajemen Keamanan Informasi (ISMS). Sebuah organisasi dapat melindungi aset informasinya dengan Sistem Manajemen Keamanan Informasi (SMKI). Organisasi membutuhkan Sistem Manajemen Keamanan Informasi (SMKI) untuk membantu melindungi aset informasi [17] [18]. Semua organisasi baik di sektor komersial maupun non-komersial diwajibkan untuk mematuhi seri ISO/IEC 27000. Rangkaian standar keamanan informasi yang paling lengkap adalah seri ISO/IEC 27000. Seri ini memberikan cara sistematis bagi organisasi untuk menangani risiko keamanan informasi, melindungi data sensitif, dan menjamin ketersediaan, integritas, dan kerahasiaan informasi.

Beberapa komponen utama dari seri ISO/IEC 27000 yang selaras dengan tujuan keamanan siber Bank Indonesia adalah sebagai berikut:

1. *Security Governance and Management*: Manajemen keamanan informasi adalah pendekatan yang terstruktur dan sistematis. Hal ini mencakup penetapan kebijakan, definisi peran dan tanggung jawab, serta pelaksanaan penilaian risiko dan manajemen risiko secara berkala.

2. *Risk Assessment and Treatment*: Mengidentifikasi dan menilai risiko keamanan informasi serta menerapkan kontrol yang tepat untuk memitigasi risiko tersebut. Komponen ini membantu Bank Indonesia dalam

mengembangkan pendekatan berbasis risiko terhadap keamanan siber.

3. *Access Control*: Komponen ini memberikan pedoman untuk menerapkan kontrol akses yang sesuai untuk menjamin bahwa hanya orang yang memiliki autorisasi yang tepat yang dapat mengakses informasi dan sistem yang sensitif.

4. *Incident Management*: Komponen ini menjelaskan langkah-langkah yang harus diambil untuk menangani masalah keamanan informasi, termasuk bagaimana mencegah terjadinya masalah tersebut dan bagaimana menanggapinya. Bagian ini membantu Bank Indonesia untuk membuat rencana manajemen insiden yang efisien.

5. *Data Classification*: Komponen ini menyoroti perlunya klasifikasi data berdasarkan sensitivitasnya dan penerapan langkah-langkah yang tepat untuk melindungi data tersebut. Komponen ini membantu Bank Indonesia untuk melindungi data sensitif secara efektif.

National Institute of Standards and Technology (NIST) adalah sebuah organisasi di dalam Departemen Perdagangan Amerika Serikat yang tidak memiliki otoritas regulasi. NIST menciptakan dan mendukung standar pengukuran keamanan siber, teknologi, dan pedoman untuk meningkatkan daya saing dan keamanan perusahaan Amerika.[19]. *Framework* NIST Cybersecurity yang dikembangkan oleh NIST di Amerika Serikat merupakan pendekatan yang diterima secara luas untuk memfasilitasi manajemen risiko keamanan siber dalam organisasi [20]. *Framework* NIST Cybersecurity menyediakan pendekatan yang fleksibel dan dapat disesuaikan untuk manajemen dan mitigasi risiko keamanan siber. *Framework* ini mencakup standar, pedoman, dan *best practice* yang berasal dari standar industri yang ada [21].

Bank Indonesia harus memastikan bahwa pedoman kebijakan keamanan sibernya sejalan dengan *best practice* industri dan menjadi landasan yang kuat untuk melindungi informasi sensitif dengan mengikuti standar dan *framework* internasional. Selain meningkatkan postur keamanan organisasi, strategi ini akan mempermudah dalam membandingkan kinerja dengan standar industri dan bekerja sama dengan mitra internasional dalam memerangi ancaman keamanan siber. Dalam rangka menetapkan kebijakan dan proses keamanan informasinya, Bank Indonesia dapat menggunakan seri ISO/IEC 27000 dan *Framework* NIST Cybersecurity sebagai sumber referensi utama.

Selama tahap peninjauan dan umpan balik, penting untuk meminta umpan balik dari tim keamanan siber Bank Indonesia. Pengetahuan dan perspektif mereka dapat memperkuat pedoman kebijakan yang disusun oleh Penulis. Penting untuk mengevaluasi dan mempertimbangkan masukan dari para tim keamanan siber Bank Indonesia secara menyeluruh. Sangat penting untuk mempertimbangkan semua komentar, ide, dan saran dari mereka. Tujuannya adalah untuk meningkatkan kualitas dan efektivitas pedoman dengan memasukkan kritik mereka yang mendalam.

Sangat penting untuk mendapatkan persetujuan resmi dari pihak yang berwenang pada tahap persetujuan pedoman kebijakan sebelum memasuki tahap selanjutnya. Bergantung pada bentuk dan *framework* tata kelola organisasi, otoritas ini bisa berbeda-beda. Pedoman harus melalui proses peninjauan sebelum disetujui untuk memastikan bahwa pedoman tersebut sesuai dengan tujuan strategis organisasi, persyaratan hukum, dan praktik bisnis yang telah ditetapkan. Setelah ditinjau dan dinyatakan sesuai, pedoman tersebut harus dipresentasikan untuk mendapatkan persetujuan. Penyerahan dokumen pedoman, dokumen tambahan yang diperlukan, dan rekomendasi apa pun kepada otoritas yang berwenang adalah prosedur umum untuk prosedur ini. Otoritas akan menilai dokumen pedoman yang telah disusun oleh Penulis berdasarkan seberapa baik pedoman tersebut sesuai dengan tujuan organisasi dan persyaratan hukum. Mendapatkan persetujuan resmi menunjukkan dukungan dan pengesahan dari otoritas yang berwenang terhadap pedoman. Tahap persetujuan merupakan tonggak utama dalam pengembangan dan penerapan kebijakan keamanan siber yang baik.

Selama tahap komunikasi dokumen pedoman, penting untuk mengkomunikasikan pedoman kebijakan keamanan siber secara efektif kepada semua pegawai Bank Indonesia. Untuk menjaga keamanan informasi, sangat penting bagi pegawai untuk mengetahui kebijakan tersebut dan memahami kewajiban mereka. Dokumen pedoman kebijakan keamanan siber harus segera didistribusikan kepada semua pegawai yang terkait. Hal ini bisa dilakukan melalui berbagai metode komunikasi, salah satunya email. Pentingnya standar dalam menjaga integritas data, melindungi informasi sensitif, dan mengurangi risiko keamanan siber harus ditekankan dalam komunikasi. Selain didistribusikan, sangat penting untuk memastikan bahwa pegawai memahami pedoman kebijakan.

Penekanan dari tahap implementasi dan kepatuhan dokumen pedoman ini adalah pada pelaksanaan pedoman kebijakan secara efisien di seluruh sistem dan prosedur di Bank Indonesia. Hal ini mencakup pengubahan kebijakan

menjadi prosedur yang dapat dilakukan dan memastikan bahwa kebijakan tersebut dimasukkan ke dalam alur kerja dan praktik yang ada. Untuk menjamin kepatuhan yang berkelanjutan terhadap kebijakan, prosedur pemantauan harus ditetapkan. Pemantauan dan penilaian rutin dilakukan selama tahap implementasi untuk memastikan pedoman kebijakan tersebut dipatuhi. Hal ini mencakup pemantauan aktivitas sistem dan menganalisis log keamanan untuk setiap anomali. Hal ini mencakup evaluasi secara berkala terhadap efisiensi kebijakan dan memastikan bahwa kebijakan tersebut ditaati. Pemantauan membantu dalam menemukan area mana saja yang perlu ditingkatkan atau dapat menimbulkan masalah keamanan. Tujuan keseluruhan dari tahap implementasi adalah menerapkan kebijakan ke dalam praktik, dan memantau kepatuhan secara teratur. Di tahap ini, Penulis bertanggung jawab untuk membuat skema tindak lanjut bagi pegawai yang melanggar pedoman kebijakan. Hal ini mencakup pengembangan *framework* yang menguraikan konsekuensi atas ketidakpatuhan terhadap kebijakan yang telah ditetapkan.

Pemetaan sanksi dilakukan berdasarkan tiga kategori pelanggaran diantaranya *low*, *medium*, dan *high*. Tujuan pemetaan sanksi adalah untuk memastikan konsistensi dalam menangani pelanggaran kebijakan. Pemetaan sanksi memberikan pedoman yang jelas untuk menangani berbagai tingkat ketidakpatuhan dan membantu meningkatkan akuntabilitas di antara para pegawai. Dengan memetakan sanksi yang sesuai untuk setiap kategori pelanggaran, Penulis membantu menciptakan sistem di mana pegawai memahami konsekuensi dari tindakan mereka dan termotivasi untuk mematuhi pedoman kebijakan. Melalui upaya tersebut, Penulis berkontribusi dalam menjaga lingkungan yang aman dengan meningkatkan kesadaran pegawai di Bank Indonesia.

Selama tahap peninjauan dan peningkatan berkelanjutan dari dokumen pedoman, sangat penting untuk meninjau dan memperbarui kebijakan keamanan siber secara berkala untuk memastikan keefektifannya yang berkelanjutan. Hal ini mencakup evaluasi efektivitas dan penerapan kebijakan saat ini dan menunjukkan peluang untuk perbaikan. Dengan melakukan tinjauan ini, Bank Indonesia dapat memastikan bahwa kebijakan mereka tetap mutakhir dan selaras dengan standar industri dan persyaratan peraturan terbaru. Umpan balik dari berbagai sumber, termasuk audit, insiden keamanan, dan tren yang muncul, memainkan peran penting dalam membentuk proses peningkatan berkelanjutan. Temuan audit memberikan informasi tentang kekuatan dan kelemahan kebijakan. Hal ini memungkinkan Bank Indonesia untuk mengatasi *gap* atau kekurangan yang teridentifikasi. Melalui analisis insiden keamanan, Bank Indonesia dapat memperoleh pemahaman tentang

potensi kerentanan atau risiko baru yang mungkin belum ditangani dalam kebijakan saat ini. Selain itu, organisasi dapat secara proaktif menyesuaikan kebijakan mereka untuk mengurangi ancaman yang berkembang dengan tetap mengikuti tren dan teknologi yang muncul dalam lanskap keamanan siber.

Tahap peninjauan dan peningkatan berkelanjutan adalah proses berkelanjutan yang memastikan kebijakan berkembang seiring dengan perubahan lanskap ancaman. Dengan meninjau dan memperbarui kebijakan keamanan siber secara teratur, memasukkan umpan balik dari berbagai sumber, dan tetap proaktif dalam menangani ancaman dan teknologi yang muncul, Bank Indonesia dapat mempertahankan postur keamanan yang kuat dan secara efektif melindungi aset mereka. Pendekatan berulang ini membantu Bank Indonesia tetap tangguh dalam menghadapi tantangan keamanan siber yang terus berkembang, serta menumbuhkan budaya peningkatan dan kemampuan beradaptasi yang berkelanjutan.

3.3.4 Implementasi

Bank Indonesia harus menerapkan tingkat kapabilitas yang ada dan yang ideal untuk menunjukkan efektivitas pedoman keamanan siber yang diusulkan. Tingkat kapabilitas yang ada saat ini mewakili praktik keamanan siber organisasi saat ini, sedangkan tingkat kapabilitas ideal menguraikan kondisi yang diinginkan yang konsisten dengan praktik terbaik industri. Dengan mengidentifikasi *gap* antara tingkat kapabilitas saat ini dan tingkat kapabilitas ideal, Bank Indonesia dapat menentukan area yang perlu ditingkatkan dan mengalokasikan sumber daya secara efektif.

Berikut daftar dokumen pedoman terkait keamanan sistem informasi yang didapatkan oleh Penulis.

Tabel 3.5. Daftar pedoman keamanan siber yang ada di Bank Indonesia

No	Pedoman Kebijakan Terkait Keamanan Sistem Informasi di Bank Indonesia
1	Pedoman Penggunaan Aset Sistem lnformasi Yang Aman
2	Pedoman Penggunaan Password
3	Pedoman Clear Desk Dan Clear Screen
4	Pedoman Penggunaan Email Yang Aman
5	Pedoman Penggunaan Internet Yang Aman
6	Pedoman Pengamanan dan Penanganan lnformasi
7	Pedoman Bekerja Secara Aman Saat Teleworking
8	Pedoman Pengamanan Penggunaan Software Zoom
9	Pedoman Pengelolaan Remote Access VPN
10	Standar Pengelolaan Layanan Internet di Bank Indonesia

Penulis melakukan analisis perbandingan antara kapabilitas yang ada saat ini di Bank Indonesia dengan kapabilitas praktik terbaik yang ideal yang diamati di organisasi lain, Kementerian Keuangan. Analisis ini bertujuan untuk mengidentifikasi kesenjangan atau area di mana ruang lingkup kebijakan di Bank Indonesia masih kurang.

Tabel 3.6: Benchmark pedoman kebijakan keamanan sistem informasi Bank Indonesia dengan organisasi lain

Ruang Lingkup Kebijakan Keamanan Siber	Institusi	
	Bank Indonesia	Organisasi Lain
Penggunaan Aset Sistem lnformasi	V	V
Penggunaan Password	V	V
Clear Desk Dan Clear Screen	V	V
Penggunaan Email	V	V
Penggunaan Internet	V	V
Pengamanan Jaringan Internet	V	V
Pengamanan dan Penanganan lnformasi	V	V
Pengamanan Perangkat End-point	V	V

Continued on next page

Tabel 3.6: Benchmark pedoman kebijakan keamanan sistem informasi Bank Indonesia dengan organisasi lain (Continued)

Pengamanan Akses Remote End-point	V	X
Pengelolaan Remote Access VPN	V	X
Pengamanan Virtual Meeting	V	X
Penggunaan Software Zoom	V	X
Perilaku Kesadaran Keamanan Siber	V	V
Pengamanan Perangkat Mobile	X	X
Pengamanan Dokumen	X	V
Penggunaan Printer	X	X
Etika Penggunaan Media Sosial	X	V

Dengan melakukan benchmarking terhadap *best practice* dari organisasi lain, Penulis mendapatkan wawasan yang berharga tentang area di mana Bank Indonesia dapat meningkatkan kebijakan keamanan sibernya. Proses ini melibatkan studi kebijakan dan praktik yang diterapkan oleh organisasi terkemuka di industri ini dan membandingkannya dengan kebijakan yang ada di Bank Indonesia. Melalui perbandingan ini, Penulis dapat menentukan area kebijakan mana yang memerlukan pengembangan atau peningkatan lebih lanjut agar selaras dengan standar industri dan *best practice*. Hal ini memberikan titik acuan untuk mengidentifikasi dan memprioritaskan ruang lingkup kebijakan yang memerlukan perhatian untuk menjembatani *gap* antara kemampuan saat ini dan kemampuan praktik terbaik yang diinginkan. Dengan memanfaatkan metodologi implementasi ini, Penulis berkontribusi pada peningkatan berkelanjutan kebijakan keamanan siber Bank Indonesia. Penulis secara aktif mencari peluang untuk meningkatkan cakupan kebijakan dan memastikan bahwa Bank Indonesia tetap mengikuti standar dan praktik industri yang terus berkembang. Melalui proses ini, Bank Indonesia dapat memperkuat postur keamanan sibernya dan secara efektif memitigasi ancaman dan kerentanan yang muncul.

Berikut *mapping* klausul dan target kontrol ISO/IEC 27001:2013.

Tabel 3.7: *Mapping* ISO/IEC 27001:2013

Scope		Control Objectives	
1.	Information security policies.	1.	Management direction for information security.
2.	Organization of information security.	2.	Internal organization.
		3.	Mobile devices and teleworking.
3.	Human resource security.	4.	Prior to employment.
		5.	During employment.
		6.	Termination and change of employment.
4.	Asset management.	7.	Responsibility for assets.
		8.	Information classification.
		9.	Media handling.
5.	Access control.	10.	Business requirements of access control.
		11.	User access management.
		12.	User responsibilities.
		13.	System and application access control.
6.	Cryptography.	14.	Cryptographic controls.
7.	Physical and environmental security.	15.	Secure areas.
		16.	Equipment.
8.	Operations security.	17.	Operational procedures and responsibilities.
		18.	Protection from malware.
		19.	Backup.
		20.	Logging and monitoring.
		21.	Control of operational software.

Continued on next page

Tabel 3.7: *Mapping* ISO/IEC 27001:2013 (Continued)

		22.	Technical vulnerability management.
		23.	Information systems audit considerations.
9.	Communications security.	24.	Network security management.
		25.	Information transfer.
10.	System acquisition, development and maintenance	26.	Security requirements of information systems.
		27.	Security in development and support processes.
		28.	Test data.
11.	Supplier relationships.	29.	Information security in supplier relationships.
		30.	Supplier service delivery management.
12.	Information security incident management.	31.	Management of information security incidents and improvements.
13.	Information security aspects of business continuity management.	32.	Information security continuity.
		33.	Redundancies.
14.	Compliance	34.	Compliance with legal and contractual requirements.
		35.	Information security reviews.

Penulis menjelaskan secara rinci tentang bagaimana kontrol atau *best practice* tertentu dapat diterapkan untuk mengatasi masalah atau persyaratan keamanan tertentu. Dalam konteks kontrol keamanan operasional, sebagai contoh pertimbangkan pencadangan data (*backup*). Pencadangan tercakup dalam klausul kontrol A.12.3.1 dalam ISO/IEC 27001:2013, yang menyatakan: ”Organisasi harus memastikan bahwa informasi yang diperlukan untuk pengoperasian sistem manajemen keamanan informasi dan ketersediaan fasilitas pemrosesan informasi

dilindungi dari kehilangan, kerusakan, dan pencurian." Tujuan tersebut dapat berupa menetapkan dan memelihara kebijakan pencadangan yang memastikan pencadangan data penting secara tepat waktu dan aman. Bank Indonesia dapat menilai pedoman kebijakannya saat ini di bidang ini dengan mengevaluasi prosedur pencadangan yang ada. Faktor-faktor seperti berikut ini dapat dipertimbangkan dalam penilaian ini:

1. Frekuensi pencadangan: Seberapa sering pencadangan dilakukan? Untuk meminimalkan risiko kehilangan data, apakah data dan sistem yang penting perlu dicadangkan secara teratur?

2. Penyimpanan data: Berapa lama file yang dicadangkan disimpan? Apakah ada kebijakan retensi yang ditetapkan yang selaras dengan tujuan pemulihan (*recovery*) dan persyaratan kepatuhan organisasi?

3. Integritas cadangan: Apakah prosedur pencadangan dirancang untuk memastikan integritas data? Apakah ada mekanisme yang diterapkan untuk verifikasi keakuratan dan kelengkapan cadangan?

4. Penyimpanan dan perlindungan: Di mana lokasi penyimpanan untuk cadangan? Untuk mengurangi risiko kerusakan fisik atau pencurian, apakah cadangan disimpan di lokasi yang aman dan di luar kantor? Untuk membatasi akses yang tidak sah ke data cadangan, apakah ada kontrol akses yang sesuai?

Dengan *mapping* klausul kontrol dan tujuan ISO/IEC 27001:2013, Bank Indonesia dapat menilai tingkat kapabilitas saat ini dan membandingkannya dengan tingkat kapabilitas yang ideal seperti yang diuraikan dalam *best practice* di industri. Perbandingan ini membantu mengidentifikasi area yang perlu ditingkatkan. Hal ini juga memungkinkan untuk alokasi dan penentuan prioritas sumber daya. Menerapkan pedoman keamanan siber yang direkomendasikan berdasarkan ISO/IEC 27000 series dan NIST Cybersecurity Framework, serta melakukan penilaian secara berkala terhadap standar-standar tersebut, akan membantu memperkuat postur keamanan informasi Bank Indonesia dan melindungi data-data sensitif.

3.3.5 Evaluasi

Bagian evaluasi melibatkan pelaksanaan analisis *gap* yang komprehensif dan mengembangkan rekomendasi berdasarkan temuan. Proses ini akan membantu

mengidentifikasi area-area di mana praktik keamanan siber Bank Indonesia saat ini menyimpang dari praktik dan standar terbaik industri, sebagaimana diuraikan dalam seri ISO/IEC 27000 dan *Framework* NIST Cybersecurity. Melalui analisis ini, proyek magang ini bertujuan untuk memberikan wawasan yang dapat ditindaklanjuti untuk membantu Bank Indonesia meningkatkan postur keamanan informasinya dan mengatasi *gap* yang teridentifikasi.

Hal pertama yang dilakukan Penulis lakukan adalah fokus untuk mengidentifikasi penambahan yang perlu dilakukan pada kebijakan keamanan informasi yang ada. Melalui perbandingan tujuan kontrol ISO 27001 dengan kebijakan yang ada saat ini, Penulis dapat mengidentifikasi area-area tertentu yang belum tercakup secara memadai. *Gap* ini terutama terjadi di bidang ancaman dan teknologi yang muncul yang belum ditangani dalam kebijakan yang ada. Untuk memastikan bahwa kebijakan-kebijakan tersebut mutakhir dan sesuai dengan *best practice* industri, Penulis menyarankan beberapa tambahan. Penambahan ini mencakup panduan khusus untuk penggunaan perangkat seluler (*mobile device*) dan media sosial.

Penulis mengevaluasi pedoman kebijakan yang ada untuk menentukan apakah ada pengurangan yang diperlukan, selain mengidentifikasi area yang perlu ditambahkan. Penting untuk memastikan bahwa kebijakan-kebijakan tersebut ringkas dan terfokus. Tidak ada duplikasi atau redundansi yang tidak perlu. Melalui analisis yang teliti, Penulis mengidentifikasi bagian-bagian tertentu yang sudah *outdated* atau berlebihan dengan kebijakan lainnya. Dengan menghapus bagian-bagian ini, tujuan Penulis adalah merampingkan kebijakan dan membuatnya lebih *user-friendly* dan lebih mudah diakses oleh pegawai.

Terakhir, Penulis melakukan evaluasi untuk menentukan apakah pembaruan terhadap pedoman kebijakan keamanan informasi yang ada diperlukan. Teknologi dan ancaman keamanan terus berkembang, dan kebijakan harus diperbarui secara berkala untuk mengimbangi perubahan ini. Penulis meninjau kebijakan-kebijakan tersebut terhadap tujuan kontrol ISO 27001. Penulis membandingkannya dengan standar industri dan *best practice* terbaru.

Penulis menambahkan ruang lingkup pedoman tentang penggunaan perangkat seluler, pengamanan dokumen, penggunaan printer, dan etika penggunaan media sosial dalam kebijakan keamanan siber. Menyadari pentingnya area-area ini dalam memastikan keamanan yang komprehensif, Penulis memasukkan pedoman khusus untuk mengatasinya. Untuk perangkat seluler, pedoman ini bisa mencakup instruksi tentang enkripsi perangkat, koneksi jaringan

yang aman, dan pembaruan perangkat lunak secara rutin. Pedoman pengamanan dokumen dapat menguraikan prosedur untuk mengklasifikasikan dan menangani informasi sensitif, menerapkan kontrol akses, dan membuang dokumen dengan aman. Pedoman penggunaan printer dapat mencakup praktik pencetakan yang aman, pembuangan materi cetak yang tepat, dan pemeliharaan rutin pengaturan keamanan printer. Pedoman etika penggunaan media sosial dapat memberikan panduan kepada pegawai mengenai penggunaan yang bertanggung jawab dan aman, termasuk perlindungan terhadap informasi rahasia dan mematuhi kode etik Bank Indonesia. Dengan adanya pedoman ini, Penulis memastikan bahwa kebijakan keamanan siber Bank Indonesia telah mencakup berbagai aspek keamanan informasi, termasuk area-area spesifik yang relevan bagi organisasi. Hal ini membantu dalam mempromosikan budaya kesadaran keamanan di kalangan pegawai dan memperkuat postur keamanan Bank Indonesia secara keseluruhan.

3.3.6 Finalisasi

Hasil evaluasi yang dilakukan selama proyek magang akan dibagikan kepada Bank Indonesia setelah selesai. Berdasarkan evaluasi tersebut, proses dan kebijakan keamanan siber Bank Indonesia saat ini masih memiliki *gap* dan perlu dikembangkan. Evaluasi ini juga memberikan rekomendasi berdasarkan *best practice* industri dan standar global, termasuk seri ISO/IEC 27000 dan *Framework* NIST Cybersecurity. Temuan-temuan evaluasi akan disajikan dengan cara yang jelas dan ringkas, dengan menyoroti area-area utama yang memerlukan perhatian dan peningkatan. akan ditujukan untuk memberikan solusi dalam pembuatan pedoman keamanan siber bagi pegawai Bank Indonesia. Pedoman ini akan menguraikan langkah-langkah dan tindakan yang diperlukan untuk meningkatkan postur keamanan informasi organisasi dan menyelaraskannya dengan standar industri dan *best practice*.

Secara keseluruhan, tahap finalisasi proyek magang ini akan memberikan Bank Indonesia evaluasi yang komprehensif atas praktik dan kebijakan keamanan sibernya saat ini, bersama dengan rekomendasi yang dapat ditindaklanjuti. Dengan menerapkan solusi yang disarankan dan menyelaraskan praktik-praktiknya dengan standar internasional, Bank Indonesia dapat memperkuat postur keamanan informasinya, melindungi data sensitif, dan memitigasi risiko yang terkait dengan ancaman keamanan siber.

3.4 Kendala dan Solusi yang Ditemukan

Selama pelaksanaan magang di Bank Indonesia terdapat beberapa kendala yang dihadapi Penulis. Berikut kendala yang dihadapi Penulis dalam pelaksanaan magang, diantaranya adalah:

1. Keterbatasan akses ke data dan informasi pedoman yang relevan tentang praktik keamanan siber yang ada di Bank Indonesia.
2. Kesulitan dalam menyusun pedoman kebijakan keamanan siber yang sesuai dengan standar internasional dan dengan kondisi spesifik di Bank Indonesia.
3. Tantangan dalam menyampaikan pedoman kebijakan keamanan siber secara efektif dan menarik.

Solusi yang dilakukan untuk mengatasi kendala yang ditemukan selama proses magang berlangsung, antara lain:

1. Menghubungi pihak-pihak terkait di Bank Indonesia untuk meminta bantuan dalam mendapatkan data dan informasi yang dibutuhkan.
2. Melakukan studi banding dengan pedoman kebijakan keamanan siber yang diterapkan di organisasi lain, serta mengkonsultasikan draft pedoman ke pihak-pihak ahli di bidang keamanan siber.
3. Membuat materi presentasi yang menampilkan poin-poin penting dari pedoman kebijakan keamanan siber.