Jurnal Sosial dan Teknologi (SOSTECH)
Volume 6, Number 8, Agustus 2026
p-ISSN 2774-5147 ; e-ISSN 2774-5155

Evaluasi Kematangan Penanganan Insiden *Insider Threat* Nirteknis Berdasarkan NIST SP 800-61: Studi Kasus Pekerja Non-AD di Industri Manufaktur Energi

Muhammad Syahdan Junus*, Muhammad Najamuddin Dwi Miharja, Hendra Arya Syaputra
Universitas Pelita Bangsa, Indonesia
Email: syahdanjns26@gmail.com*, Najamuddin.dwi@pelitabangsa.ac.id, hendraarya23@gmail.com

Keywords:
Non-Technical Insider Threat; NIST SP 800-61; Security Policy Enforcement; Incident Handling Maturity; Non-AD Workforce.

Abstract
Insider threats have been studied almost exclusively for knowledge workers with access to digital systems, resulting in mitigation strategies dominated by technical identity- and access-based controls. A conceptual gap arises in organizations with a non-digital workforce, where conventional controls become ineffective. This study evaluates the handling of a non-technical insider threat incident at PT X, an energy manufacturing company, involving a former non-Active Directory (non-AD) employee who recorded and published production data. Using a qualitative, descriptive case study approach, the incident handling was mapped to the four phases of the NIST SP 800-61 framework, assessed for maturity on a scale of 1–5, and measured for effectiveness across four parameters. The study results show that all phases received identical scores at level 2 (Initial/Ad Hoc), indicating that the handling activities took place without documented procedures and relied on individual initiative. Rapid response (0 days) and successful enforcement (H+1) were not matched by procedural compliance and institutionalization of post-incident learning. This study concludes that in the non-AD population, incident management maturity is not determined by the sophistication of technical controls, but rather by the strength of administrative and physical control enforcement. These findings provide implications for organizations with a non-digital workforce to shift the focus of security strengthening from the technical dimension to the procedural and structural dimensions.

Kata Kunci:
Insider Threat Nirteknis; NIST SP 800-61; Penegakan Kebijakan Keamanan; Kematangan Penanganan Insiden; Pekerja Non-AD.

Abstrak
Ancaman dari dalam (*insider threat*) selama ini dikaji hampir secara eksklusif pada pekerja pengetahuan yang memiliki akses terhadap sistem digital, sehingga strategi mitigasi didominasi oleh kontrol teknis berbasis identitas dan akses. Celah konseptual muncul pada organisasi dengan populasi pekerja non-digital, di mana kontrol konvensional menjadi tidak berlaku. Penelitian ini mengevaluasi penanganan insiden *insider threat* nirteknis di PT X, perusahaan manufaktur energi, yang melibatkan mantan pekerja *non-Active Directory* (non-AD) yang merekam dan memublikasikan area produksi. Dengan pendekatan kualitatif studi kasus deskriptif, penanganan insiden dipetakan ke dalam empat fase kerangka NIST SP 800-61, dinilai kematangannya pada skala 1–5, dan diukur efektivitasnya melalui empat parameter. Hasil penelitian

menunjukkan seluruh fase memperoleh skor identik pada tingkat 2 (*Initial/Ad Hoc*), yang berarti aktivitas penanganan berlangsung tanpa prosedur terdokumentasi dan bergantung pada inisiatif individual. Respons cepat (0 hari) dan keberhasilan penindakan (H+1) tidak diimbangi dengan kepatuhan prosedur dan pelembagaan pembelajaran pasca-insiden. Penelitian ini menyimpulkan bahwa pada populasi non-AD, kematangan penanganan insiden tidak ditentukan oleh kecanggihan kontrol teknis, melainkan oleh kekuatan penegakan kontrol administratif dan fisik. Temuan ini memberikan implikasi bagi organisasi dengan tenaga kerja non-digital untuk mengalihkan fokus penguatan keamanan dari dimensi teknis ke dimensi prosedural dan struktural.

PENDAHULUAN

Ancaman keamanan informasi yang dihadapi perusahaan multinasional tidak hanya berasal dari luar, tetapi juga dari pihak internal yang dikenal sebagai *insider threat*. Ancaman jenis ini tergolong paling berbahaya karena pelaku memiliki akses dan pengetahuan terhadap sistem maupun data sensitif organisasi (Cappelli et al., 2012). Berbeda dengan penyerang eksternal yang harus menembus lapisan pertahanan perimeter terlebih dahulu, pelaku internal beroperasi menggunakan hak akses yang sah, sehingga aktivitasnya sulit dibedakan dari aktivitas kerja normal dan kerap baru terdeteksi setelah dampaknya terwujud. Berbagai kajian mitigasi *insider threat* telah berkembang pesat (Inayat et al., 2024), dan sebagian besar menempatkan faktor manusia sebagai inti persoalan, bukan semata kegagalan kontrol teknis (Pathirana et al., 2026; Zangana et al., 2025). Kajian tersebut juga menunjukkan bahwa ancaman internal tidak selalu bersifat sengaja, melainkan mencakup kelalaian dan pelanggaran prosedur yang dilakukan tanpa niat merugikan organisasi. Di Indonesia, kerangka NIST dan standar keamanan informasi telah diterapkan pada beragam konteks organisasi, mulai dari penilaian risiko siber (Handoyo & Nigrum, 2023; Ramadhanty, 2024) hingga analisis serangan *insider threat* (Rahman et al., 2026), meskipun umumnya masih berfokus pada organisasi berorientasi teknologi informasi dengan pengguna sistem digital.

Namun, hampir seluruh literatur tersebut berangkat dari asumsi implisit bahwa pelaku adalah pekerja pengetahuan (knowledge worker) yang berinteraksi dengan sistem digital. Akibatnya, strategi mitigasi terkonsentrasi pada kontrol berbasis identitas dan akses, seperti manajemen akun Active Directory, pencabutan hak akses, analisis log, dan Data Leakage Protection (Herrera Montano et al., 2022).

Asumsi ini meninggalkan celah konseptual pada organisasi yang sebagian besar tenaga kerjanya adalah pekerja produksi tanpa jejak digital korporat, atau non-Active Directory. Pada populasi ini, seluruh arsenal kontrol teknis konvensional pada dasarnya tidak berlaku, sehingga kerangka evaluasi yang berpusat pada dimensi digital menjadi kurang relevan.

Kekosongan tersebut menjadi nyata pada sebuah insiden di PT X, sebuah perusahaan manufaktur energi multinasional. Seorang mantan pekerja berstatus perjanjian kerja waktu tertentu (PKWT) merekam area produksi menggunakan perangkat pribadi selama masa kerja aktif, lalu memublikasikan rekaman tersebut ke media sosial sekitar lima pekan setelah kontraknya berakhir. Insiden ini memperlihatkan adanya celah serius pada kontrol preventif, bukan karena ketiadaan kebijakan, melainkan karena lemahnya penegakan (enforcement) atas larangan penggunaan telepon seluler yang sudah berlaku formal di area produksi. Larangan

tersebut tidak dilengkapi prosedur pendukung seperti pemeriksaan fisik, penitipan perangkat, atau sanksi tegas.

Untuk mengevaluasi penanganan insiden secara sistematis, penelitian ini menggunakan kerangka kerja NIST SP 800-61 Rev. 2 (Cichonski et al., 2012) yang membagi penanganan insiden ke dalam empat fase operasional, yaitu Preparation, Detection & Analysis, Containment, Eradication & Recovery, dan Post-Incident Activity. Kerangka ini dipilih karena bersifat teknis operasional dan tersegmentasi jelas, sehingga dibandingkan kerangka tata kelola yang lebih umum (ISACA, 2018) maupun standar manajemen insiden yang lebih berorientasi pada proses organisasional (*Information Technology, Information Security Incident Management, Part 1: Principles and Process, ISO/IEC 27035-1:2023,* 2023).

Urgensi penelitian ini terletak pada semakin banyaknya organisasi industri manufaktur dan energi yang memiliki tenaga kerja non-digital dalam jumlah besar, namun kerangka evaluasi keamanan informasi yang tersedia masih didominasi oleh perspektif organisasi berbasis teknologi. Tanpa kerangka evaluasi yang sesuai, organisasi dengan populasi non-AD rentan terhadap insiden *insider threat* yang tidak terdeteksi oleh kontrol teknis konvensional. Kebaruan penelitian ini terletak pada pengembangan pendekatan evaluasi kematangan penanganan insiden yang secara spesifik dirancang untuk konteks non-teknis, dengan mengadaptasi kerangka NIST SP 800-61 pada populasi pekerja tanpa akun Active Directory. Berbeda dengan penelitian sebelumnya yang berfokus pada kontrol teknis, penelitian ini menyoroti pentingnya penegakan kontrol administratif dan fisik sebagai determinan utama kematangan penanganan insiden pada populasi non-AD. Tujuan penelitian ini adalah mengevaluasi kematangan penanganan insiden *insider threat* nirteknis di PT X berdasarkan kerangka NIST SP 800-61, serta mengidentifikasi faktor-faktor yang memengaruhi efektivitas penanganan insiden pada populasi pekerja non-AD.

Kontribusi penelitian ini bersifat teoretis dan praktis. Secara teoretis, penelitian ini memperluas cakupan kajian *insider threat* dengan menyoroti konteks populasi non-AD yang selama ini terabaikan dalam literatur. Penelitian ini juga mengadaptasi model kematangan penanganan insiden pada konteks nirteknis, yang berbeda secara fundamental dari konteks teknis yang mendominasi literatur. Secara praktis, penelitian ini memberikan rekomendasi bagi organisasi dengan populasi pekerja non-AD dalam memperkuat penegakan kebijakan keamanan dan melembagakan prosedur penanganan insiden. Manfaat penelitian ini diharapkan dapat menjadi acuan bagi praktisi keamanan informasi, manajemen organisasi, dan pembuat kebijakan dalam merancang strategi mitigasi *insider threat* yang lebih komprehensif dan sesuai dengan karakteristik tenaga kerja non-digital.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus deskriptif (Farquhar et al., 2020), yang sesuai untuk fenomena kompleks yang melibatkan interaksi kebijakan administratif, perilaku manusia, dan infrastruktur teknis. Objek penelitian adalah proses penanganan insiden *insider threat* pada PT X, dengan fokus pada insiden pengunggahan rekaman area produksi yang terjadi pada Februari 2025. Data primer dikumpulkan melalui wawancara mendalam terhadap tiga informan lintas fungsi, yaitu Manajer IT (INF-01), Administrator Sistem (INF-02), dan Staf HR (INF-03), observasi partisipan pada area produksi, serta audit dokumentasi prosedur operasional standar (SOP). Data sekunder mencakup audit

log Active Directory yang mengonfirmasi bahwa pelaku tidak memiliki akun sistem. Validitas temuan dijaga melalui triangulasi sumber dan teknik (Delso-Vicente et al., 2025; Madiyaningsih & Ramli, 2023), serta empat kriteria keabsahan data kualitatif berupa kredibilitas, transferabilitas, dependabilitas, dan konfirmabilitas (Force, 2020).

Potensi bias dari peran ganda peneliti sebagai praktisi Information Security Management (ISM) dimitigasi melalui member check dan penyandaran kesimpulan pada bukti non-informan. Analisis dilakukan dengan memetakan penanganan insiden ke dalam empat fase NIST SP 800-61, kemudian menilai kematangan tiap fase menggunakan skala 1 sampai 5 yang diadaptasi dari model kematangan tata kelola (*Security, Cybersecurity and Privacy Protection, Information Security Management Systems, Requirements, ISO/IEC 27001:2022*, 2022), mulai dari Non-Existent (1) hingga Optimized (5).

Penetapan skor mengikuti kaidah berikut. Tingkat 1 diberikan bila tidak ditemukan kebijakan maupun praktik penanganan. Tingkat 2 bila praktik berlangsung tetapi tanpa prosedur terdokumentasi sehingga bergantung pada inisiatif pelaksana. Tingkat 3 (Defined) bila prosedur terdokumentasi dan dijalankan secara konsisten. Tingkat 4 bila pelaksanaan diukur melalui indikator kinerja, dan tingkat 5 bila hasil pengukuran digunakan untuk perbaikan berkelanjutan. Suatu fase hanya menerima skor tertentu apabila seluruh kriteria pada tingkat tersebut terpenuhi.

Efektivitas penanganan diukur melalui empat parameter yang dirancang selaras dengan terminologi NIST SP 800-61, yaitu Response Time (RT), Containment Success Rate (CSR), Compliance Level (CL), dan Lessons Learned Implementation (LLI). Keempat parameter dioperasionalkan sebagai berikut. RT adalah selisih hari antara insiden terdeteksi dan tindakan penanganan pertama. CSR adalah status tercapainya penghentian penyebaran dampak, dalam kasus ini keberhasilan takedown konten.

CL adalah tingkat kesesuaian langkah penanganan dengan prosedur operasional standar yang terdokumentasi. LLI adalah tingkat konversi rekomendasi pascainsiden menjadi program yang terjadwal dan terukur. Titik nol RT ditetapkan pada deteksi, bukan pada terjadinya perbuatan, sehingga parameter ini tidak menangkap jeda antara kegagalan kontrol dan terungkapnya insiden. Analisis kesenjangan (gap analysis) digunakan untuk membandingkan kondisi aktual dengan kondisi ideal, dan hasilnya divisualisasikan dalam bentuk radar chart serta gap chart.

Penelitian dilaksanakan atas izin penuh manajemen PT X. Seluruh informan memberikan persetujuan sebelum wawancara, dan identitas organisasi maupun individu disamarkan dalam pelaporan. Penulis pertama merupakan praktisi pada departemen Information Security Management di organisasi yang menjadi objek penelitian. Peran ganda tersebut dinyatakan secara terbuka dan dimitigasi melalui prosedur yang telah diuraikan.

HASIL DAN PEMBAHASAN

Kronologi dan Alur Penanganan Insiden

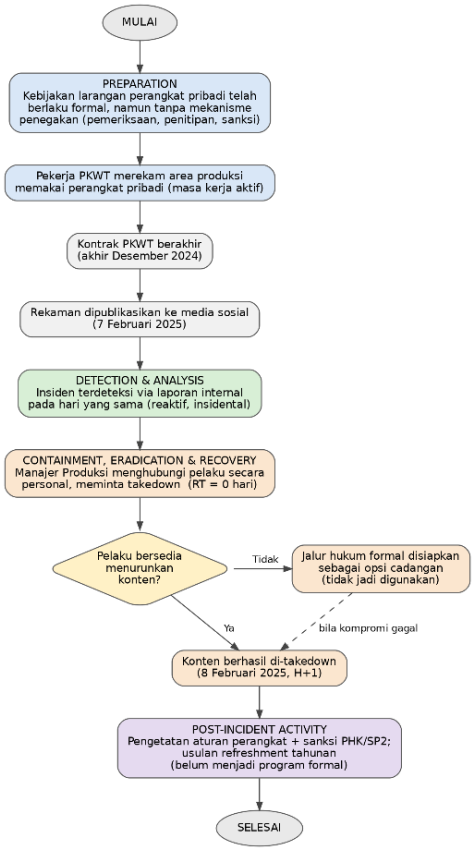
Insiden bermula dari perekaman area produksi menggunakan perangkat pribadi pada masa kerja aktif, sementara kebijakan larangan telepon seluler telah berlaku formal namun tanpa mekanisme penegakan. Perekaman terjadi saat pelaku masih berstatus karyawan, sedangkan publikasi baru dilakukan sekitar lima pekan setelah kontrak berakhir, ketika

organisasi tidak lagi memiliki sarana pengendalian terhadapnya, baik administratif maupun teknis. Kronologi ringkas insiden disajikan pada Tabel 1.

Tabel 1. Kronologi Insiden

Tanggal	Peristiwa
Masa kerja aktif (sebelum akhir Desember 2024)	Pelaku merekam area produksi menggunakan perangkat pribadi. Larangan telepon seluler berlaku formal tanpa mekanisme pemeriksaan atau penitipan perangkat
Akhir Desember 2024	Kontrak PKWT mantan karyawan berakhir
7 Februari 2025	Rekaman dipublikasikan ke media sosial dan terdeteksi Tim ISM pada hari yang sama melalui laporan internal (RT = 0 hari)
7 Februari 2025	Manajer Produksi menghubungi pelaku secara personal untuk meminta *takedown* konten
8 Februari 2025	Konten berhasil di-*takedown* (H+1) melalui pendekatan personal, bukan SOP terdokumentasi

Kronologi tersebut selanjutnya dipetakan ke dalam empat fase NIST SP 800-61, mulai dari celah preventif hingga tindak lanjut pascainsiden, sebagaimana disajikan pada Gambar 1.



Gambar 1. Diagram alir penanganan insiden PT X berdasarkan fase NIST SP 800-61

Alur pada Gambar 1 memperlihatkan bahwa keempat fase memang terlewati, tetapi belum menjelaskan seberapa matang pelaksanaan masing-masing, sehingga diperlukan pembandingan terhadap kondisi ideal.

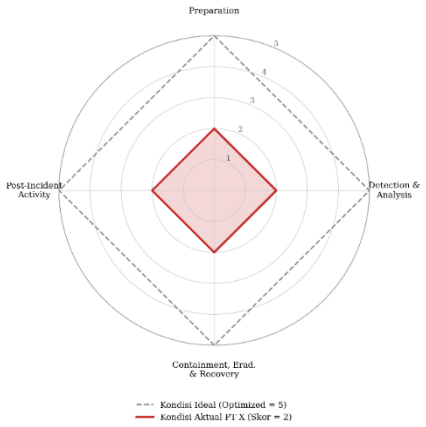
Analisis Kesenjangan dan Skor Kematangan

Hasil pemetaan kondisi aktual terhadap kondisi ideal menunjukkan bahwa keempat fase memperoleh skor kematangan identik pada tingkat 2 (*Initial/Ad Hoc*), sebagaimana dirangkum pada Tabel 2. Tingkat 2 menandakan bahwa aktivitas penanganan sudah berlangsung tetapi belum terstandardisasi, sehingga pelaksanaannya bergantung pada inisiatif pelaksana dan tidak dapat diulang secara konsisten.

Tabel 2. *Gap Analysis* dan *Maturity Scoring* per Fase

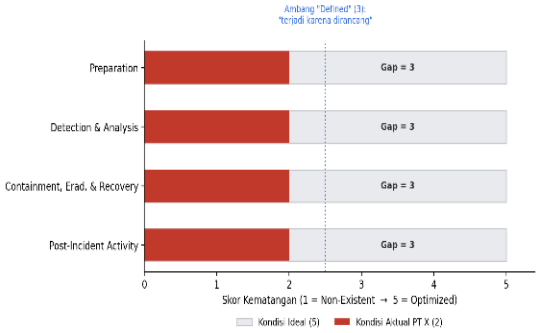
Fase NIST SP 800-61	Kondisi Aktual PT X	Skor
Preparation	Kebijakan larangan perangkat pribadi berlaku formal, tetapi penegakannya bergantung pada pengawasan individual tanpa prosedur operasional.	2
Detection & Analysis	Insiden terdeteksi reaktif melalui laporan internal, bukan mekanisme deteksi yang dirancang	2
Containment, Eradication & Recovery	*Containment* berhasil pada H+1 melalui pendekatan personal-informal, bukan SOP terdokumentasi	2
Post-Incident Activity	Tindak lanjut bersifat reaktif, usulan program berkala masih berstatus rekomendasi	2

Skor identik pada keempat fase menghasilkan pola simetris pada Gambar 2.



Gambar 2. *Radar chart* skor kematangan per fase NIST SP 800-61

Kesamaan skor tersebut membuat *radar chart* kurang informatif dalam menonjolkan besaran kesenjangan, sehingga disajikan pula visualisasi komplementer berupa *gap chart* (Gambar 3) yang memperlihatkan selisih terhadap kondisi ideal (*Optimized* = 5).



Gambar 3. *Gap chart* Kesenjangan Kematangan terhadap Kondisi Ideal per Fase

Pembacaan silang terhadap empat parameter evaluasi memperkuat temuan sentral. RT yang unggul (nol hari) dan CSR yang tercapai pada H+1 berdampingan dengan CL yang rendah dan LLI yang belum dilembagakan. Konfigurasi ini, cepat namun rendah kepatuhan dan minim pembelajaran, merupakan tanda operasional organisasi yang menangani insiden secara reaktif-heroik alih-alih preventif-sistemik. Skor identik pada keempat fase menegaskan bahwa kelemahan PT X bukan defisit pada satu titik yang dapat diperbaiki secara tambal sulam, melainkan defisit struktural yang berulang pada setiap simpul siklus penanganan.

Faktor Manusia dan Lokalisasi Titik Kegagalan

Temuan empiris PT X beririsan langsung dengan tesis bahwa risiko *insider threat* pada dasarnya merupakan persoalan faktor manusia dan bukan semata kegagalan kontrol teknis [3], [4]. Kasus PT X bersifat nirteknis dalam arti seluruh rantai peristiwa, mulai dari perekaman hingga publikasi, berlangsung tanpa menyentuh satu pun sistem korporat.

Karakteristik nirteknis ini mengisolasi variabel faktor manusia dari kebisingan kontrol teknis, sehingga hubungan antara kelemahan penegakan dan materialisasi risiko dapat diamati dalam bentuknya yang paling murni. Titik kegagalan kontrol yang paling menentukan terjadi di hulu, yaitu ketika perangkat pribadi dibawa masuk dan digunakan untuk merekam area terlarang tanpa terdeteksi, bukan pada saat publikasi di hilir.

Dengan demikian, akar dari persoalan PT X bukanlah keterlambatan pencabutan akses digital, yang memang tidak relevan karena ketiadaan akun sistem, melainkan lemahnya penegakan kebijakan pengendalian perangkat pribadi yang sudah berlaku. CL yang rendah merupakan gejala terukur dari kebijakan yang tidak memiliki mekanisme penegakan, sejalan dengan temuan bahwa kepatuhan terhadap kebijakan keamanan informasi sangat ditentukan oleh faktor penegakan dan perilaku pada tataran organisasi (Technology, 2024).

Pemetaan lapisan kontrol menegaskan implikasi ini. Ketika lapisan kontrol keamanan dipetakan ke dalam kategori administratif, fisik, dan teknis yang bersesuaian dengan keluarga kontrol pada NIST SP 800-53 (Technology, 2025) dan tema kontrol ISO/IEC 27001:2022 [19], tampak bahwa tindakan korektif PT X baru menyentuh dimensi deteren dan belum menyentuh keterlaksanaan penegakan (*enforceability*).

Konsekuensi terberatnya adalah ketergantungan pada personel kunci yang tidak dilembagakan. Selama keberhasilan bersandar pada inisiatif individual, organisasi pada hakikatnya mengelola risiko dengan keberuntungan, dan keberuntungan bukanlah kontrol.

Kerangka Validitas Temuan

Sebagai studi kasus tunggal, penelitian ini tidak mengklaim generalisasi statistik, melainkan menyandarkan diri pada generalisasi analitis, yaitu kemampuan menghubungkan temuan spesifik dengan proposisi teoretis yang lebih luas. Dalam kerangka ini, kasus PT X berfungsi sebagai kasus ekstrem sekaligus revelatoris yang bernilai tinggi justru karena karakteristik nirteknisnya.

Temuan yang dapat dipertahankan bukanlah persentase keberhasilan penanganan, melainkan proposisi analitis bahwa pada organisasi dengan populasi pekerja non-digital, kematangan penanganan insiden ditentukan oleh kekuatan kontrol administratif-fisik dan pelembagaan prosedur, bukan oleh kecepatan respons individual maupun kecanggihan kontrol teknis.

Transferabilitas dinilai oleh pembaca yang membandingkan konteksnya dengan konteks penelitian, sehingga temuan ini paling relevan bagi organisasi berpopulasi non-AD dan bergeser pada organisasi berpengguna sistem digital. Penggunaan satu insiden sebagai unit analisis menjadikan triangulasi (Denzin, 1978; Guba, 1985; Yin, 2018) menjaga kredibilitas, bukan memperluas cakupan empiris. Penskoran dilakukan oleh peneliti tunggal tanpa penilai pembanding, sehingga uji kesepakatan antarpenilai tidak dapat dilakukan. Keterbatasan ini dimitigasi dengan menyandarkan penilaian pada kondisi aktual yang dapat diverifikasi, yaitu ada atau tidaknya dokumen prosedur beserta bukti pelaksanaannya, bukan pada penilaian subjektif atas kualitas penanganan.

KESIMPULAN

Penelitian ini menyimpulkan bahwa penanganan insiden *insider threat* nirteknis di PT X berada pada tingkat kematangan 2 (Initial/Ad Hoc) secara konsisten pada keempat fase NIST SP 800-61. Respons yang cepat tidak diimbangi oleh kepatuhan dan pelembagaan pembelajaran, sehingga keberhasilan penanganan bertumpu pada individu alih-alih prosedur. Akar persoalan bukan ketiadaan kebijakan, melainkan lemahnya penegakan kebijakan yang sudah ada, dan pada populasi pekerja non-AD kematangan penanganan insiden ditentukan oleh penegakan kontrol administratif-fisik, bukan oleh kecanggihan kontrol teknis. Temuan ini menunjukkan bahwa organisasi dengan populasi non-AD memerlukan pendekatan yang berbeda dalam menangani *insider threat,* di mana penegakan kebijakan administratif dan fisik menjadi lebih determinan dibandingkan kontrol teknis.

Untuk penelitian selanjutnya, disarankan untuk melakukan studi komparatif antarorganisasi dengan populasi non-AD yang berbeda untuk menguji transferabilitas temuan ini. Penelitian juga perlu dikembangkan dengan melibatkan multiple raters dalam penskoran kematangan untuk meningkatkan reliabilitas dan mengurangi bias penilaian. Studi longitudinal yang mengikuti implementasi perbaikan prosedur penanganan insiden juga direkomendasikan untuk mengamati peningkatan kematangan dari waktu ke waktu. Selain itu, penelitian kuantitatif dengan sampel yang lebih besar dapat dilakukan untuk mengukur hubungan antara tingkat penegakan kebijakan dan efektivitas penanganan insiden pada populasi non-AD. Pengembangan instrumen evaluasi kematangan yang spesifik untuk konteks nirteknis juga menjadi agenda penelitian yang penting untuk menjembatani kesenjangan antara kebutuhan praktis organisasi dan ketersediaan kerangka evaluasi yang sesuai.

REFERENSI

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes*. Addison-Wesley.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Delso-Vicente, A. T., Diaz-Marcos, L., Aguado-Tevar, O., & de Blanes-Sebastián, M. G. (2025). Factors influencing employee compliance with information security policies: A systematic literature review of behavioral and technological aspects in cybersecurity. *Future Business Journal*, *11*(1 AR-28). https://doi.org/10.1186/s43093-025-00452-7

Denzin, N. K. (1978). *The research act: A theoretical introduction to sociological methods* (2nd ed.). McGraw-Hill.

Farquhar, J., Michels, N., & Robson, J. (2020). Triangulation in industrial qualitative case study research: Widening the scope. *Industrial Marketing Management*, *87*, 160–170. https://doi.org/10.1016/j.indmarman.2020.02.001

Force, J. T. (2020). *Security and privacy controls for information systems and organizations*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Guba, Y. S. L. dan E. G. (1985). Naturalistic Inquiry. *Beverly Hills, CA: Sage Publications*.

Handoyo, E., & Nigrum, I. E. (2023). Penilaian risiko keamanan siber kampus menggunakan framework cybersecurity NIST 1.1. *Jurnal CoSciTech (Computer Science and Information Technology)*, *4*(3), 677–685. https://doi.org/10.37859/coscitech.v4i3.5628

Herrera Montano, I., Garcia Aranda, J. J., Ramos Diaz, J., Molina Cardin, S., de la Torre Diez, I., & Rodrigues, J. J. P. C. (2022). Survey of techniques on data leakage protection and methods to address the insider threat. *Cluster Computing*, *25*(6), 4289–4302. https://doi.org/10.1007/s10586-022-03668-2

Inayat, U., Farzan, M., Mahmood, S., Zia, M. F., Hussain, S., & Pallonetto, F. (2024). Insider threat mitigation: Systematic literature review. *Ain Shams Engineering Journal*, *15*(9 AR-103068). https://doi.org/10.1016/j.asej.2024.103068

Information Technology, Information Security Incident Management, Part 1: Principles and Process, ISO/IEC 27035-1:2023. (2023). International Organization for Standardization.

ISACA. (2018). *COBIT 2019 Framework: Introduction and Methodology*. ISACA.

Madiyaningsih, I., & Ramli, K. (2023). IT maturity level analysis using framework COBIT 5 work for management cyber incident: Case study of company Z in ICT field. *Gema Wiralodra*, *14*(2), 952–960. https://doi.org/10.31943/gw.v14i2.476

Pathirana, N., Roberts, R., Kalutarage, H., & McDermott, C. D. (2026). Integrating human factors into insider threat detection: A systematic review. *ACM Computing Surveys*, *58*(10 AR-260).

Rahman, R., Lestari, D., & Lestari, C. I. (2026). Analisis keamanan sistem informasi terhadap serangan insider threat. *INOMATEC: Jurnal Inovasi Dan Kajian Multidisipliner Kontemporer*, *1*(3).

Ramadhanty, N. (2024). Implementasi kerangka keamanan NIST dan ISO/IEC 27001 dalam menghadapi ancaman risiko siber. *Journal of Indonesian Management*, *4*(4). https://doi.org/10.53697/jim.v4i4.1973

Security, Cybersecurity and Privacy Protection, Information Security Management Systems, Requirements, ISO/IEC 27001:2022. (2022). International Organization for Standardization.

Technology, N. I. of S. and. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Technology, N. I. of S. and. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). Sage Publications.

Zangana, H. M., Sallow, Z. B., & Omar, M. (2025). The human factor in cybersecurity: Addressing the risks of insider threats. *Jurnal Ilmiah Computer Science, 3*(2), 76–85.