E-ISSN : 3025-1311
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 10 No 7 Tahun 2025

PERAN AUDIT DAN HUKUM DALAM KEAMANAN INFORMASI PADA SISWA MADRASAH ALIYAH (MA) LABORATORIUM JAMBI

Rizka Fadhilah [1*], Anjelina Safitri [2], Riyan Nuriyadin [3]
[1,2,3] Program Studi Sistem Informasi, Universitas Islam Negeri Sultan Thaha Saifuddin Jambi
E-mail: riskafadhilah97@gmail.com, anjelynasafitri9@gmail.com, riyannuriyadin123@gmail.com

ABSTRACT

The development of information technology has brought significant changes in data management and administrative processes in various sectors, including educational institutions. Madrasah Aliyah, as an institution that has implemented digitalization, requires a robust information security system to protect student data, teachers, and school activities. This study aims to provide an understanding of the role of audits and legal aspects in maintaining information security, especially for MA Laboratorium Jambi students. The method used is a descriptive approach through socialization activities and direct presentations to students regarding information security audits, applicable legal regulations in Indonesia, and the importance of digital evidence in law enforcement. The results of the activities indicate that students gained a better understanding of cyber risks, information security governance, and legal bases such as the ITE Law and the Personal Data Protection Law. With this education, students are expected to be able to implement safe digital behavior and understand that activities in cyberspace have legal consequences.
Keywords: Information Security, Information System Audit, ITE Law, Personal Data Protection, Digital Evidence, Madrasah Aliyah.

ABSTRAK

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam pengelolaan data dan proses administrasi di berbagai sektor, termasuk lembaga pendidikan. Madrasah Aliyah sebagai institusi yang telah menerapkan digitalisasi membutuhkan sistem keamanan informasi yang kuat untuk melindungi data siswa, guru, maupun kegiatan sekolah. Penelitian ini bertujuan memberikan pemahaman mengenai peran audit dan aspek hukum dalam menjaga keamanan informasi, khususnya bagi siswa MA Laboratorium Jambi. Metode yang digunakan adalah pendekatan deskriptif melalui kegiatan sosialisasi dan presentasi langsung kepada siswa mengenai audit keamanan informasi, regulasi hukum yang berlaku di Indonesia, serta pentingnya bukti digital dalam penegakan hukum. Hasil kegiatan menunjukkan bahwa siswa memperoleh pemahaman yang lebih baik terkait risiko siber, tata kelola keamanan informasi, serta dasar hukum seperti UU ITE dan UU Perlindungan Data Pribadi. Dengan adanya edukasi ini, siswa diharapkan mampu menerapkan perilaku digital yang aman dan memahami bahwa aktivitas di dunia maya memiliki konsekuensi hukum.
Kata Kunci: Keamanan Informasi, Audit Sistem Informasi, UU ITE, Perlindungan Data Pribadi, Bukti Digital, Madrasah Aliyah.

Article History
Received: Desember 2025
Reviewed: Desember 2025
Published: Desember 2025

Plagiarism Checker No 796
Prefix DOI : Prefix DOI : 10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

1. PENDAHULUAN

Pengelolaan keamanan, pemanfaatan teknologi, dan penggunaan sistem informasi kini menjadi kebutuhan penting bagi berbagai instansi, termasuk sektor pemerintahan, industri, perusahaan, pendidikan, dan kesehatan, karena teknologi informasi mampu meningkatkan efisiensi dan kualitas layanan sesuai proses bisnis. Namun, ketergantungan ini juga meningkatkan risiko gangguan terhadap aset informasi, seperti pencurian atau penyalahgunaan data, sehingga diperlukan penerapan sistem manajemen keamanan informasi yang tepat. Dalam dunia pendidikan, proses digitalisasi beberapa tahun terakhir membuat sekolah semakin bergantung pada sistem informasi untuk administrasi, penyimpanan data, dan pembelajaran, yang pada saat sama membuka peluang serangan siber yang semakin kompleks. Penelitian di Indonesia menunjukkan bahwa institusi pendidikan menjadi salah satu target utama kebocoran data akibat lemahnya kontrol keamanan internal (Putra et al., 2020). Hal ini menegaskan bahwa keamanan informasi merupakan kebutuhan fundamental, bukan sekadar dukungan teknis tambahan.

Audit merupakan proses pengumpulan serta pengujian data oleh pihak yang berkompeten dan independen untuk menilai apakah informasi dan sistem yang digunakan telah sesuai dengan standar yang ditetapkan. Dalam konteks sistem informasi, audit membantu memastikan bahwa sistem yang berjalan mampu mendukung pencapaian tujuan organisasi secara efektif dan efisien. Pada lingkungan sekolah, audit keamanan informasi berperan penting untuk memeriksa kesiapan sistem terhadap berbagai risiko, mengidentifikasi celah keamanan, dan memastikan bahwa kontrol proteksi diterapkan dengan baik. Penelitian juga menunjukkan bahwa audit yang dilakukan secara rutin dapat meningkatkan ketahanan keamanan siber institusi pendidikan melalui penguatan aspek teknis maupun penglolaan (History & License, 2024). Dengan demikian, audit berperan sebagai instrumen evaluasi sekaligus alat pengawasan keberlanjutan keamanan informasi.

Selain aspek teknis, regulasi hukum menjadi faktor penting yang mendorong institusi pendidikan untuk mengelola data secara bertanggung jawab. Melalui UU Perlindungan Data Pribadi (UU PDP), sekolah sebagai pengendali data wajib menjaga kerahasiaan dan integritas informasi peserta didik serta menerapkan langkah keamanan yang memadai. Penelitian juga menegaskan bahwa lembaga pendidikan harus memahami konsekuensi hukum dari pengelolaan data yang tidak aman, termasuk sanksi administratif dan kerugian reputasi. UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi hadir sebagai jawaban atas meningkatnya urgensi perlindungan data di Indonesia, memberikan kepastian hukum, dan mencegah penyalahgunaan informasi pribadi (Inovasi et al., 2025). Meskipun kerangka hukum lain seperti UU ITE dan KUHP telah tersedia, penegakan aturan masih menghadapi tantangan, terutama dalam penggunaan forensik digital dan kebutuhan kerja sama internasional yang lebih kuat (Hukum et al., 2025). Penerapan audit dan kepatuhan hukum menjadi sangat penting karena sekolah telah mengintegrasikan teknologi dalam administrasi, penilaian, dan penyimpanan arsip digital, sehingga siswa MA Laboratorium dapat merasakan keamanan yang lebih baik terhadap perlindungan data pribadinya. Dengan keamanan informasi yang kuat, kepercayaan siswa terhadap tata kelola sekolah juga akan semakin meningkat.

2. METODE PENELITIAN

Pendekatan yang digunakan adalah deskriptif dengan metode sosialisasi langsung. Kegiatan sosialisasi dilaksanakan pada hari kamis, 25 September 2025 di Madrasah Aliyah (MA) Laboratorium Jambi yang melibatkan siswa sebagai audiens. Yang dimana kami melakukan prensentasi tentang audit keamanan informasi, peran audit dalam keamanan informasi, aspek hukum dalam keamanan informasi, dasar hukum di indonesia, dan bukti digital dalam penegekan hukum. Setelahnya ada sesi diskusi antara pemateri dengan audiens.

3. HASIL DAN PEMBAHASAN

1. Peran Audit Keamanan informasi

Audit keamanan informasi adalah proses pemeriksaan sistematis untuk menilai sejauh mana suatu organisasi telah melindungi data dan sistemnya dari ancaman. Audit ini bertujuan memastikan bahwa kebijakan, prosedur, serta teknologi yang digunakan benar-benar efektif menjaga kerahasiaan, keaslian, dan ketersediaan informasi. Bagi siswa Madrasah Aliyah (MA) Laboratorium, pemahaman tentang audit keamanan informasi penting agar mereka lebih sadar terhadap risiko siber, mampu menerapkan perilaku digital yang aman, serta dapat melindungi data pribadi maupun informasi sekolah dari penyalahgunaan. Ada beberapa peran audit dalam keamanan informasi yaitu sebagai berikut:

1. Memastikan penerapan kebijakan keamanan
2. Mengidentifikasi resiko dan kelemahan sistem
3. Mengukur kepatuhan terhadap standar ISO 270001
4. Memberikan rekomendasi perbaikan

2. Aspek Hukum dalam Keamanan Informasi

Keamanan informasi tidak hanya ditopang oleh penggunaan teknologi, tetapi juga oleh penerapan aturan hukum yang mengaturnya. Regulasi berfungsi sebagai landasan untuk melindungi setiap individu agar data pribadi, transaksi digital, dan aktivitas daring tetap terjaga keamanannya. Tanpa regulasi yang jelas, tindakan seperti pencurian data, penyebaran konten terlarang, maupun penipuan secara online akan sulit untuk diberi sanksi.

Di Indonesia, pemerintah telah menetapkan berbagai undang-undang dan kebijakan untuk menciptakan ketertiban dalam ruang siber. Peraturan tersebut tidak hanya melindungi pengguna, tetapi juga memberikan konsekuensi hukum bagi pihak yang melakukan pelanggaran, sehingga masyarakat terdorong untuk lebih cermat dan bertanggung jawab ketika memanfaatkan teknologi informasi. Bagi siswa Madrasah Aliyah (MA) Laboratorium, pemahaman terhadap aturan hukum ini sangat penting agar mereka dapat menggunakan internet secara bijak, menghindari pelanggaran digital, serta menyadari bahwa tindakan di dunia maya memiliki risiko dan konsekuensi hukum yang nyata. Saat ini, Indonesia memiliki beberapa dasar hukum yang mengatur keamanan informasi, antara lain:

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

Mengatur penggunaan teknologi informasi, transaksi elektronik, dan dokumen digital. Pengakuan sah bukti elektronik, larangan penyalahgunaan data, serta sanksi bagi penyebaran hoaks, pencemaran nama baik, penipuan online, dan akses ilegal.

2. UU No. 19 Tahun 2016 (Perubahan UU ITE)

Merupakan revisi UU ITE yang memperjelas pasal-pasal sebelumnya, terutama terkait ujaran kebencian, pencemaran nama baik, dan penyalahgunaan media sosial. Revisi ini juga memberikan perlindungan lebih adil bagi pengguna internet.

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

Mengatur hak masyarakat atas data pribadi, kewajiban penyelenggara sistem elektronik, dan sanksi bila terjadi kebocoran atau penyalahgunaan data. Poin penting: data pribadi tidak boleh dipakai tanpa izin pemilik, dan pelanggar bisa dikenai sanksi administratif maupun pidana.

4. Peraturan Pemerintah & Permenkominfo

Menjadi aturan turunan dari UU yang lebih teknis, misalnya tentang penyelenggaraan sistem elektronik, tata cara perlindungan data, dan standar keamanan siber.

5. KUHP & KUHAP

Meskipun tidak khusus mengatur teknologi, KUHP dan KUHAP digunakan dalam penegakan hukum pidana yang melibatkan bukti digital. Misalnya, pencurian data bisa dijerat dengan pasal pencurian, penipuan online bisa dikenakan pasal penipuan dalam KUHP.

3. Bukti Digital Dalam Penegakan Hukum

Dalam penegakan hukum, bukti digital memiliki kedudukan yang sama pentingnya dengan bukti konvensional. Berdasarkan UU ITE, data elektronik seperti pesan singkat, email, rekaman suara, log aktivitas server, hingga CCTV dapat dijadikan alat bukti yang sah di pengadilan. Agar dapat digunakan secara sah, bukti digital harus dijaga keasliannya, tidak dimanipulasi, dan mengikuti rantai penguasaan *(chain of custody)*. Dengan pengelolaan yang tepat, bukti digital mampu menjadi senjata utama dalam mengungkap kasus kejahatan siber sekaligus memberikan kepastian hukum bagi masyarakat.

4. KESIMPULAN

Berdasarkan kegiatan sosialisasi dan pembahasan materi, dapat disimpulkan bahwa keamanan informasi merupakan aspek penting yang harus diperhatikan dalam lingkungan pendidikan, terutama di Madrasah Aliyah yang mulai memanfaatkan sistem digital dalam proses administrasi dan pembelajaran. Audit keamanan informasi berperan penting dalam memastikan bahwa sistem yang digunakan sekolah telah memenuhi standar perlindungan data dan mampu mengidentifikasi celah keamanan. Selain itu, regulasi hukum seperti UU ITE, UU Perlindungan Data Pribadi, serta aturan turunan lainnya memberikan landasan yang jelas bagi sekolah dan siswa dalam menjaga keamanan data serta mencegah penyalahgunaan informasi. Pemahaman mengenai bukti

digital juga menjadi sangat penting karena bukti elektronik kini diakui sebagai alat bukti yang sah dalam penegakan hukum. Secara keseluruhan, siswa MA Laboratorium menunjukkan peningkatan pemahaman terkait risiko siber, aturan hukum, serta pentingnya menjaga keamanan informasi di lingkungan sekolah.

5. DAFTAR PUSTAKA

history, A., & License, I. (2024). Pentingnya Sistem Informasi Audit Dalam Meningkatkan Keamanan Data Perusahaan. *5*(4), 1–8.

Hukum, S., Judijanto, L., & Nugroho, B. (2025). *Regulasi Keamanan Siber Dan Penegakan Hukum Terhadap Cybercrime Di Indonesia*. *3*(3), 118–124.

Inovasi, J., Penelitian, H., & Vol, P. (2025). *Urgensi Perlindungan Data Pribadi Dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022*. *5*(2), 247–257.

Keadilan, J. P., Fahmi, M. H., Tambunan, H. M., & Semarang, U. N. (2024). *Ancaman Cybercrime Di Indonesia*. *3*(2), 72–80.

Morizha, K. Al, Mayla, Z., & Informasi, S. K. (2025). *Audit Keamanan Sistem Informasi Menggunakan*. *19*, 338–345.

Paramita, S., Siregar, S. A., Damanik, R. A., & Irawan, M. D. (2022). *Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (Kami) Iso 27001 : 2013*. *3*(4), 374–379.

Putra, D. Y., Wati, T., & P, I. W. W. (2020). *Audit Keamanan Sistem Informasi Berdasarkan Sni - Iso 27001 Pada Sistem Informasi Akademik Universitas Pembangunan Nasional " Veteran " Jakarta*. *Sinaptika*.