Analisis Sistem Informasi Sumber Daya Manusia (HRIS) Menggunakan NIST SP 800-30 Pada PT. Andhana Kirana Yasa

Halvis Aquariyanto Fauzan[1], Anggi Elanda[2], Mockamad Wahidin[3]
[1]Program Studi Sistem Informasi, STMIK ROSMA
Karawang, Indonesia
halvis.fauzan@mhs.rosma.ac.id, anggi@rosma.ac.id , m.wahidin@dosen.rosma.ac.id

ABSTRAK

PT. Andhana Kirana Yasa menggunakan Human Resource Information System (HRIS) sebagai sistem informasi dalam mendukung pengelolaan data karyawan, absensi, cuti, payroll, dan administrasi sumber daya manusia. Seiring dengan pemanfaatan teknologi informasi, sistem HRIS memiliki berbagai risiko yang bisa memengaruhi kerahasiaan, integritas, dan ketersediaan informasi. Oleh karena itu, penelitian ini dilangsungkan dalam menelaah risiko keamanan pada sistem HRIS menggunakan framework NIST SP 800-30.

Penelitian ini menerapkan pendekatan deskriptif kualitatif melalui metode pengambilan data yakni wawancara dan dokumen ceklis. Analisis risiko dilakukan berdasarkan tahapan NIST SP 800-30 yang meliputi System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendation, dan Results Documentation.

Hasil penelitian menunjukkan bahwa sistem HRIS PT. Andhana Kirana Yasa memiliki beberapa risiko keamanan, seperti akses tidak sah, kebocoran data, penyalahgunaan hak akses, dan human error. Berdasarkan analisis yang dilakukan, sebagian besar aset berada pada tingkat risiko tinggi sehingga memerlukan perhatian khusus dalam pengelolaan keamanan sistem. Penelitian ini menghasilkan rekomendasi pengendalian berupa penguatan keamanan akses, pengelolaan hak akses pengguna, monitoring aktivitas sistem, serta pemeliharaan dan backup data secara berkala. Temuan yang ada diproyeksikan bisa dijadikan bahan evaluasi bagi perusahaan untuk memperketat keamanan sistem HRIS dan meminimalkan risiko yang dapat mengganggu operasional perusahaan.

Kata kunci: Human Resource Information System (HRIS), Analisis Risiko, Keamanan Informasi, NIST SP 800-30, Manajemen Risiko.

ABSTRACT

PT. Andhana Kirana Yasa uses a Human Resource Information System (HRIS) to support employee data management, attendance, leave, payroll, and human resource administration. Along with the use of information technology, HRIS systems pose various risks that can impact the confidentiality, integrity, and availability of information. Therefore, this study was conducted to examine security risks in the HRIS system using the NIST SP 800-30 framework.

This study employed a qualitative descriptive approach through data collection methods, including interviews and document checklists. The risk analysis was conducted based on the NIST SP 800-30 stages, which include System Characterization, Threat Identification,

Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendation, and Results Documentation.

The results indicate that PT. Andhana Kirana Yasa's HRIS system faces several security risks, such as unauthorized access, data breaches, misuse of access rights, and human error. Based on the analysis, most assets are at high risk, requiring special attention in system security management. This research yielded control recommendations in the form of strengthening access security, managing user access rights, monitoring system activity, and regular data maintenance and backup. The findings are projected to serve as evaluation material for companies to tighten HRIS system security and minimize risks that could disrupt operations.

Keywords: Human Resource Information System (HRIS), Risk Analysis, Information Security, NIST SP 800-30, Risk Management.

Pendahuluan

Organisasi dan perusahaan pada khususnya telah sangat terpengaruh oleh transformasi yang dibawa oleh kemajuan teknologi informasi di era digital modern. Keputusan yang lebih baik dan tepat waktu dimungkinkan karena kemampuan TI untuk menangani data dengan lebih cepat, akurat, dan efisien. Organisasi sering menggunakan HRIS, atau sistem informasi sumber daya manusia, sebagai salah satu implementasi teknologi informasi.

Sistem informasi sumber daya manusia (Human Resource Information Systems/HRIS) menangani berbagai tugas dan data yang berkaitan dengan SDM, termasuk penggajian, pelacakan kehadiran, perekrutan, dan tinjauan kinerja. Peningkatan efisiensi operasional, berkurangnya kesalahan pemrosesan data, dan informasi yang lebih akurat dan transparan adalah semua manfaat yang dapat diperoleh perusahaan dari implementasi HRIS. Selain itu, HRIS sangat penting dalam memfasilitasi pengambilan keputusan strategis berbasis data.

Permasalahan utama yang dihadapi adalah belum adanya analisis risiko secara terstruktur terhadap HRIS yang diterapkan. Tanpa analisis risiko yang jelas, perusahaan tidak dapat mengidentifikasi ancaman yang mungkin terjadi, mengetahui tingkat kerentanan sistem, serta memahami dampak yang dapat ditimbulkan. Hal ini menyebabkan perusahaan kesulitan dalam menentukan langkah mitigasi yang tepat untuk mengurangi risiko yang ada.

Analisis risiko sistem informasi memerlukan prosedur yang sistematis. Penilaian risiko keamanan sistem informasi dapat dilakukan melalu kerangka kerja seperti NIST SP 800-30. Untuk membantu perusahaan menilai risiko dan menerapkan strategi mitigasi yang sesuai, kerangka kerja ini menawarkan pendekatan sistematis untuk mengidentifikasi aset, ancaman, kerentanan, dan konsekuensi risiko.

Tujuan dilangsungkannya penelitian ini ialah menganalisis sistem informasi SDM PT. Andhana Kirana Yasa menggunakan NIST SP 800-30 untuk mengidentifikasi potensi risiko keamanan. Keputusan tentang manajemen risiko dan peningkatan keamanan sistem informasi di masa mendatang kemungkinan besar juga akan dipengaruhi oleh temuan penelitian ini.

Materi dan Metode

Sistem Informasi Sumber Daya Manusia (HRIS)

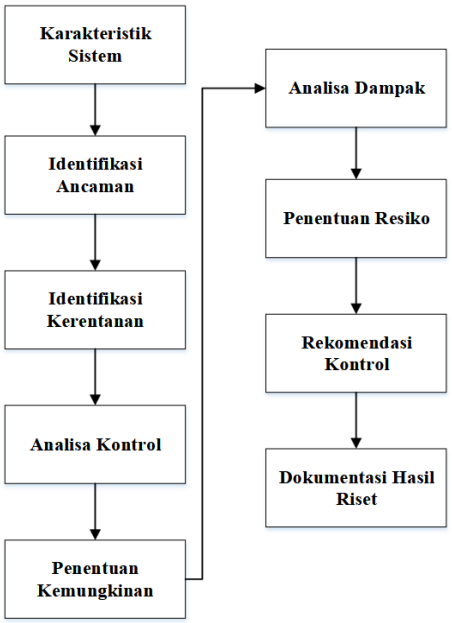
HRIS adalah sistem manajemen basis data dan informasi terkomputerisasi yang digunakan perusahaan untuk melacak dan memahami informasi yang berkaitan dengan departemen SDM-nya. HRIS memungkinkan bisnis untuk mengelola data mereka dengan lebih baik dengan menggabungkan berbagai tugas SDM ke dalam satu platform digital.[1]

Manajemen data personel, penggajian, pelatihan, kehadiran, dan evaluasi kinerja adalah beberapa komponen utama dari HRIS. Dengan menerapkan HRIS, bisnis dapat menyederhanakan pengambilan keputusan terkait SDM, meningkatkan akurasi data, dan mengurangi ketergantungan pada proses manual. Selain itu, HRIS memungkinkan integrasi data lintas departemen, yang meningkatkan konsistensi dan memberikan akses ke informasi secara real-time.

Metode Penelitian

Penelitian ini menggunakan metode deskriptif kualitatif untuk menganalisis risiko keamanan pada Human Resource Information System (HRIS) di PT. Andhana Kirana Yasa. Pendekatan ini dipilih karena penelitian berfokus pada identifikasi ancaman, kerentanan, dampak, dan tingkat risiko yang terdapat pada sistem HRIS berdasarkan kondisi aktual perusahaan.

Pengumpulan data dilakukan melalui wawancara dengan pihak yang terlibat dalam penggunaan dan pengelolaan HRIS, seperti admin HRIS dan staf Human Resource, serta menggunakan dokumen ceklis untuk memperoleh informasi mengenai aset, ancaman, kerentanan, dan pengendalian yang telah diterapkan pada sistem. Data yang diperoleh kemudian dianalisis menggunakan framework NIST SP 800-30 sebagai pedoman analisis risiko.



Gambar 1. 1 Prosedur Penelitian

Tahapan analisis risiko yang dilakukan meliputi:

1. System Characterization
2. Threat Identification
3. Vulnerability Identification

4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Hasil dari tahapan tersebut digunakan untuk mengetahui tingkat risiko keamanan pada HRIS PT. Andhana Kirana Yasa serta menghasilkan rekomendasi pengendalian yang dapat diterapkan guna meningkatkan keamanan dan keandalan sistem informasi perusahaan.

Hasil dan Pembahasan

1. Karakteristik Sistem

System Characterization merupakan tahap awal dalam analisis risiko menerapkan framework NIST SP 800-30 yang bertujuan untuk mengidentifikasi aset yang berkaitan dengan sistem Human Resource Information System (HRIS) pada PT Andhana Kirana Yasa. Identifikasi aset dilakukan untuk mengetahui komponen yang memiliki nilai penting bagi perusahaan dan berpotensi terdampak apabila terjadi ancaman keamanan informasi.

.

Tabel 1. 1 Karakteritik Sistem

No	ID Aset	Nama Aset	Proses Bisnis	Kategori Aset
1	SW_1	Sistem HRIS	Mengelola data dan aktivitas sumber daya manusia perusahaan	Software
2	DT_1	Data Karyawan	Menyimpan data identitas dan informasi karyawan	Data
3	DT_2	Data Absensi	Mencatat kehadiran dan aktivitas absensi karyawan	Data
4	DT_3	Data Cuti dan Izin	Mengelola pengajuan dan persetujuan cuti karyawan.	Data
5	DT_4	Data Payroll	Menyimpan informasi penggajian dan tunjangan karyawan	Data
6	SDM_1	Admin HRIS	Mengelola data dan hak akses pengguna sistem	Sumber Daya Manusia
7	SDM_2	Staf Human Resource	Mengelola administrasi kepegawaian melalui HRIS	Sumber Daya Manusia
8	SDM_3	Karyawan	Menggunakan HRIS untuk absensi, cuti, dan informasi kepegawaian	Sumber Daya Manusia
9	VEN_1	Vendor HRIS	Mengelola sistem, server, maintenance, dan pembaruan aplikasi	Pihak Ketiga

2. Identifikasi Ancaman (Threat Identification)

Berdasarkan hasil wawancara dan observasi, sistem HRIS PT Andhana Kirana Yasa menyimpan berbagai data penting seperti data karyawan, absensi, cuti, dan payroll. Oleh karena itu, sistem memiliki potensi ancaman yang dapat menyebabkan gangguan operasional maupun kerugian bagi perusahaan apabila tidak dikelola dengan baik.

Tabel 1. 2 Identifikasi Ancaman

No	Kode	Jenis Kejadian	Keterangan	Aset
1	W1	Password lemah	Password pengguna yang mudah ditebak	Sistem HRIS
2	W2	Kurangnya kesadaran keamanan pengguna	Pengguna kurang memahami pentingnya keamanan informasi	Admin HRIS, Karyawan
3	W3	Monitoring aktivitas pengguna belum optimal	Aktivitas pengguna belum dipantau secara maksimal	Sistem HRIS
4	W4	Ketergantungan pada vendor	Pengelolaan sistem sepenuhnya dilakukan vendor	Sistem HRIS
5	W5	Kesalahan input data	Pengguna melakukan kesalahan saat memasukkan data	Data Karyawan, Data Absensi
6	T1	Akses tidak sah	Pihak yang tidak berwenang mengakses sistem HRIS	Sistem HRIS, Data Karyawan
7	T2	Phishing	Pencurian akun pengguna melalui email atau tautan palsu	Admin HRIS, Karyawan
8	T3	Malware atau Virus	Serangan malware yang dapat merusak sistem atau data	Sistem HRIS
9	T4	Kebocoran data	Data karyawan diketahui atau disebarkan pihak yang tidak berwenang	Data Karyawan, Data Payroll
10	T5	Penyalahgunaan hak akses	Pengguna memanfaatkan hak akses untuk kepentingan tertentu	Sistem HRIS
11	T6	Gangguan jaringan	Koneksi internet terganggu sehingga sistem tidak dapat diakses	Sistem HRIS

No	Kode	Jenis Kejadian	Keterangan	Aset
12	T7	Kegagalan sistem	Terjadi error atau gangguan pada aplikasi HRIS	Sistem HRIS
13	T8	Kehilangan data	Data hilang akibat kesalahan sistem atau pengguna	Data Karyawan, Data Payroll

3. Identifikasi Kerentanan (Vulnerability Identification)

Berdasarkan hasil wawancara dan observasi, ditemukan beberapa kerentanan yang berkaitan dengan penggunaan sistem, pengelolaan hak akses, keamanan data, serta faktor pengguna.

Tabel 1. 3 Identifikasi Kerentanan

No	Ancaman	Kerentanan	Aset Terdampak
1	Akses tidak sah	Password pengguna mudah ditebak	Sistem HRIS
2	Akses tidak sah	Pengguna tidak melakukan logout setelah menggunakan sistem	Sistem HRIS
3	Kebocoran data	Pengelolaan hak akses belum sepenuhnya diawasi secara berkala	Data Karyawan
4	Penyalahgunaan hak akses	Monitoring aktivitas pengguna belum optimal	Sistem HRIS
5	Human Error	Kurangnya kesadaran pengguna terhadap keamanan informasi	Admin HRIS, Karyawan
6	Human Error	Kesalahan penginputan data oleh pengguna	Data Karyawan
7	Malware atau Virus	Pengguna mengakses file atau tautan yang tidak diketahui keamanannya	Sistem HRIS
8	Phishing	Pengguna kurang memahami ciri-ciri email atau tautan palsu	Admin HRIS, Karyawan
9	Kehilangan data	Ketergantungan pada proses backup yang dilakukan vendor	Data Karyawan, Data Payroll
10	Gangguan sistem	Ketergantungan terhadap layanan vendor HRIS	Sistem HRIS
11	Gangguan jaringan	Koneksi internet yang tidak stabil	Sistem HRIS
12	Kegagalan sistem	Error aplikasi yang memerlukan penanganan vendor	Sistem HRIS

4. Analisis Kontrol (Control Analysis)

Berdasarkan hasil wawancara dan observasi, PT Andhana Kirana Yasa telah menerapkan beberapa bentuk pengendalian keamanan pada sistem HRIS. Pengendalian tersebut dilakukan baik oleh perusahaan maupun vendor sebagai pihak ketiga yang mengelola sistem

HRIS. Pengendalian yang diterapkan berfokus pada keamanan akses pengguna, perlindungan data, pengelolaan sistem, dan penanganan gangguan yang terjadi pada sistem.

Tabel 1. 4 Analisis Kontrol

No	Ancaman/Kerentanan	Pengendalian yang Diterapkan
1	Password lemah	Pengguna diwajibkan menggunakan akun login pribadi
2	Akses tidak sah	Sistem menggunakan username dan password untuk autentikasi pengguna
3	Penyalahgunaan hak akses	Hak akses dibatasi sesuai tugas dan jabatan pengguna
4	Kebocoran data karyawan	Data hanya dapat diakses oleh pengguna yang memiliki wewenang
5	Human error	Pengguna diberikan arahan mengenai penggunaan sistem HRIS
6	Malware atau virus	Perangkat kerja menggunakan antivirus
7	Kehilangan data	Backup data dilakukan secara berkala oleh vendor
8	Gangguan sistem	Vendor melakukan maintenance dan pembaruan sistem secara berkala
9	Kegagalan sistem	Vendor menyediakan layanan perbaikan apabila terjadi gangguan
10	Gangguan jaringan	Perusahaan menggunakan jaringan internet yang mendukung operasional HRIS
11	Phishing	Akses akun dibatasi sesuai identitas pengguna
12	Monitoring aktivitas pengguna	Pengawasan dilakukan oleh bagian HR dan admin HRIS

5. Penentuan Kemungkinan Risiko (Likelihood Determination)

Tahap ini dilakukan untuk menilai kemungkinan terjadinya risiko berdasarkan ancaman dan kerentanan yang ditemukan.

Tabel 1. 5 Penentuan Likelihood Risiko Sistem

Kode Aset	Nama Aset	Risiko	Nilai Likelihood	Tingkat Kemungkinan
SW_1	Sistem HRIS	Gangguan sistem HRIS	0,80	Sering
DT_1	Data Karyawan	Kebocoran data	0,50	Sedang
DT_2	Data Absensi	Kesalahan input data	0,70	Sering
DT_3	Data Cuti dan Izin	Kesalahan pengelolaan data	0,70	Sering
DT_4	Data Payroll	Kebocoran data payroll	0,50	Sedang
SDM_1	Admin HRIS	Akses tidak sah	0,60	Sedang

SDM_2	Staf Human Resource	Human error	0,70	Sering
SDM_3	Karyawan	Penyalahgunaan akun	0,60	Sedang
VEN_1	Vendor HRIS	Gangguan layanan vendor	0,20	Sangat Jarang

6. Analisis Dampak (Impact Analysis)

Analisis dampak dilakukan untuk mengetahui konsekuensi yang mungkin terjadi apabila risiko benar-benar terjadi

Tabel 1. 6 Tingkat dampak

Kode Aset	Nama Aset	Dampak	Tingkat Dampak
SW_1	Sistem HRIS	Sistem tidak dapat digunakan sehingga menghambat aktivitas pengelolaan SDM	Sangat Besar
DT_1	Data Karyawan	Kebocoran data pribadi karyawan	Sangat Besar
DT_2	Data Absensi	Kesalahan data absensi yang memengaruhi perhitungan kehadiran	Besar
DT_3	Data Cuti dan Izin	Kesalahan data cuti yang mengganggu administrasi karyawan	Sedang
DT_4	Data Payroll	Kesalahan atau kebocoran data penggajian	Sangat Besar
SDM_1	Admin HRIS	Penyalahgunaan hak akses yang memengaruhi keamanan sistem	Besar
SDM_2	Staf Human Resource	Human error yang menyebabkan kesalahan pengelolaan data	Besar
SDM_3	Karyawan	Kesalahan penggunaan sistem oleh pengguna	Sedang
VEN_1	Vendor HRIS	Gangguan layanan yang menyebabkan keterlambatan akses sistem	Kecil

7. Penentuan Tingkat Risiko (Risk Determination)

Penentuan tingkat risiko dilakukan dengan mengombinasikan nilai likelihood dan impact menggunakan matriks risiko.

Tabel 1. 7 Penentuan Kemungkinan

Likelihood	Impact Rendah (1)	Impact Sedang (3)	Impact Tinggi (5)
Tinggi	Sedang	Tinggi	Tinggi
Sedang	Rendah	Sedang	Tinggi

Rendah	Rendah	Rendah	Sedang

8. Rekomendasi Kontrol

Rekomendasi yang dihasilkan meliputi:

a. Penerapan Multi-Factor Authentication (MFA).
b. Penguatan kebijakan kata sandi pengguna.
c. Pembatasan hak akses berdasarkan peran (role-based access control).
d. Monitoring aktivitas pengguna secara berkala.
e. Backup data rutin dan pengujian proses pemulihan data.
f. Pelatihan keamanan informasi bagi pengguna sistem.

Implementasi rekomendasi tersebut diharapkan dapat mengurangi tingkat risiko dan meningkatkan keamanan sistem HRIS di PT. Andhana Kirana Yasa.

Kesimpulan

Penelitian ini berhasil menganalisis risiko keamanan pada Human Resource Information System (HRIS) PT. Andhana Kirana Yasa menggunakan framework NIST SP 800-30. Hasil penelitian menunjukkan adanya ancaman seperti akses tidak sah, kebocoran data, phishing, malware, dan human error. Sebagian besar aset HRIS berada pada tingkat risiko tinggi, sehingga memerlukan perhatian khusus dalam pengelolaan keamanan sistem. Oleh karena itu, diperlukan penguatan kontrol keamanan, pengelolaan hak akses, monitoring aktivitas pengguna, serta backup data secara berkala untuk mengurangi risiko dan menjaga keamanan informasi perusahaan.

Daftar Pustaka

Dassler, G. (2019). *Human_Resource_Management*. *16*, 1–684.

Elanda, A., & Lintang Buana, R. (2021). *Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus : STMIK Rosma)*. *14*(1), 141–151. http://journal.stekom.ac.id/index.php/elkom■page1

JOGIYANTO, H. M. (2007). *Sistem Informasi Keperilakuan*. Penerbit Andi Yogyakarta.

Kasus, S., Badan, :, Statistik, P., Barat, K., Putri, T. S., Mutiah, N., Prawira, D., Informasi, J. S., Mipa, F., Tanjungpura, U., Prof, J., Hadari, H., & Pontianak, N. (n.d.). *Coding : Jurnal Komputer dan Aplikasi*.

Kenneth C, L. J. P. L. (2021). *Management_Information_Systems_Managing*. 649.

Michael E. Whitman, H. J. M. (2017). *Principles_of_Information_Security*. 1–656.

Sommerville, Ian. (2016). *Software engineering*. Pearson.

Stallings, W. (2017). *Effective Cybersecurity: Understanding and Using Standards and Best Practices*.

Thomas R. Peltier Justin Peltier John Blackley. (2016). *Information Security Fundamentals*.

United Nations Industrial Development Organization. (2021). *ISO 31000:2018 : Risk management - a practical guide*. United Nations Industrial Development Organization ; International Standards Organization.

US DEPARTMENT OF COMMERCE. (2012). *Guide for conducting risk assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

US DEPARTMENT OF COMMERCE. (2020). *Security and Privacy Controls for Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r5

Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security Sixth Edition*. www.cengage.com.

Wisnu Alfiansyah, M., Michael Lauw, C., & Fahmi, R. (2025). AUDIT KEAMANAN TEKNOLOGI INFORMASI DENGAN NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY (NIST) 800-30 PADA PD INDAH PERMAI GROUP. *Jurnal Manajemen Informatika & Sistem Informasi (MISI)*, *8*(1). https://doi.org/10.36595/misi.v5i2

Zuhriyah, A., & Pakarbudi, A. (n.d.). *SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika Penilaian Risiko Keamanan Informasi Menggunakan Standar NIST SP 800-30 pada PT.XYZ*. https://doi.org/10.31284/p.snestik.2024.5835