INNOVATIVE: Journal Of Social Science Research
Volume 5 Nomor 4 Tahun 2025 Page 7542-7556
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Analisis ISO 27001: 2022 Terhadap Ketahanan Infrastruktur ICT Perguruan Tinggi Dari Serangan Ransomware (Studi Kasus ICT UIN Ar-Raniry)

Safira Mustaqillah[1✉], Aulia Syarif Aziz[2]
UIN Ar-Raniry Banda Aceh
Email: 200212013@student.ar-raniry.ac.id[1✉]

Abstrak

Ketahanan infrastruktur teknologi informasi menjadi aspek krusial bagi perguruan tinggi yang bergantung pada sistem digital, termasuk UIN Ar-Raniry. Penelitian ini mengevaluasi praktik backup informasi oleh tim ICT serta kontribusinya terhadap ketahanan sistem, dengan mengacu pada kontrol A.5.34 ISO 27001:2022. Metode yang digunakan adalah kuantitatif deskriptif melalui kuesioner dan analisis statistik. Fokus kajian meliputi perencanaan, perlindungan data cadangan, dan kesiapan pemulihan insiden. Hasil menunjukkan backup dilakukan rutin namun tanpa dokumentasi formal dan prosedur pemulihan terstruktur. Meskipun ISO 27001 belum diterapkan secara resmi, kontrol A.5.34 berpotensi menjadi acuan strategis. Disarankan penyusunan SOP backup, pengujian restore berkala, dan penguatan kontrol keamanan ICT.

Kata kunci: *ISO 27001:2022, A.5.34, Backup Informasi, Ketahanan ICT, Perguruan Tinggi*

Abstract

The resilience of information technology infrastructure is crucial for higher education institutions that rely on digital systems, including UIN Ar-Raniry. This study evaluates the information backup practices of the ICT team and their contribution to system resilience, referring to control A.5.34 of ISO 27001:2022. A descriptive quantitative method was used, involving questionnaires and statistical analysis. The evaluation focuses on planning, backup data protection, and incident recovery readiness. Findings show that while backups are performed regularly, they lack formal documentation and structured recovery procedures. Although ISO 27001 has not been formally implemented, control A.5.34 has the potential to serve as a strategic reference. The study recommends establishing backup SOPs, conducting regular restore tests, and strengthening ICT security controls.

Keywords: *ISO 27001:2022, A.5.34, Information Backup, ICT Resilience, Higher Education*

PENDAHULUAN

Era digital yang semakin mendunia saat ini, menjadikan keamanan informasi sebagai prioritas utama bagi individu, organisasi, dan pemerintah. Meskipun teknologi memberikan banyak kemudahan, ada risiko serius jika pengelolaannya tidak tepat. Salah satu risiko utama adalah masalah keamanan informasi, yang dapat menimbulkan kerancuan dan gangguan dalam sistem teknologi informasi dan komunikasi. (Fauzia Anis Sekar Ningrum et al., 2024).

Dalam keamanan jaringan, terdapat tiga aspek utama yang harus diamati: ketersediaan, keaslian dan kerahasiaan. Seiring berkembangnya teknologi, keamanan jaringan menjadi semakin penting karena setiap individu berupaya menjaga integritas serta melindungi data mereka dari ancaman (Aziz, 2021).

Kemajuan teknologi informasi membuat perguruan tinggi semakin bergantung pada sistem digital untuk pembelajaran dan manajemen data, namun juga meningkatkan risiko ancaman siber seperti ransomware dan malware. Keamanan siber penting untuk melindungi sistem dan data vital. Institusi wajib menerapkan teknologi, kebijakan, dan prosedur guna menjaga keamanan, reputasi, kepatuhan regulasi, dan kelangsungan layanan (Prasetyo et al., 2024).

Standar ISO/IEC 27001, khususnya kontrol A.5.34 tentang backup data yang aman, terdokumentasi, dan teruji, dapat digunakan untuk menganalisis keamanan informasi di organisasi, termasuk di bidang pendidikan (Tuga & Aziz, 2019). Meskipun UIN Ar-Raniry belum menerapkan standar ini secara formal, unit ICT telah melakukan backup, namun efektivitasnya terhadap ancaman seperti ransomware belum dievaluasi secara mendalam.

Penelitian ini bertujuan mengevaluasi praktik backup informasi di ICT UIN Ar-Raniry berdasarkan kontrol A.5.34 ISO/IEC 27001:2022. Evaluasi ini diharapkan dapat

mengidentifikasi kelemahan dalam perencanaan backup. ISO/IEC 27001 sendiri merupakan standar keamanan informasi yang banyak digunakan secara global, dengan edisi terbarunya dirilis pada 25 Oktober 2022 untuk menjawab tantangan keamanan siber dan meningkatkan kepercayaan digital.(Jelita et al., 2024).

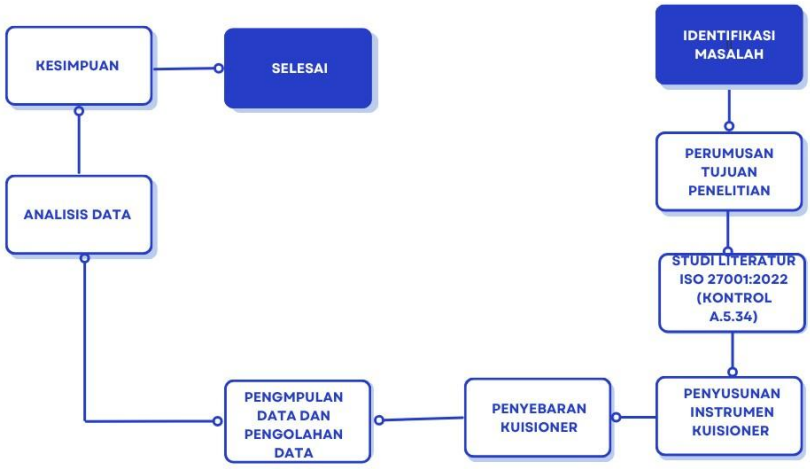
METODE PENELITIAN

Desain Penelitian.

Penelitian ini menggunakan pendekatan kuantitatif deskriptif untuk mengevaluasi praktik backup informasi di ICT UIN Ar-Raniry berdasarkan kontrol A.5.34 ISO 27001:2022. Data dikumpulkan melalui kuesioner skala Likert yang disebarkan kepada staf ICT dan mahasiswa, dengan instrumen disesuaikan menurut peran masing-masing dalam pengelolaan dan pemanfaatan sistem informasi(Meilani et al., 2020).

Untuk menggambarkan proses penelitian secara sistematis, peneliti menyusun diagram alur yang mencakup tahapan dari perumusan masalah, penyusunan instrumen, pengumpulan data, hingga analisis dan interpretasi hasil. Alur ini disusun berdasarkan pendekatan kuantitatif deskriptif evaluatif, dengan fokus pada evaluasi implementasi kontrol A.5.34 ISO 27001:2022 di lingkungan ICT UIN Ar-Raniry. Penyajian ini bertujuan memberikan gambaran menyeluruh dan terstruktur mengenai tahapan metodologis yang dilakukan.

Diagram alur penelitian tersebut dapat dilihat pada Gambar 1 di bawah ini :



Gambar 1. Alir Diagram Penelitian

Populasi Dan Sampel

Populasi penelitian ini mencakup seluruh staf ICT dan mahasiswa UIN Ar-Raniry yang terlibat dalam pengelolaan atau pemanfaatan sistem informasi kampus. Mengingat jumlah staf ICT yang relevan terbatas dan jumlah mahasis¥wa sangat besar, peneliti menggunakan

purposive sampling untuk staf ICT dan convenience sampling untuk mahasiswa, berdasarkan aksesibilitas dan relevansi terhadap fokus penelitian.

Penelitian ini menggunakan sampel sebanyak 110 orang, yang terdiri dari:

1. Staf ICT (10 orang)

Dipilih secara purposif dari personel yang memiliki tanggung jawab langsung terhadap backup informasi, meliputi:

1. Administrator Jaringan
2. Pengelola Server
3. Tim Keamanan Informasi
4. Teknisi Infrastruktur
5. Helpdesk atau Layanan Pengguna
6. Kepala Bidang Sistem Informasi
7. Operator Data Center
8. Tim Pemulihan Bencana
9. Analis Sistem
10. Kepala Seksi Teknologi Informasi

2. Mahasiswa (100 orang)

Dipilih secara convenience dari berbagai fakultas di UIN Ar-Raniry yang aktif menggunakan sistem ICT kampus, dengan tujuan mendapatkan gambaran persepsi pengguna terhadap ketahanan sistem informasi.

Instrumen dan Prosedur Penelitian

Instrumen penelitian berupa kuesioner tertutup dengan skala Likert 1–5, dari "sangat tidak setuju" hingga "sangat setuju," yang umum digunakan untuk mengukur sikap dan persepsi(Utami, 2023). Kuesioner mencakup indikator utama: perencanaan backup, keamanan backup, pengujian pemulihan, dan ketahanan infrastruktur ICT. Isi instrumen disesuaikan untuk staf ICT dan mahasiswa sesuai peran dan keterlibatan mereka dalam sistem informasi kampus.

Data dikumpulkan menggunakan metode non-probability sampling dengan dua teknik, purposive sampling untuk staf ICT yang memiliki keahlian dan tanggung jawab di bidang jaringan dan keamanan informasi, serta convenience sampling untuk mahasiswa berdasarkan kemudahan akses dan ketersediaan partisipan dari berbagai fakultas (Amanda et al., 2019).

Sebelum analisis, instrumen diuji kelayakannya melalui uji validitas dan reliabilitas. Uji validitas menggunakan Pearson Product Moment, dengan kriteria item valid jika r- hitung > r-tabel pada signifikansi 5% ($p < 0,05$), dan semua item memenuhi syarat ini. Uji reliabilitas

menggunakan Cronbach's Alpha, yang menunjukkan nilai di atas 0,90 untuk seluruh variabel, menandakan konsistensi internal sangat tinggi dan instrumen dapat diandalkan untuk pengumpulan data.

Setelah data terkumpul, dilakukan uji asumsi klasik berupa uji normalitas dan heteroskedastisitas. Selanjutnya, analisis regresi linier berganda dimanfaatkan untuk menilai sejauh mana variabel independen memberikan dampak terhadap variabel dependen, untuk mengukur ketahanan infrastruktur ICT. Analisis dilakukan dengan software SPSS, dengan interpretasi hasil berdasarkan nilai signifikansi, koefisien regresi, dan koefisien determinasi (R^2) (Janah & Kartini, 2022).

Teknik Analisis Data

Penelitian ini menggunakan pendekatan kuantitatif dengan bantuan SPSS. Uji validitas dilakukan dengan Pearson Product Moment untuk memastikan item kuesioner sahih, dan uji reliabilitas menggunakan Cronbach's Alpha, dengan nilai > 0,60 yang menunjukkan instrumen reliabel dan konsisten

Uji normalitas (Kolmogorov-Smirnov), heteroskedastisitas (scatter plot), dan regresi linier berganda digunakan untuk menganalisis pengaruh variabel backup terhadap ketahanan ICT. Uji t mengukur pengaruh parsial, R^2 menunjukkan kontribusi total variabel bebas.

HASIL DAN PEMBAHASAN

Penelitian ini bertujuan mengevaluasi praktik backup informasi di ICT UIN Ar-Raniry dan menilai kontribusinya terhadap ketahanan infrastruktur kampus terhadap serangan siber, khususnya ransomware. Data diperoleh melalui kuesioner tertutup skala Likert yang disebarkan kepada 10 staf ICT dan 100 mahasiswa dari berbagai fakultas.

Hasil penelitian mencakup uji validitas dan reliabilitas, uji asumsi klasik (normalitas dan heteroskedastisitas), serta regresi linier berganda untuk mengukur pengaruh perencanaan backup, keamanan backup, dan pengujian pemulihan terhadap ketahanan infrastruktur ICT.

Evaluasi Kontrol A.5.34 Terhadap Ketahanan Infrastruktur

UIN Ar-Raniry, sebagai perguruan tinggi negeri di Banda Aceh, mengandalkan infrastruktur ICT untuk mendukung kegiatan akademik dan administrasi. Dengan meningkatnya ancaman siber seperti ransomware, institusi perlu memiliki sistem backup yang aman dan andal. ISO/IEC 27001:2022, khususnya kontrol A.5.34, menekankan pentingnya proses backup yang terdokumentasi, aman, dan diuji secara berkala untuk menjaga ketersediaan data saat terjadi gangguan.(April, 2025).

Penelitian ini mengevaluasi penerapan kontrol A.5.34 di ICT UIN Ar-Raniry, mencakup kebijakan backup, keamanan data, dan uji pemulihan, untuk menilai ketahanan data terhadap ancaman siber sesuai standar ISO.

Responden

Penelitian ini melibatkan dua kelompok responden dengan pendekatan non-probability sampling. Sampel staf ICT diambil menggunakan purposive sampling, yaitu pemilihan individu yang memiliki pemahaman mendalam tentang implementasi backup informasi.

Sebanyak 10 staf ICT dilibatkan, mencakup personel jaringan, server, keamanan informasi, dan layanan pengguna. Responden mahasiswa dipilih dengan teknik convenience sampling, berdasarkan kemudahan akses dan ketersediaan partisipasi Sebanyak 100 mahasiswa dari berbagai fakultas berpartisipasi untuk memberikan gambaran persepsi pengguna terhadap ketahanan infrastruktur ICT UIN Ar-Raniry.

Evaluasi Kelayakan Instrumen Penelitian

Untuk keperluan analisis dan kejelasan penyajian data, hasil uji instrument penelitian dibedakan antara responden staf ICT dan Mahasiswa.

1. Uji Validitas

Instrumen penelitian diuji validitasnya terhadap dua kelompok responden, yaitu staf ICT dan mahasiswa, menggunakan korelasi Pearson Product Moment. Item dinyatakan valid jika r hitung > r tabel.

Seluruh item kuesioner valid untuk kedua kelompok responden. Pada staf ICT (n=10) dengan r tabel 0,632, dan mahasiswa (n=100) dengan r tabel 0,195, semua item memenuhi kriteria. Instrumen dinyatakan layak untuk analisis berikutnya.

Tabel 1. Hasil Uji Validasi Staff dan Mahasiswa

Kelompok Responden	Jumlah Item	r Tabel	Jumlah Item	Keterangan
Staff ICT	20	0,632	20	Valid
Mahasiswa	20	0,195	20	Valid

Sumber :Data Primer Diolah (2025)

Berdasarkan hasil pengujian, seluruh item pada variabel Perencanaan Backup (X1), Keamanan Backup (X2), Pengujian Pemulihan (X3), dan Ketahanan Infrastruktur ICT (Y) dinyatakan valid. Untuk mahasiswa (N=100), nilai r tabel 0,195 dengan korelasi 0,596–

0,873. Untuk staf ICT (N=10), r tabel 0,632 dengan korelasi 0,677–0,997. Seluruh item memenuhi kriteria validitas dan layak digunakan sebagai instrumen pengumpulan data.

2. Uji Reliabilitas

Uji reliabilitas mengukur konsistensi kuesioner sebagai alat ukur. Instrumen dianggap reliabel jika nilai Cronbach's Alpha > 0,60, artinya respon yang diberikan stabil dan dapat dipercaya untuk penelitian selanjutnya.

Hasil uji reliabilitas penelitian ini di sajikan pada table 2 di bawah ini :

Tabel 2. Hasil Uji Reliabilitas Staff dan Mahasiswa

Variabel	Cronbach's Alpha (Staff ICT)	Cronbach's Alpha (Mahasiswa)	Keterangan
Perencanaan Backup (X1)	0,940	0,926	Reliabel
Keamanan Backup (X2)	0,932	0,941	Reliabel
Pengujian Pemulihan (X3)	0,921	0,910	Reliabel
Ketahanan Infrastruktur ICT (Y)	0,913	0,913	Reliabel

Sumber : Data Primer Diolah (2025)

3. Uji Asumsi Klasik

a. Uji Normalitas

Uji normalitas dilakukan untuk memastikan data berdistribusi normal, sehingga analisis seperti regresi linier dapat diterapkan secara tepat. Pengujian dilakukan dengan dua metode: One-Sample Kolmogorov-Smirnov Test dan P-P Plot.

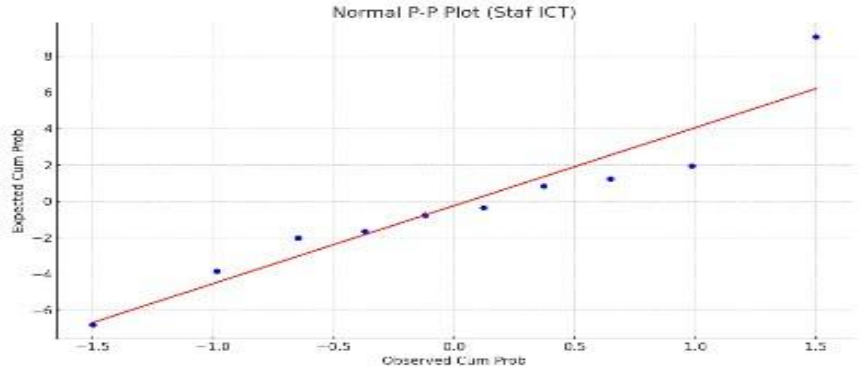
Pengambilan keputusan didasarkan pada nilai signifikansi (Sig.) dari uji Kolmogorov-Smirnov. Jika Sig. > 0,05, data dianggap berdistribusi normal; jika <0,05, data tidak normal. Hasil uji ini memastikan data memenuhi syarat untuk analisis lebih lanjut.

Tabel 3. Hasil Uji Normalitas Staff dan Mahasiswa

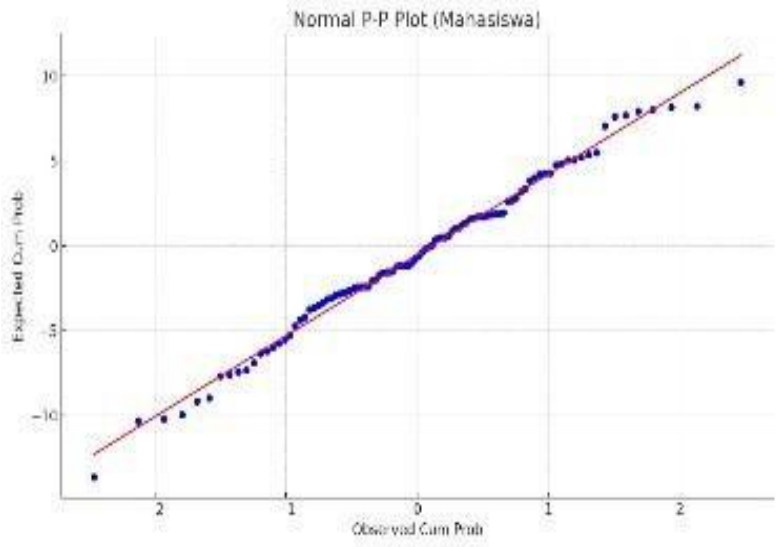
Responden	N	Mean	Std. Deviasi	Nilai Statistik K-S	Sig. (Asymp. 2-tailed)	Distribusi
Staf ICT	10	0	4,788	0,216	0,200	N
Mahasiswa	100	0	5,228	0,060	0,200	N

Sumber : Data Primer Diolah (2025)

Berdasarkan pada tabel di atas, hasil uji normalitas menunjukkan nilai signifikansi (Asymp. Sig. (2-tailed)[c]) sebesar 0,200 yang lebih besar dari 0,05. Oleh karena itu, dapat disimpulkan bahwa residual memiliki distribusi yang normal.



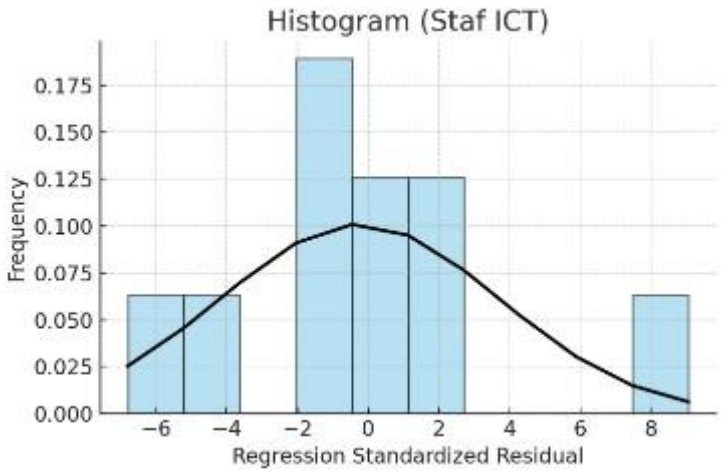
Gambar 1. Hasil Uji Normalitas Staff ICT



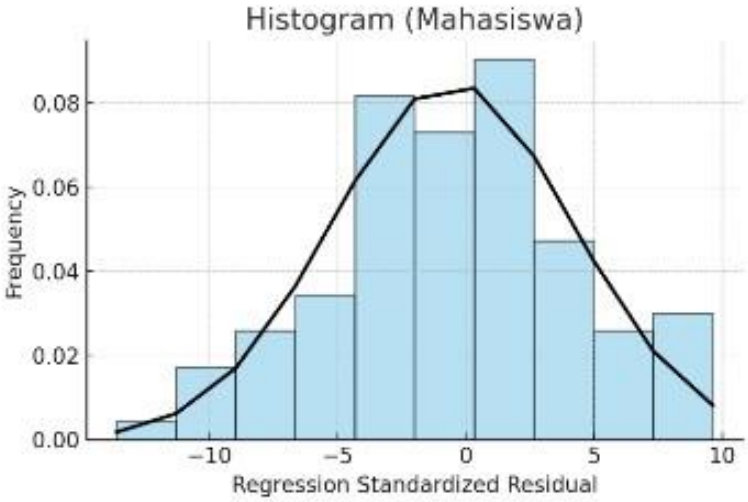
Gambar 2. Hasil Uji Normalitas Mahasiswa

Berdasarkan grafik P-P Plot, titik-titik data mengikuti pola garis diagonal, menunjukkan bahwa residual mendekati distribusi normal. Tidak adanya penyimpangan ekstrem atau outlier mencolok mengindikasikan distribusi data yang wajar dan simetris. Secara visual, hal ini mendukung kesimpulan bahwa data berdistribusi normal.

Distribusi titik-titik data yang mengikuti garis diagonal pada P-P Plot menunjukkan bahwa asumsi normalitas residual terpenuhi, yang merupakan syarat penting dalam analisis regresi linier, ANOVA, dan uji t. Asumsi ini memastikan validitas hasil analisis statistik. Dengan terpenuhinya normalitas secara statistik dan visual, data dalam penelitian ini layak untuk dilanjutkan ke tahap analisis inferensial.



Gambar 3. Grafik Histogram Staff ICT

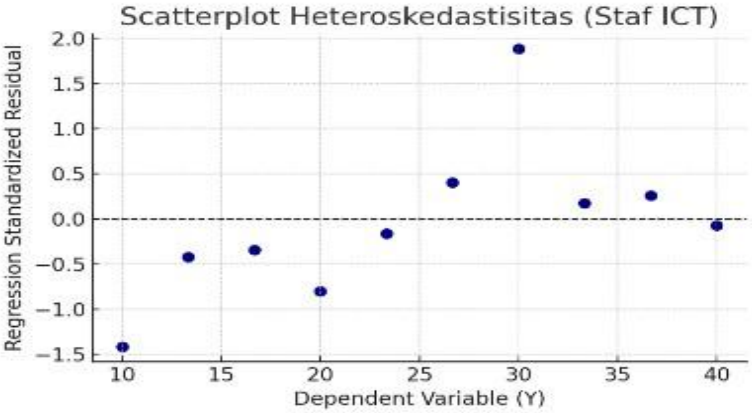


Gambar 4. Grafik Histogram Mahasiswa

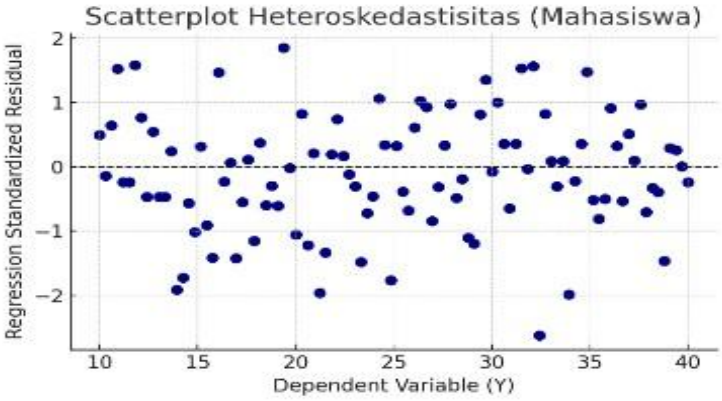
Pola pada gambar grafik histogram diatas seimbang, yang mengindikasikan bahwa model regresi layak untuk digunakan dan memenuhi asumsi normalitas.

b. Uji Heterokedastisitas

Dalam regresi berganda, uji heteroskedastisitas penting untuk memastikan bahwa varian residual antar pengamatan bersifat konstan. Jika varian residual sama, disebut homoskedastisitas; jika bervariasi, disebut heteroskedastisitas. Model regresi yang baik seharusnya menunjukkan homoskedastisitas. Hal ini dapat dilihat melalui scatter plot, di mana sebaran titik yang acak dan tidak membentuk pola tertentu mengindikasikan tidak adanya heteroskedastisitas.



Gambar 5. Hasil Uji Heterokedastisitas Staff ICT



Gambar 6. Hasil Uji Heterokedastisitas Mahasiswa

Berdasarkan scatterplot, titik-titik residual dari kedua kelompok responden tersebar dan data terlihat acak dan merata di sekitar garis horizontal tanpa menunjukkan pola yang jelas. Hal ini menandakan tidak ditemukannya indikasi heteroskedastisitas. Dengan demikian, model regresi telah memenuhi asumsi homoskedastisitas sehingga dapat digunakan untuk analisis selanjutnya.

4. Analisis Regresi Berganda

Analisis ini bertujuan untuk mengidentifikasi seberapa besar pengaruh variabel bebas terhadap variabel terikat(Prasetyo, 2022). Penelitian ini memanfaatkan regresi linier berganda guna mengevaluasi dampak dari perencanaan backup terhadap variabel yang diteliti (X1), keamanan backup (X2), dan pengujian pemulihan (X3) terhadap ketahanan infrastruktur ICT (Y) di UIN Ar-Raniry. Adapun persamaan umum yang digunakan yaitu:

$$Y = a + b_1X_1 + b_2X_2 + b_3X_3 + e \quad (1)$$

Dimana:

- Y = Ketahanan Infrastruktur ICT
- a = Konstanta
- b_1 = Koefisien regresi variabel X1 (Perencanaan Backup)

- b_2 = Koefisien regresi variabel X2 (Keamanan Backup)
- b_3 = Koefisien regresi variabel X3 (Pengujian Pemulihan)
- e = Error (kesalahan residual)

Perhitungan regresi linier berganda dilakukan untuk menguji pengaruh Perencanaan Backup (X_1), Keamanan Backup (X_2), dan Pengujian Pemulihan (X_3) terhadap Ketahanan Infrastruktur ICT (Y). Hasil analisis regresi linier berganda melalui SPSS dalam studi ini ditampilkan pada tabel dibawah ini:

Tabel 4. Hasil Uji Regresi Linier Berganda Staff ICT dan Mahasiswa

Variabel	Staf ICT (Sig.)	Mahasiswa (Sig.)	Variabel
Perencanaan Backup (X1)	0,778	0,226	Perencanaan Backup (X1)
Keamanan Backup (X2)	0,306	0,829	Keamanan Backup (X2)

Sumber : Data Primer Diolah(2025)

Pada analisis regresi linier berganda terhadap seluruh staf ICT UIN Ar-Raniry, diperoleh persamaan: $Y = 7{,}227 - 0{,}217X_1 + 0{,}823X_2 - 0{,}005X_3 + e$. Di mana Y adalah ketahanan infrastruktur ICT, X_1 perencanaan backup, X_2 keamanan backup, dan X_3 pengujian pemulihan. Karena data mencakup seluruh populasi, analisis ini bersifat evaluatif, fokus pada arah dan besar pengaruh, bukan signifikansi statistik.

Berdasarkan hasil regresi, perencanaan backup (X_1) memiliki signifikansi 0,778 dan koefisien -0,217, menunjukkan pengaruh negatif yang tidak signifikan terhadap ketahanan ICT. Keamanan backup (X_2) memiliki signifikansi 0,306 dan koefisien tertinggi sebesar 0,823, menunjukkan bahwa meski belum signifikan, faktor ini dinilai paling berkontribusi oleh staf. Pengujian pemulihan (X_3) tidak dianalisis karena tidak tercantum dalam tabel.

Sementara itu, hasil analisis regresi terhadap 100 mahasiswa menghasilkan persamaan:

$$Y = -0{,}870 + 0{,}233\,X_1 + 0{,}378\,X_2 + 0{,}399\,X_3 + e. \quad (2)$$

Berbeda dengan data staf, data mahasiswa diambil sebagai sampel, sehingga analisis ini mencerminkan persepsi mahasiswa terhadap ketahanan ICT berdasarkan penerapan kontrol backup sesuai ISO 27001:2022.

Tabel menunjukkan bahwa perencanaan backup (X_1) memiliki signifikansi 0,226, cukup berpengaruh meski belum signifikan Keamanan backup (X_2) tidak signifikan (0,829), meskipun pengaruhnya positif. Pengujian pemulihan (X_3), meski tidak ditampilkan, memiliki pengaruh paling besar dalam model mahasiswa dengan koefisien regresi 0,399.

Secara umum, terdapat perbedaan pandangan antara staf dan mahasiswa. Staf menilai keamanan backup sebagai faktor utama dalam ketahanan ICT, sementara mahasiswa lebih menekankan pentingnya perencanaan dan pengujian pemulihan.

Perbedaan ini dapat menjadi masukan penting dalam merancang kebijakan backup informasi yang lebih komprehensif dan sesuai kebutuhan pengguna di lingkungan kampus.

5. Uji Hipotesis

a. Uji t

Melalui uji t, dapat dianalisis kontribusi masing-masing variabel bebas terhadap variabel terikat secara parsial. Jika signifikansi < 0,05 atau t hitung > t tabel, maka berpengaruh signifikan. Jika > 0,05 atau t hitung < t tabel, maka tidak signifikan(Christalisana, 2018). Beberapa tahap pengujian hipotesis sebagai berikut:

Tabel 5. Hasil Uji t Staff ICT dan Mahasiswa

Variabel	Sig. (Staf ICT)	Sig. (Mahasiswa)
Perencanaan Backup (X1)	0,778	0,226
Keamanan Backup (X2)	0,306	0,829
Pengujian Pemulihan (X3)	0,986	0,638

Sumber : Data Primer diolah(2025)

Berdasarkan hasil regresi linier berganda, tidak ada variabel yang berpengaruh signifikan terhadap ketahanan infrastruktur ICT pada staf ICT, karena nilai signifikansi semua variabel di atas 0,05: perencanaan backup (p = 0,778), keamanan backup (p = 0,306), dan pengujian pemulihan (p = 0,986). Artinya, meskipun aspek backup diterapkan, dampaknya belum terasa signifikan menurut persepsi staf.

Berdasarkan hasil uji t pada mahasiswa, ketiga variabel memiliki nilai signifikansi di atas 0,05: perencanaan backup (0,226), keamanan backup (0,829), dan pengujian pemulihan (0,638). Dengan demikian, secara statistik tidak ada variabel yang berpengaruh signifikan terhadap ketahanan ICT menurut persepsi mahasiswa.

b. Uji R^2

Nilai koefisien determinasi (R^2) merefleksikan proporsi variabel dependen yang dapat dijelaskan oleh variabel independen. Semakin mendekati angka 1, maka semakin tinggi tingkat kontribusinya(Soedyafa et al., 2020). Variabel dominan ditentukan dari koefisien regresi tertinggi[13]. SPSS versi 27 digunakan dalam pengujian R^2, hasil dapat dilihat pada tabel berikut :

Tabel 6. Hasil Data Koefisien Determinasi (R^2) staff Ict dan Mahasiswa

Model	R	R Square	Adjusted R Square	Std. Error of Estimate
Staf ICT Mahasiswa	0,658	0,433	0,415	2,342
	0,463	0,214	-0,179	3,619

Sumber : Data Primer Diolah(2025)

Hasil regresi menunjukkan nilai R sebesar 0,658 (mahasiswa) dan 0,463 (staf ICT), menandakan hubungan positif antara X_1, X_2, dan X_3 terhadap Y. Hubungan ini lebih kuat menurut mahasiswa dibanding staf.

Nilai R^2 sebesar 0,433 pada mahasiswa menunjukkan bahwa 43,3% persepsi ketahanan ICT dijelaskan oleh ketiga variabel tersebut. Sedangkan pada staf ICT, R^2 sebesar 0,214 berarti hanya 21,4% variasi ketahanan ICT yang dapat dijelaskan oleh model. Sisanya dipengaruhi faktor lain di luar variabel penelitian.

Pembahasan

Berdasarkan hasil regresi, nilai R 0,658 pada mahasiswa dan 0,463 pada staf ICT menunjukkan hubungan positif antara perencanaan backup (X_1), keamanan backup (X_2), dan pengujian pemulihan (X_3) terhadap ketahanan infrastruktur ICT (Y). Hubungan ini kuat pada mahasiswa dan sedang pada staf, artinya mahasiswa menilai implementasi backup lebih berkontribusi terhadap keandalan sistem dibanding staf ICT.

Nilai R^2 sebesar 0,433 pada mahasiswa berarti 43,3% variasi ketahanan ICT dijelaskan oleh ketiga variabel bebas, sedangkan pada staf ICT hanya 21,4%. Kerena Data staff ICT mencakup seluruh populasi (10 Orang), interpretasi bersifat evaluative, bukan inferensial. Faktor diluar variabel yang di teliti memberikan pengaruh terhadap sisanya.

SIMPULAN

Penelitian ini menunjukkan bahwa praktik backup informasi di ICT UIN Ar-Raniry telah dilakukan secara rutin, namun belum sepenuhnya sesuai dengan standar kontrol A.5.34 ISO 27001:2022. Masih terdapat kekurangan dalam hal dokumentasi, keamanan data cadangan, dan pengujian pemulihan. Dari hasil analisis, staf ICT menilai keamanan backup paling penting, sedangkan mahasiswa lebih menekankan perencanaan dan pengujian pemulihan. Persepsi mahasiswa menjelaskan ketahanan ICT lebih baik (43,3%) dibanding staf (21,4%). Meski ISO belum diterapkan formal, kontrol A.5.34 terbukti relevan. Disarankan institusi menyusun SOP backup, rutin uji pemulihan, dan mulai integrasikan prinsip ISO 27001:2022 untuk memperkuat ketahanan terhadap serangan siber seperti ransomware.

DAFTAR PUSTAKA

Aziz, A. S. (2021). Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius Design And Security Analysis On Freeradius Centralized Authentication System. Journal of Informatics and …, 7(2), 106–112. http://www.jurnal.uui.ac.id/index.php/jics/article/view/1744

Fauzia Anis Sekar Ningrum, Yudha Riwanto, Inggrid Yanuar Risca Pratiwi, & Muhammad Ainul Fikri. (2024). Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI. Jurnal Informatika Polinema, 10(3), 437–444. https://doi.org/10.33795/jip.v10i3.5154

Janah, M., & Kartini, A. Y. (2022). Penerapan Metode Regresi Linier Berganda Pada Kasus Balita Gizi Buruk Di Kabupaten Bojonegoro. Jurnal Statistika Dan Komputasi, 1(2), 74–82. https://doi.org/10.32665/statkom.v1i2.1170

Jelita, L. D. A., Al Azam, M. N., & Nugroho, A. (2024). Evaluasi Keamanan Teknologi Informasi

Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022. Jurnal SAINTEKOM, 14(1), 84–94. https://doi.org/10.33020/saintekom.v14i1.623

Prasetyo, H., Ibrahim, I., Milhan Hijrah Moelyana, M., & Muhammad Abid, Z. (2024). Keamanan Cyber dalam Menghadapi Tantangan Ancaman Masa Depan di Universitas Bhayangkara Jakarta Raya. Journal of Information and Information Security (JIFORTY), 5(2), 235–244. http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Tuga, M. A., & Aziz, A. (2019). Analisis Manajemen Keamanan Sistem Informasi Akademik Universitas Kanjuruhan Malang Menggunakan Standar Iso 27001: 2013. Semnas SENASTEK Unikama 2019, 2, 764–771. https://conference.unikama.ac.id/artikel/index.php/senastek/article/view/257

April, S. (2025). *Systematic Literature Review : Implementasi Iso / Iec 27001 Dalam Penguatan Keamanan Informasi Di Indonesia Systematic Literature Review : Implementation of ISO / IEC 27001 in Strengthening Information Security in Indonesia*. 196–201.

Christalisana, C. (2018). Pengaruh Pengalaman Dan Karakter Sumber Daya Manusia Konsultan Manajemen Konstruksi Terhadap Kualitas Pekerjaan Pada Proyek Di Kabupaten Pandeglang. *Jurnal Fondasi*, *7*(1), 87–98. https://doi.org/10.36055/jft.v7i1.3305

Meilani, L., Suroso, A. I., & Yuliati, L. N. (2020). Evaluasi Keberhasilan Sistem Informasi Akademik dengan Pendekatan Model DeLone dan McLean. *Jurnal Sistem Informasi Bisnis*, *10*(2), 137–144. https://doi.org/10.21456/vol10iss2pp137-144

Prasetyo, R. A. (2022). Analisis Regresi Linear Berganda Untuk Melihat Faktor Yang Berpengaruh Terhadap Kemiskinan di Provinsi Sumatera Barat. *Journal of Mathematics UNP*, *7*(2), 62. https://doi.org/10.24036/unpjomath.v7i2.12777

Soedyafa, D. A., Rochmawati, L., & Sonhaji, I. (2020). Koefisien Korelasi (R) Dan Koefisien Determinasi (R2). *Jurnal Penelitian Politeknik Penerbangan Surabaya Edisi XXX*, *5*(4), 289–296.