MANAJEMEN RISIKO PENGGUNAAN TEKNOLOGI *NETWORK ATTACHED STORAGE* (NAS) PADA PT SIGMA ENERGY COMPRESSINDO TBK MENGGUNAKAN PENDEKATAN *RISK ASSESSMENT*

RIFQI NANDI HARIANSYAH

NIM 2105421090

Skripsi yang Ditulis untuk Memenuhi Sebagian Persyaratan untuk Memperoleh Gelar Sarjana Sain Terapan

PROGRAM STUDI ADMINISTRASI BISNIS TERAPAN

JURUSAN ADMINISTRASI NIAGA

POLITEKNIK NEGERI JAKARTA

2025

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah mendorong perusahaan untuk mengelola dan menyimpan data dalam jumlah besar secara efisien dan aman. Salah satu teknologi penyimpanan data yang banyak digunakan adalah *Network Attached Storage* (NAS), yang memungkinkan penyimpanan terpusat dan akses data melalui jaringan. NAS memiliki keunggulan dalam hal skalabilitas, efisiensi biaya, dan kemudahan pengelolaan dibandingkan sistem penyimpanan tradisional (Affandi, 2022).

Namun, pelaksanaan NAS juga memiliki resiko yang substansial, terutama dari segi keamanan data. Ancaman seperti serangan siber, *malware*, dan akses tidak sah dapat menyebabkan pelanggaran data, kerusakan sistem, dan gangguan operasi. Selain itu, NAS akan menjadi titik terkuat kegagalan di jaringan sehingga apabila terjadi kerusakan maka seluruhnya

Manajemen risiko adalah sistematis proses dalam mengevaluasi, mengidentifikasi dan mengendalikan risiko yang mungkin berdampak terhadap pencapaian tujuan perusahaan (Hopkin, 2018). Dalam konteks keseluruhan proyek NAS, manajemen risiko terlibat dari penilaian terhadap beragam ancaman keamanan, kerentanan teknikal, juga potensi gangguan operasional yang mungkin mempengaruhi integritas dan ketersediaan data perusahaan. Dengan menggunakan pendekatan risk assessment, perusahaan dapat menentukan tingkat kemungkinan dan dampak dari risiko yang dihadapi dan kemudian mengembangkan Identifikasi risiko atas penggunaan NAS melibatkan beragam hal seperti risiko kegagalan perangkat keras, serangan siber, kerugian data akibat kesalahan manusia, atau bahkan musibah alam yang mempengaruhi sistem fisiknya. Analisis risiko untuk memahami tingkat kemungkinan munculnya peristiwa tersebut dan skala pengaruhnya terhadap operasional perusahaan.

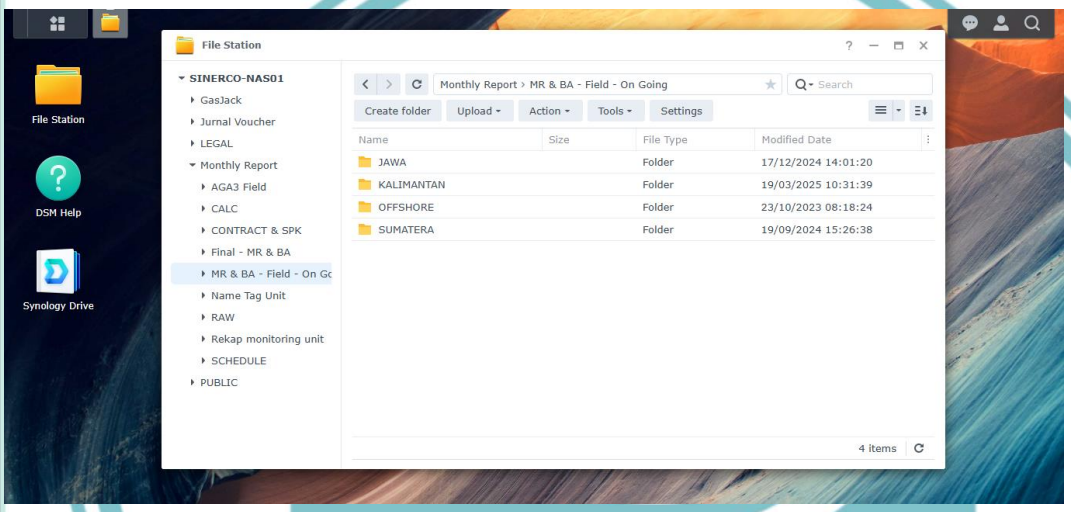
Selanjunya, evaluasi risiko membiarkan perusahaan menentukan prioritas penanganan atas kriteria tingkat risiko yang diterima atau ditolaknya. Pengendalian risiko dapat dilakukan melalui beraneka seperti menerapkan enkripsi data, membangun sistem redundansi, menyiapkan backup berkala, serta memperkuat mekanisme otorisasi dan sentralisasi pengguna (Disterer, 2013). Sementara itu, monitoring risiko secara berkala diperlukan untuk memastikan bahwa tindakan pengendalian yang telah diimplementasikan tetap efektif di tengah perubahan kondisi teknologi dan lingkungan eksternal.

PT Sigma Energy Compressindo Tbk, yang merupakan perusahaan yang beroperasi di sektor energi, memerlukan data untuk memperkuat atas kegiatan operasional, perawatan, serta pelaporan finansial dan teknisnya. Alasannya karena perusahaan tersebut mengandalkan teknologi informasi untuk menunjang operasionalnya yang rumit, di antaranya menggunakan NAS untuk menyimpan dan mengelola data. Implementasi teknologi NAS diharapannya akan menjadi solusi memperbaiki keefisiennya pengelolaan data di PT Sigma Energy Compressindo Tbk.

Implementasi teknologi NAS diharapkan dapat menjadi solusi dalam meningkatkan efisiensi pengelolaan data di PT Sigma Energy Compressindo Tbk. NAS memungkinkan akses data yang lebih cepat, keamanan yang lebih baik, serta kemudahan dalam pencadangan dan pemulihan data. Dengan adanya sistem NAS, data operasional dapat dikelola secara terpusat, sehingga memudahkan tim dalam mengakses dan memperbarui data secara real-time. Namun, penerapan teknologi ini juga memiliki tantangan, seperti biaya implementasi, kebutuhan akan pelatihan bagi karyawan, serta integrasi dengan sistem yang sudah ada.

Dengan sistem ini, *file* data terkait performa unit dapat disimpan secara *online* dalam satu lokasi terpusat yang mudah diakses oleh seluruh tim yang membutuhkan, baik di kantor pusat maupun di lapangan. NAS memungkinkan data dari lapangan, seperti laporan harian, parameter teknis, dan catatan operasional, untuk diunggah secara langsung dan *real-time*, sehingga mengurangi risiko kehilangan data atau keterlambatan dalam penyampaian informasi.

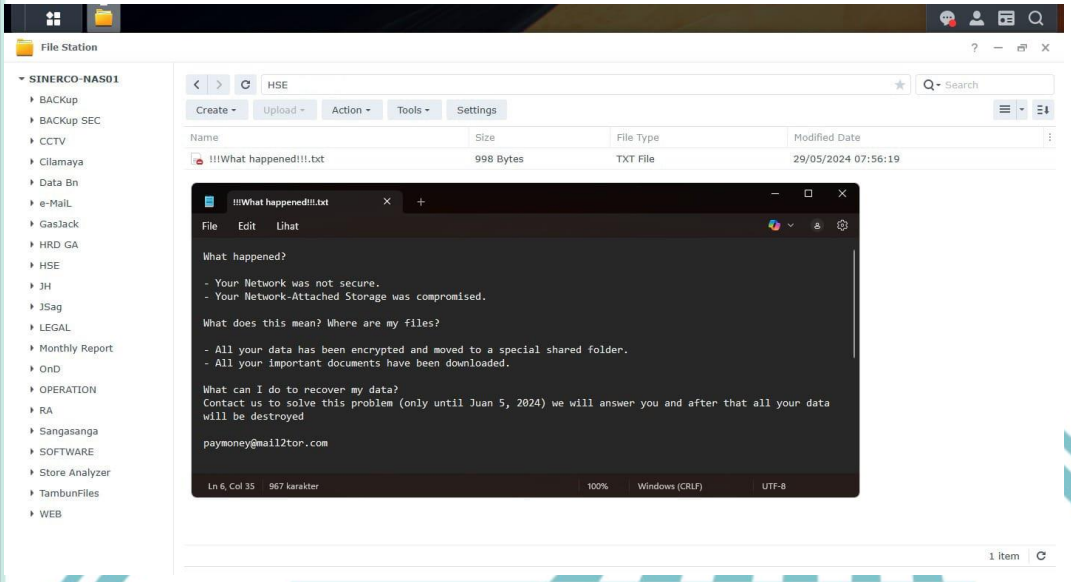
Selain itu, penggunaan *private cloud* meningkatkan efisiensi kerja karena akses ke *file* menjadi lebih cepat dan fleksibel, tanpa harus bergantung pada metode transfer data manual seperti penggunaan perangkat eksternal. Hal ini juga mendukung pengambilan keputusan yang lebih cepat dan akurat oleh manajemen, karena data-data penting mengenai performa unit selalu tersedia kapan pun dibutuhkan.



Gambar 1.1 Contoh File Unit di Lapangan
Sumber: Data diolah, 2025

Berdasarkan gambar 1.1 keamanan data pun lebih terjamin dengan adanya kontrol akses yang dapat disesuaikan berdasarkan kebutuhan setiap pengguna. Dengan demikian, adopsi teknologi *private cloud* berupa NAS ini tidak hanya membantu memudahkan pengelolaan dan pertukaran data, tetapi juga memperkuat efektivitas monitoring performa unit, mendukung efisiensi operasional, dan meningkatkan kemampuan perusahaan untuk merespon perubahan kondisi lapangan secara cepat dan tepat

Namun, dengan meningkatnya ketergantungan pada teknologi ini, perusahaan juga menghadapi risiko yang terkait dengan keamanan dan keandalan sistem penyimpanan data.



Gambar 1.2 Kasus Terkena Ancaman *Malware* di Departemen HSE
Sumber: Data diolah, 2025

Berdasarkan gambar 1.2 terjadi insiden serius yang berdampak langsung terhadap sistem penyimpanan data di Departemen *Health, Safety, and Environment* (HSE) PT Sigma Energy Compressindo Tbk. Berdasarkan tangkapan layar dari sistem NAS, ditemukan sebuah file bernama *"!!!What happened!!!.txt"* yang berisi pesan bahwa sistem telah disusupi oleh *ransomware*. Dalam pesan tersebut dinyatakan bahwa jaringan perusahaan tidak aman dan NAS telah berhasil diretas. Seluruh data penting telah dienkripsi dan dipindahkan ke folder khusus, serta dokumen-dokumen penting telah diunduh oleh pihak yang tidak bertanggung jawab. Pelaku menuntut komunikasi melalui email anonim, dengan ancaman bahwa data akan dihancurkan jika tidak ada tanggapan sebelum batas waktu yang ditentukan. Insiden ini menunjukkan bahwa sistem keamanan data perusahaan perlu dievaluasi dan diperkuat secara menyeluruh. Diperlukan respons cepat dan terkoordinasi dari tim IT, manajemen risiko, dan seluruh pihak terkait untuk memitigasi dampak, memulihkan sistem, serta melakukan investigasi guna mengidentifikasi sumber dan metode serangan. Dengan melakukan analisis manajemen risiko secara komprehensif, PT Sigma Energy Compressindo Tbk dapat memahami potensi ancaman dan merancang strategi mitigasi yang tepat, sehingga

implementasi teknologi NAS dapat tetap mendukung keamanan informasi dan tujuan operasional perusahaan secara optimal.

Oleh karena itu, diperlukan analisis manajemen risiko yang komprehensif untuk mengidentifikasi, menilai, dan mengelola risiko yang mungkin timbul dari penggunaan NAS di lingkungan PT Sigma Energy Compressindo Tbk. Pendekatan *risk assessment* dapat membantu perusahaan dalam memahami potensi ancaman, kerentanan, dan dampak dari risiko yang dihadapi, serta merancang strategi mitigasi yang efektif. Dengan demikian, PT Sigma Energy Compressindo Tbk dapat memastikan bahwa penggunaan teknologi NAS mendukung tujuan operasional dan keamanan informasi perusahaan secara optimal.

Berdasarkan penjelasan dan permasalahan yang penulis jelaskan di atas, penulis tertarik membahas permasalahan tersebut dalam skripsi dengan judul ***"Analisis Manajemen Risiko Penggunaan Teknologi Network Attached Storage (NAS) Pada PT Sigma Energy Compressindo Tbk Menggunakan Pendekatan Risk Assessment"***

1.2 Identifikasi Masalah

Adapun identifikasi masalah dalam penelitian ini yang sesuai dengan penjabaran dari latar belakang di atas adalah sebagai berikut:

a. Implementasi NAS membawa manfaat namun juga menimbulkan potensi risiko seperti serangan siber, *malware*, dan kegagalan sistem.
b. Kurangnya pemahaman menyeluruh mengenai potensi ancaman dan kerentanan yang dapat terjadi pada sistem NAS di lingkungan PT Sigma Energy Compressindo Tbk.
c. Belum adanya analisis risiko secara komprehensif yang digunakan untuk mengidentifikasi dan mengelola risiko dari penggunaan NAS.
d. Perlu adanya pendekatan sistematis melalui risk assessment untuk menjamin keamanan dan keandalan data perusahaan.

1.3 Rumusan Masalah

Berdasarkan identifikasi permasalahan dan pembatasan masalah di atas, penulis merumuskan masalah sebagai berikut:

1. Apa saja risiko yang timbul dari penggunaan teknologi NAS di PT Sigma Energy Compressindo Tbk?
2. Bagaimana cara mengidentifikasi, mengalisis dan menilai risiko tersebut dengan pendekatan risk assessment?
3. Strategi mitigasi apa yang dapat diterapkan untuk mengurangi dampak risiko dari penggunaan NAS?

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Mengidentifikasi potensi risiko yang terkait dengan penggunaan teknologi NAS di PT Sigma Energy Compressindo Tbk.
b. Menilai tingkat ancaman, kerentanan, dan dampak dari risiko yang dihadapi melalui pendekatan risk assessment.
c. Memberikan rekomendasi strategi mitigasi risiko guna meningkatkan keamanan dan keandalan sistem penyimpanan data perusahaan.

1.5 Manfaat Penelitian

Adapun manfaat yang diharapkan oleh penulis dalam penelitian ini adalah sebagai berikut:

a. Manfaat Teoritis

1) Penelitian ini diharapkan dapat memberikan manfaat teoritis berupa penambahan wawasan dan literatur akademik di bidang manajemen risiko teknologi informasi, khususnya yang berkaitan dengan penggunaan teknologi NAS.
2) Penelitian ini juga memberikan kontribusi teoritis dalam penerapan pendekatan risk assessment sebagai metode analisis yang sistematis untuk mengidentifikasi, menilai, dan mengelola risiko pada sistem penyimpanan data berbasis jaringan.

3) Hasil penelitian ini dapat menjadi referensi akademik bagi penelitian selanjutnya yang membahas topik serupa.
4) Penelitian ini turut memperkaya pemahaman mengenai pengelolaan risiko teknologi informasi dalam konteks dunia industri.

b. Manfaat Praktis

1) Penelitian ini diharapkan memberikan manfaat praktis bagi perusahaan, terutama dalam meningkatkan keamanan data dan stabilitas operasional melalui penerapan strategi mitigasi risiko yang tepat.
2) Analisis manajemen risiko terhadap penggunaan teknologi NAS memungkinkan perusahaan untuk memahami potensi ancaman dan kerentanan yang ada.
3) Dengan pemahaman tersebut, perusahaan dapat mengambil langkah-langkah preventif dan korektif yang sesuai untuk mengurangi risiko.
4) Strategi mitigasi yang dihasilkan dari penelitian ini dapat dijadikan pedoman dalam perencanaan dan pengelolaan sistem penyimpanan data perusahaan.
5) Hal ini bertujuan untuk memastikan kontinuitas operasional serta perlindungan terhadap informasi penting perusahaan.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan terhadap analisis manajemen risiko penggunaan NAS dengan pendekatan *Risk Assesment* dapat ditarik kesimpulan yaitu:

a. Risiko yang Timbul dari Penggunaan Teknologi NAS di PT Sigma Energy Compressindo Tbk

   Penggunaan NAS di PT Sigma Energy Compressindo Tbk memiliki beberapa risiko yang perlu diperhatikan, seperti gangguan koneksi internet dan listrik yang dapat menghambat akses serta sinkronisasi data. Selain itu, ancaman dari *malware*, kegagalan perangkat keras, serangan siber, dan kesalahan manusia *(human error)* juga berpotensi mengganggu keamanan dan kelangsungan operasional data perusahaan. Oleh karena itu, diperlukan langkah mitigasi seperti penggunaan perangkat pendukung (UPS), pembaruan sistem secara berkala, pencadangan data, serta peningkatan pemahaman dan kewaspadaan pengguna dalam mengelola sistem NAS.

b. Identifkasi dan analisis risiko

   Risiko yang terjadi pada penerapan NAS di PT. Sigma Energy Compressindo Tbk yaitu ketergantungan listrik dan internet, ancaman keamanan seperti *malware* dan virus serta akses tidak sah dari pihak eksternal, dan risiko kerusakan perangkat keras. Risiko ini diidentifikasi dari diskusi internal berdasarkan fakta di lapangan dan pengalaman penggunaan. Risiko yang dianggap paling bahaya adalah akses tidak sah dari pihak eksternal karena berpotensi penyalahgunaan data sebagai aset perusahaan. Kemudian disusul dengan *malware* dan virus.

c. Evaluasi dan Mitigasi Risiko

   Setiap risiko memiliki tingkat risiko yang berbeda beda. Evaluasi risiko dilakukan sebagai dasar penyusunan strategi mitigasi. Risiko yang berada pada tingkat tinggi memiliki mitigasi yaitu melakukan pembaharuan

sistem untuk menjaga keamana data. Risiko pada tingkat sedang dilakukan mitigasi dengan melakukan pemantauan dan himbauan secara berkala untuk mematuhi alur penggunaan NAS. Untuk risiko pada tingkat rendah hanya dilakukan mitigasi dengan melakukan *back up* melalui NAS.

5.2 Saran

Berdasarkan hasil penelitian yang disimpulkan maka terdapat beberapa saran sebagai berikut:

a. Untuk Perusahaan
   1) Perusahaan perlu untuk membentuk tim IT khusus untuk membantu melaksanakan operasional NAS.
   2) Mempelajari NAS lebih dalam untuk mengetahui fitur yang dapat menjadi monitor sebagai pemantauan dan pencatatan aktivitas pengguna secara *real time* untuk memastikan tidak ada penyimpangan dan kesesuaian dengan prosedur penggunaan NAS.
   3) Perusahaan perlu untuk melakukan pemeliharaan dan perawatan berkala pada perangkat untuk memimalisir risiko kerusakan perangkat keras

a. Untuk Industri Sejenis
   1) Industri sejenis perlu untuk melakukan adopsi NAS secara bertahap agar seluruh elemen siap.
   2) Industri sejenis disarankan untuk melakukan pemetaan risiko penggunaan NAS untuk meminimalisir risiko.
   3) Industri sejenis yang menggunakan NAS disarankan untuk berbagi pengalaman dalam pengelolaan NAS.

b. Untuk Penelitian Selanjutnya
   1) Penelitian mendatang disarankan untuk lebih fokus pada aspek keamanan siber dalam penggunaan NAS, seperti analisis terhadap potensi serangan *ransomware*, *data breach*, dan efektivitas sistem enkripsi.

2) Penellitian selanjutnya dapat dilakukan studi perbandingan NAS dengan sistem penyimpanan lain seperti *cloud* untuk menilai efektivitas dan risiko penggunaannya