JPM Jurnal Prima Manajemen
E-ISSN : 3123-7266

Strategi Mitigasi Risiko *End of Support* Perangkat Jaringan pada *Data Center* Bank XYZ

Naufalarizqa Ramadha Meisa Putra
Teknik Informatika, Fakultas Teknik, Universitas Satya Negara Indonesia,
Jakarta, Indonesia
naufalarizqa@usni.ac.id

Abstract
End of Support (EoS) is a critical phase in the lifecycle of information technology infrastructure that may significantly increase operational, security, and compliance risks if not properly managed. In the banking industry, particularly in sharia banking institutions with high availability requirements, the sustainability of Data Center (DC) and disaster recovery center (DRC) network devices is crucial to ensuring uninterrupted services. This study aims to analyze the management strategy for End of Support network devices in the DC and DRC environments of Bank XYZ. The research applies a qualitative descriptive method based on internal assessment documents, asset inventory analysis, and action plan evaluation. The results show that 47 network devices in the DC and DRC environments have reached End of Support status, requiring immediate renewal to mitigate cybersecurity and operational risks. The action plan involves device identification, feasibility assessment, hardware refreshment, migration Timeline arrangement, and risk mitigation through privilege access management and continuous monitoring. This study highlights the importance of proactive asset lifecycle management as part of IT governance to maintain operational resilience and regulatory compliance in the banking sector.
Keywords: *End of Support; IT Asset Management; Data Center; Risk Management.*

Abstrak
End of Support (*EoS*) merupakan fase kritis dalam siklus hidup infrastruktur teknologi informasi yang berpotensi menimbulkan risiko operasional, keamanan, dan kepatuhan apabila tidak dikelola secara tepat. Dalam industri perbankan yang menuntut ketersediaan layanan tinggi, keberlanjutan perangkat jaringan di *Data Center* (*DC*) dan *Disaster Recovery Center* (*DRC*) menjadi faktor krusial dalam menjaga stabilitas layanan. Penelitian ini bertujuan untuk menganalisis strategi manajemen perangkat jaringan yang telah memasuki masa *End of Support* di lingkungan *DC* dan *DRC* Bank XYZ. Metode penelitian yang digunakan adalah kualitatif deskriptif dengan pendekatan studi kasus, berdasarkan analisis dokumen internal, inventaris aset teknologi informasi, serta evaluasi rencana tindak lanjut. Hasil kajian menunjukkan bahwa terdapat 47 perangkat jaringan *DC* dan *DRC* yang telah mencapai status *End of Support* dan memerlukan peremajaan untuk memitigasi risiko keamanan siber dan gangguan operasional. Strategi pengelolaan dilakukan melalui identifikasi aset, penilaian kelayakan, pembaruan perangkat, penyusunan *Timeline* migrasi, serta penerapan mitigasi risiko melalui *privileged access management* dan monitoring berkala. Penelitian ini menegaskan pentingnya pengelolaan siklus hidup aset TI secara proaktif sebagai bagian dari tata kelola teknologi informasi untuk menjaga keberlangsungan operasional dan kepatuhan regulasi di sektor perbankan.
Kata Kunci: *End of Support*; Manajemen Aset TI; *Data Center*; Manajemen Risiko.

Article info
Received 20 Januari 2026
Revised 25 Januari 2026
Accepted 30 Januari 2026
Available Online 1 Februari 2026
naufalarizqa@usni.ac.id

1. PENDAHULUAN

Transformasi digital dalam industri perbankan menuntut ketersediaan infrastruktur teknologi informasi (TI) yang andal, aman, dan berkesinambungan. Bank XYZ sebagai salah satu bank terbesar di Indonesia memiliki ketergantungan yang tinggi terhadap perangkat jaringan dalam mendukung operasional layanan perbankan berbasis teknologi. *Data Center* (*DC*) dan *Disaster Recovery Center* (*DRC*) berfungsi sebagai pusat utama pengolahan dan pemulihan data yang harus memiliki tingkat reliabilitas dan keamanan yang tinggi.

Salah satu tantangan utama dalam pengelolaan infrastruktur TI adalah perangkat jaringan yang telah memasuki fase *End of Support* (*EoS*). *EoS* menandakan berakhirnya dukungan resmi dari *vendor*, termasuk pembaruan keamanan dan dukungan teknis. Kondisi ini berpotensi meningkatkan risiko kerentanan keamanan, ketidakpatuhan terhadap regulasi, serta gangguan operasional yang dapat berdampak pada layanan perbankan.

Berdasarkan ketentuan Otoritas Jasa Keuangan (OJK) dan hasil audit internal, bank diwajibkan untuk melakukan identifikasi dan pengelolaan perangkat TI yang telah atau akan memasuki masa *EoS*. Data aset teknologi informasi periode Agustus 2024 menunjukkan terdapat 47 perangkat jaringan di lingkungan *DC* dan *DRC* Bank XYZ yang telah berstatus *End of Support*. Kondisi ini menuntut adanya strategi manajemen yang terstruktur dan terukur dalam rangka menjaga keberlangsungan operasional dan meminimalkan risiko.

Penelitian ini bertujuan untuk mengkaji strategi manajemen perangkat jaringan *End of Support* di lingkungan *DC* dan *DRC* pada Bank XYZ, dengan fokus pada perencanaan peremajaan perangkat, mitigasi risiko, serta implikasinya terhadap tata kelola TI. Kajian ini diharapkan dapat memberikan kontribusi praktis bagi pengelolaan aset TI di sektor perbankan serta menjadi referensi akademik dalam bidang manajemen teknologi informasi.

2. KAJIAN TEORI

2.1 *End of Support* dalam Siklus Hidup Aset TI

End of Support merupakan tahap akhir dalam siklus hidup produk teknologi informasi di mana *vendor* tidak lagi menyediakan dukungan teknis, pembaruan perangkat lunak, maupun *patch* keamanan. Dalam konteks manajemen aset TI, fase *EoS* menjadi indikator penting untuk melakukan evaluasi kelayakan dan perencanaan pembaruan infrastruktur.

2.2 Manajemen Risiko Infrastruktur Jaringan

Manajemen risiko infrastruktur jaringan mencakup identifikasi, analisis, dan mitigasi risiko yang timbul akibat keterbatasan teknologi, ancaman keamanan, maupun kegagalan operasional. Perangkat jaringan yang telah *EoS* memiliki tingkat risiko yang lebih tinggi karena tidak lagi memperoleh pembaruan keamanan, sehingga rentan terhadap serangan siber.

2.3 Tata Kelola Teknologi Informasi di Perbankan

End of Support merupakan tahap akhir dalam siklus hidup produk teknologi informasi di mana *vendor* tidak lagi menyediakan dukungan teknis, pembaruan perangkat lunak, maupun *patch* keamanan. Dalam konteks manajemen aset TI, fase *EoS* menjadi indikator penting untuk melakukan evaluasi kelayakan dan perencanaan pembaruan infrastruktur.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi kasus. Data dikumpulkan melalui analisis dokumen internal terkait Kajian *End of Support* Perangkat Jaringan Bank XYZ, inventaris aset teknologi informasi, serta rencana tindakan (*action plan*) yang telah disusun oleh unit terkait. Dokumen tersebut memuat informasi teknis seperti jenis perangkat, usia penggunaan, status dukungan pabrikan, *lifecycle*, serta risiko operasional dan keamanan yang terkait dengan status *End of Support*.

Teknik analisis data dilakukan dengan cara mengelompokkan dan membandingkan informasi berdasarkan kategori perangkat (misalnya *router, switch, firewall, dan load balancer*), lokasi operasional (*DC* dan *DRC*), status *End of Support* (*EoS*, *End of Life*, atau masih dalam dukungan), serta strategi tindak lanjut yang telah direncanakan. Pengelompokan ini memberikan gambaran sistematis mengenai prioritas penggantian perangkat, urgensi risiko, hingga kesiapan organisasi dalam melakukan peremajaan infrastruktur.

Pendekatan kualitatif deskriptif memungkinkan peneliti untuk memahami secara mendalam dinamika pengelolaan perangkat jaringan *EoS* dalam konteks operasional perbankan yang menuntut ketersediaan layanan tinggi, ketahanan operasional, serta kepatuhan terhadap regulasi industri keuangan. Selain itu, pendekatan ini membantu mengidentifikasi faktor-faktor non-teknis seperti keterbatasan anggaran, jadwal implementasi, dan koordinasi antar unit sebagai bagian dari strategi tata kelola teknologi informasi.

4. HASIL DAN PEMBAHASAN

4.1 Identifikasi Perangkat Jaringan *End of Support*

Hasil identifikasi aset teknologi informasi menunjukkan bahwa hingga periode Agustus 2024 terdapat 47 perangkat jaringan yang telah memasuki masa *End of Support* (*EoS*) dan masih digunakan pada lingkungan *Data Center* (*DC*) serta *Disaster Recovery Center* (*DRC*). Perangkat-perangkat tersebut terdiri atas *switch, router, serta hardware management console*, yang berperan penting dalam mendukung konektivitas layanan perbankan Bank XYZ.

Distribusi perangkat *EoS* tidak hanya terkonsentrasi pada satu fungsi tertentu, melainkan tersebar pada berbagai lapisan layanan kritikal, mulai dari layanan *web*, aplikasi, basis data, layanan internal, hingga konektivitas eksternal. Kondisi ini menunjukkan bahwa isu *EoS* bukan hanya persoalan aset usang, tetapi berpotensi berdampak langsung terhadap keandalan operasional dan kontinuitas bisnis bank.

Tabel 4.1 Distribusi Perangkat Jaringan *End of Support* berdasarkan Lokasi

Lokasi	Jumlah Perangkat	Persentase
Data Center (DC)	1	49%
Disaster Recovery Center (*DRC*)	2	51%
Total	47	100%

Sumber: (Bank XYZ, 2024)

Berdasarkan Tabel 4.1, terlihat bahwa jumlah perangkat *EoS* di *DC* dan *DRC* relatif seimbang. Hal ini menunjukkan bahwa risiko yang timbul akibat perangkat *EoS* bersifat simetris antara pusat data utama dan pusat pemulihan bencana, sehingga membutuhkan pendekatan pengelolaan yang terintegrasi dan berkelanjutan.

Tabel 4.2 Klasifikasi Perangkat *End of Support* berdasarkan Jenis

Jenis Perangkat	Jumlah	Persentase
Switch	43	91%
Router	1	2%
Hardware Management Console	3	7%
Total	47	100%

Sumber: (Bank XYZ, 2024)

Mayoritas perangkat *EoS* merupakan *switch* jaringan, yang berfungsi sebagai tulang punggung komunikasi data antar sistem. Tingginya proporsi *switch EoS* mengindikasikan meningkatnya risiko gangguan layanan apabila tidak segera dilakukan peremajaan perangkat secara sistematis.

4.2 Strategi Peremajaan dan *Evergreen*

Strategi utama yang diterapkan dalam pengelolaan perangkat jaringan *End of Support* adalah *evergreen strategy*, yaitu proses peremajaan infrastruktur dengan mengganti perangkat lama menggunakan perangkat baru yang masih mendapatkan dukungan *vendor* baik dari sisi teknis maupun keamanan. Peremajaan tidak dilakukan secara serentak, melainkan melalui pendekatan bertahap (*phased migration*) guna menjaga stabilitas layanan perbankan yang bersifat *mission critical*. Dalam praktiknya, perangkat baru telah dipersiapkan dan diaktifkan terlebih dahulu, sementara perangkat lama masih difungsikan sebagai *fallback* hingga proses migrasi dinyatakan stabil.

Tabel 4.3 Ringkasan Strategi *Evergreen* Perangkat Jaringan

Aspek	Implementasi
Pendekatan	*Evergreen / Refreshment*
Prinsip	Bertahap dan *minim downtime*
Fokus	Keberlangsungan operasional
Perangkat Lama	Digunakan sebagai cadangan sementara
Perangkat Baru	Seri terkini dan masih *supported*

Sumber: (Bank XYZ, 2024)

Berdasarkan Tabel 4.3, terlihat bahwa strategi ini mencerminkan penerapan prinsip manajemen risiko dan tata kelola TI, di mana keputusan teknis selalu dikaitkan dengan dampak bisnis dan reputasi institusi perbankan.

4.3 *Timeline* Migrasi dan Implementasi

Proses peremajaan perangkat jaringan dilaksanakan melalui tahapan yang terstruktur mulai dari pengadaan perangkat, pengiriman, instalasi dan konfigurasi, hingga migrasi logikal jaringan. Seluruh tahapan disusun dalam *Timeline* jangka menengah dan panjang guna memastikan kesiapan sumber daya serta koordinasi lintas unit kerja. Setiap fase juga dilengkapi dengan standar keberhasilan, mekanisme *fallback*, serta prosedur komunikasi agar proses transisi dapat dilakukan secara aman tanpa mengganggu layanan operasional yang bersifat *mission critical*.

Tabel 4.4 *Timeline* Implementasi Peremajaan Perangkat Jaringan

Tahapan	Periode	Status
Pengadaan Perangkat	Oktober 2023	Selesai
Pengiriman Perangkat	November 2023	Selesai
Instalasi & Konfigurasi Fase 1	Juni 2024	Selesai
Readiness Cabling DC–DRC	Desember 2026	*On Progress*
Migrasi Logikal & *Testing*	Maret 2027	*On Progress*
Dismantle Perangkat Lama *EoS*	Juni 2027	*On Progress*

Sumber: (Bank XYZ, 2024)

Timeline yang direncanakan hingga tahun 2027 menunjukkan bahwa pengelolaan *EoS* diposisikan sebagai inisiatif strategis jangka panjang, bukan sekadar tindakan reaktif terhadap temuan audit. Pendekatan ini memberikan ruang mitigasi apabila terjadi kendala teknis maupun operasional selama proses migrasi berlangsung.

4.4 Mitigasi Risikio

Selama masa transisi, perangkat jaringan yang telah berstatus *End of Support* namun masih digunakan berpotensi menimbulkan risiko keamanan siber dan operasional. Oleh karena itu, bank menerapkan beberapa langkah mitigasi untuk menekan risiko tersebut hingga seluruh proses migrasi selesai.

Tabel 4.5 Langkah Mitigasi Risiko Perangkat *EoS*

Risiko	Strategi Mitigasi
Kerentanan keamanan	Monitoring berkala aktivitas jaringan
Akses tidak sah	Implementasi *Privilege Access Management (PAM)*
Gangguan operasional	Perangkat lama sebagai backup sementara
Kegagalan migrasi	*Rollback plan* dan pengujian bertahap

Sumber: (Bank XYZ, 2024)

Penerapan *Privilege Access Management* (*PAM*) menjadi kontrol kunci untuk membatasi akses administratif hanya kepada personel yang berwenang, sehingga meminimalkan potensi penyalahgunaan akses selama perangkat *EoS* masih dioperasikan. Dikombinasikan dengan monitoring berkala, strategi ini memperkuat postur keamanan hingga proses migrasi perangkat jaringan selesai sepenuhnya.

5. KESIMPULAN DAN SARAN

Pengelolaan perangkat jaringan yang telah memasuki masa *End of Support* (*EoS*) merupakan aspek yang sangat penting dalam menjaga keberlangsungan operasional serta keamanan sistem informasi di sektor perbankan. Berdasarkan hasil kajian terhadap perangkat jaringan di lingkungan *Data Center* (*DC*) dan *Disaster Recovery Center* (*DRC*), dapat disimpulkan bahwa Bank XYZ telah menerapkan strategi manajemen yang terstruktur dan sistematis. Strategi tersebut meliputi proses identifikasi aset teknologi informasi, peremajaan perangkat melalui pendekatan *evergreen*, penyusunan *Timeline* migrasi yang bertahap, serta penerapan langkah mitigasi risiko selama masa transisi. Pendekatan ini menunjukkan adanya keselarasan antara kebijakan pengelolaan infrastruktur teknologi informasi dengan prinsip tata kelola TI yang baik serta tuntutan

regulasi perbankan, khususnya yang berkaitan dengan manajemen risiko dan keberlangsungan layanan.

Meskipun demikian, pengelolaan perangkat *EoS* perlu terus ditingkatkan agar risiko operasional dan keamanan dapat diminimalkan secara berkelanjutan. Oleh karena itu, disarankan agar bank memperkuat kebijakan manajemen siklus hidup aset teknologi informasi melalui evaluasi berkala terhadap status dukungan perangkat dan perencanaan penggantian sejak dini. Selain itu, integrasi perencanaan *End of Support* ke dalam strategi jangka panjang teknologi informasi akan membantu meningkatkan efisiensi pengelolaan infrastruktur, mengoptimalkan penggunaan sumber daya, serta mendukung pencapaian tujuan bisnis bank secara berkelanjutan.

DAFTAR PUSTAKA

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors for information technology governance (ITG). *International Journal of Information Management, 36*(6), 907–916. https://doi.org/10.1016/j.ijinfomgt.2016.05.017.

Cybersecurity governance in public institutions: Managing digital risks and resilience. (2025). *Visioner: Jurnal Pemerintahan Daerah di Indonesia, 17*(3). https://doi.org/10.54783/jv.v17i3.1424.

Evaluation of Information Technology Governance at Mikroskil University Using COBIT 2019 Framework with BAI11 Domain. (2022). *International Journal of Research and Applied Technology (INJURATECH), 2*(2), 128–143. https://doi.org/10.34010/injuratech.v2i2.8085.

Identification of IT Governance Capability Level of COBIT 2019 at The KOMINFO City of Bitung, North Sulawesi. (2023). *TeIKa, 13*(01), 1–15. https://doi.org/10.36342/teika.v13i01.3064.

Khadka, K., Ullah, A.B. Human factors in cybersecurity: an interdisciplinary review and framework proposal. Int. J. Inf. Secur. 24, 119 (2025). https://doi.org/10.1007/s10207-025-01032-0.

Marinos, L., & Lourenço, M. (2016). Cybersecurity governance for critical infrastructures. *Computer Law & Security Review, 32*(5), 742–754. https://doi.org/10.1016/j.clsr.2016.07.012.

Security infrastructure service and information security management capability audit to improve system security in preventing cyber attacks using COBIT 2019. (2024). *G-Tech: Jurnal Teknologi Terapan, 9*(1). https://doi.org/10.70609/gtech.v9i1.6319.

Turel, O., & Bart, C. (2014). Board-level IT governance and organizational performance. *European Journal of Information Systems, 23*(2), 223–239. https://doi.org/10.1057/ejis.2012.61.

Von Solms, R., & Von Solms, B. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security, 26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Wicaksono, J. A., Widodo, A. P., & Adi, K. (2023). *Systematic literature review on information technology governance in government*. *Telematika: Jurnal Telematika dan Teknologi Informasi, 20*(2), 226–237. https://doi.org/10.31315/telematika.v20i2.9642.