

## **Pelatihan Manajemen Resiko Teknologi Informasi Untuk Meningkatkan Keamanan dan Efisiensi Operasional di Lembaga Pendidikan**

**Yusra Fadhillah<sup>1</sup>, Muhammad Noor Hasan Siregar<sup>2</sup>, Heri Dia Anata Batubara<sup>3</sup>,  
Novita Aswan<sup>4</sup>, Ferawati Artauli Hasibuan<sup>5</sup>**

*<sup>1,2,3,4,5</sup> Universitas Graha Nusantara Padangsidimpuan, Indonesia*

### **Corresponding Author**

**Nama Penulis:** Yusra Fadhillah

**E-mail:** [yusra.fadilah18@gmail.com](mailto:yusra.fadilah18@gmail.com)

### **Abstrak**

*Di era teknologi informasi yang semakin berkembang, institusi pendidikan sangat bergantung pada teknologi informasi untuk mendukung berbagai bagian operasional mereka, seperti manajemen data, administrasi, dan pembelajaran online. Namun, ketergantungan ini membawa risiko keamanan data dan masalah operasional yang dapat mengganggu proses pendidikan. Tujuan dari program pengabdian masyarakat ini adalah untuk melatih karyawan dan manajemen lembaga pendidikan YPKS Padangsidimpuan dalam manajemen risiko teknologi informasi (TI) untuk meningkatkan keamanan dan efisiensi operasional. Peserta akan mendapatkan pemahaman dasar tentang manajemen risiko TI dalam sesi pelatihan dan workshop. Mereka juga akan mempelajari metode untuk mengidentifikasi dan menganalisis risiko serta teknik mitigasi untuk mengurangi risiko yang telah ditemukan. Program ini juga mencakup langkah-langkah untuk menerapkan kebijakan keamanan data, pemantauan risiko, dan evaluasi berkelanjutan untuk memastikan keamanan data sensitif dan kelancaran operasional. Diharapkan hasilnya adalah peningkatan kesadaran akan pentingnya manajemen risiko TI, dokumen yang jelas tentang identifikasi dan rencana mitigasi risiko, peningkatan keamanan, dan peningkatan efisiensi operasional. Oleh karena itu, institusi pendidikan dapat menciptakan lingkungan digital yang lebih aman dan lebih siap untuk menangani insiden TI. Diharapkan bahwa program ini akan memberikan kontribusi besar dalam meningkatkan keamanan dan efisiensi sistem pendidikan di era komputer dan internet.*

**Kata kunci** - Manajemen Resiko TI, Keamanan Data, Teknologi Informasi, Efisiensi Operasional, Lembaga Pendidikan

### **Abstract**

*In the growing era of information technology, educational institutions rely heavily on information technology to support various parts of their operations, such as data management, administration, and online learning. However, this dependency brings data security risks and operational issues that can disrupt the education process. The objective of this community service program is to train employees and management of educational institutions in information technology (IT) risk management to improve security and operational efficiency. Participants will gain a basic understanding of IT risk management in training sessions and workshops. They will also learn methods to identify and analyze risks as well as mitigation techniques to reduce risks that have been found. The program also covers steps to implement data security policies, risk monitoring, and continuous evaluation to ensure the security of sensitive data and smooth operations. The expected outcomes are increased awareness of the importance of IT risk management; clear documents on risk identification and mitigation plans; improved security; and increased operational efficiency. Educational institutions can therefore create a safer digital environment and be better equipped to handle IT incidents. It is hoped that this program will make a major contribution to improving the security and efficiency of education systems in the computer age.*

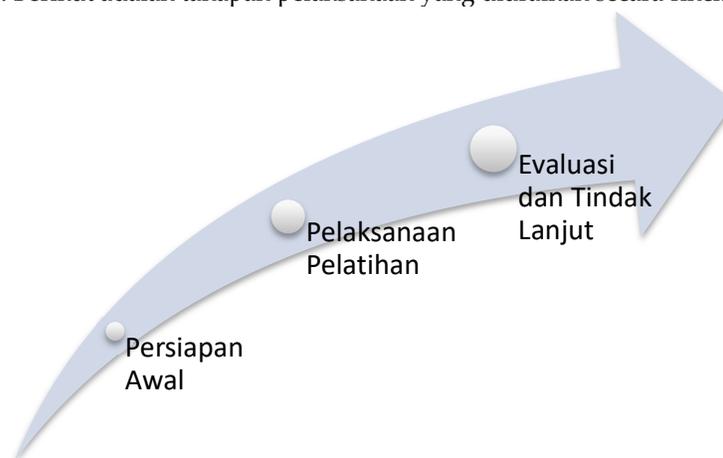
**Keywords** - IT Risk Management, Data Security, Information Technology, Operational Efficiency, Educational Institutions

## PENDAHULUAN

Dalam era digital saat ini, institusi pendidikan menghadapi masalah yang semakin sulit untuk mengelola dan melindungi data mereka. Proses sehari-hari di sekolah, perguruan tinggi, dan lembaga pendidikan lainnya sekarang memerlukan teknologi informasi (TI) (Sutomo dan Saputra, 2017). Berbagai elemen TI termasuk administrasi, pembelajaran jarak jauh, dan penyimpanan data pribadi siswa dan karyawan. Namun, lebih banyak bergantung pada teknologi ini meningkatkan risiko terhadap efisiensi operasional dan keamanan data. Semakin banyak insiden keamanan siber yang terjadi di institusi pendidikan adalah topik yang mendasari penulisan artikel ini. Serangan siber, kebocoran data, dan gangguan operasional dapat merusak uang dan reputasi. Studi sebelumnya menunjukkan bahwa institusi pendidikan sering menjadi sasaran serangan karena kurangnya infrastruktur keamanan dan kurangnya kesadaran akan pentingnya manajemen risiko TI. 67% lembaga pendidikan mengalami pelanggaran data dalam dua tahun terakhir, menurut pengabdian masyarakat Ponemon Institute (2018). Lebih dari 80% insiden keamanan di pendidikan dikaitkan dengan kesalahan manusia dan kurangnya pelatihan keamanan, menurut studi tambahan yang dilakukan oleh Verizon (2019) (Yusuf dan Kholik, 2023). Pengabdian masyarakat ini menunjukkan bahwa kesadaran dan kemampuan manajemen risiko TI di lembaga pendidikan harus ditingkatkan. Untuk meningkatkan keamanan dan efisiensi operasional lembaga pendidikan, pengabdian masyarakat ini bertujuan untuk mengembangkan program pelatihan yang komprehensif tentang manajemen risiko TI. Pelatihan ini diharapkan dapat membekali staf dan manajemen dengan pengetahuan dan keterampilan yang diperlukan untuk mengidentifikasi, menilai, dan mengelola risiko TI secara efektif (Yusuf *et al.*, 2023). Dengan menerapkan pelatihan ini, lembaga pendidikan YPKS Padansidimpuan dapat membangun infrastruktur keamanan yang lebih kuat dan menciptakan lingkungan operasional yang lebih efisien dan aman. Oleh karena itu, pengabdian masyarakat ini berkonsentrasi pada pembuatan dan pelaksanaan pelatihan manajemen risiko TI sebagai cara untuk mengatasi masalah keamanan dan operasional di institusi pendidikan. Diharapkan pengabdian masyarakat ini akan menghasilkan peningkatan keamanan informasi dan efisiensi operasional di sektor pendidikan (Sandy dan Solihin, 2021).

## METODE

Untuk memastikan bahwa pelatihan manajemen risiko TI efektif dan sesuai dengan kebutuhan sekolah, bagian ini menjelaskan prosedur dan tahapan pelaksanaan yang digunakan (Wijaya, Siregar dan Kartika, 2023). Berikut adalah tahapan pelaksanaan yang diuraikan secara rinci:



**Gambar 1.**  
Metode Pelaksanaan

1. Persiapan Awal
  - a. Analisis Kebutuhan

Tujuannya adalah untuk mengidentifikasi kebutuhan spesifik Lembaga Pendidikan terkait manajemen resiko TI. Langkah-langkah yang dapat dilakukan adalah

    - a) Melakukan wawancara dengan manajeen staf TI untuk memahami tantangan dan resiko yang ada.
    - b) Melakukan penyebaran kuesioner guna mengumpulkan data tentang tingkat kesadaran dan praktik keamanan saat ini
    - c) Melakukan audit awal infrastruktur TI untuk kebutuhan identifikasi kerentanan dan area yang memerlukan perhatian khusus
  - b. Pengembangan Modul Pelatihan

Tujuannya untuk melakukan pengembangan materi pelatihan yang sesuai dengan kebutuhan yang telah dilakukan identifikasi. Langkah -langkah yang dapat di lakukan adalah:

    - a) Mengembangkan kurikulum yang mencakup dasar-dasar manajeen resiko TI, analisis dan mitigasi resiko, kebijakan keamanan informasi dan rencana tanggapan insiden
    - b) Menyusun bahan ajar seperti presentasi, manua, studi kasus dan panduan praktis
    - c) Membuat konten e-learning yang interaktif untuk mendukung pembelajaran jarak jauh
2. Pelaksanaan Pelatihan
  - a. Workshop Tatap Muka

Tujuannya adalah untuk memberikan pelatihan langsung kepada staf dan manajemen Lembaga Pendidikan. Langkah-langkah yang dilakukan dalam tahap ini adalah:

    - a) Melakukan penjadwaan sesi pelatihan di lokasi yang mudah di akses oleh semua peserta
    - b) Mengadakan sesi interaktif yang mencakup presentasi teori, diskusi kelompok dan Latihan praktis
    - c) Melibatkan fasilitator berpengalaman yang dapat memberikan contoh konkret dan menjawab pertanyaan peserta
  - b. E-Learning

Tujuan dilakukannya adalah untuk menyediakan fleksibilitas dala belajar dengan akses online ke materi pelatihan. Langkah-langkah yang dilakukan adalah:

    - a) Menyediakan akses ke platform e-learning dengan modul interaktif, video dan kuis untuk mengevaluasi pemahaman peserta
    - b) Melakukan pemantauan kemajuan terhadap peserta melalui sistem manajemen pembelajaran (LMS) dan memberikan umpan balik secara berkala.
    - c) Megadakan sesi tanya jawab online untuk membahas topik yang membutuhkan klasifikasi lebih lanjut
  - c. Simulasi dan Pelatihan

Tujuannya adalah untuk menguji kesiapan respon terhadap insiden keamanan. Langkah – Langkah yang dilakukan adalah:

    - a) Merancang scenario simulasi insiden siber yang realitis sesuai dengan ancaman yang mungkin dihadapi oleh sekolah atau Lembaga Pendidikan
    - b) Melaksanakan Latihan pemulihan bencana yang melibatkan seluruh tim TI dan manajemen
    - c) Melakukan evaluasi respon tim selama simulasi dan memberikan umpan balik untuk perbaikan.

3. Evaluasi dan Tindak Lanjut
  - a. Penilaian Efektivitas Pelatihan

Tujuannya dilakukan untuk mengukur keberhasilan pelatihan dalam meningkatkan keamanan dan efisiensi operasional Langkah-langkah dalam hal ini adalah:

    - a) Menyebarkan survei pasca pelatihan untuk mendapatkan umpan balik dari peserta mengenai konten dan penyimpanan pelatihan.
    - b) Melakukan wawancara dengan manajemen untuk menilai perubahan dalam praktik kerja dan kebijakan keamanan
    - c) Menggunakan indikator kinerja untuk menilai dampak pelatihan terhadap keamanan dan efisiensi operasional.
  - b. Pembaruan dan Perbaikan

Tujuan dilakukannya adalah untuk mengembangkan pelatihan berkelanjutan dan memastikan relevansi materi. Langkah-langkah yang dapat dilakukan adalah:

    - a) Mengumpulkan umpan balik dari peserta secara berkala untuk dilakukannya identifikasi area yang memerlukan perbaikan
    - b) Melakukan review berkala terhadap materi pelatihan berdasarkan perkembangan terbaru dalam teknologi dan ancaman siber
    - c) Melakukan revisi dan meningkatkan modul pelatihan untuk menjaga keberlanjutan dan efektivitas.

Dengan metode pelaksanaan yang terstruktur ini, diharapkan dapat menghasilkan pelatihan manajemen resiko TI yang di implementasikan secara efektif, menghasilkan peningkatan signifikan dalam kemandirian dan efisiensi operasional di sekolah maupun Lembaga Pendidikan.

## **HASIL DAN PEMBAHASAN**

Sekolah telah menunjukkan peningkatan keamanan dan efisiensi operasional melalui pelatihan manajemen risiko teknologi informasi (TI). Dalam hal peningkatan pengetahuan dan kesadaran Pelatihan berhasil meningkatkan kesadaran staf dan manajemen tentang pentingnya manajemen risiko TI. Peserta menunjukkan peningkatan signifikan dalam pemahaman mereka tentang berbagai jenis risiko TI dan cara mengelolanya. Dalam kesiapan menghadapi insiden, Latihan simulasi dan pemulihan bencana membantu manajemen dan tim TI menjadi lebih siap untuk menghadapi insiden keamanan. Ini membantu menemukan dan memperbaiki kekurangan dalam tanggapan terhadap insiden, yang meningkatkan kesiapan dan responsivitas terhadap ancaman siber. Analisis kebutuhan mengungkap bahwa mayoritas staf dan manajemen memiliki kesadaran yang rendah tentang risiko TI dan praktik keamanan yang baik. Infrastruktur TI memiliki beberapa kerentanan, terutama dalam pengelolaan akses dan penyimpanan data. Modul pelatihan yang dikembangkan mencakup dasar-dasar manajemen risiko TI, teknik analisis dan mitigasi risiko, kebijakan keamanan informasi, serta rencana tanggapan insiden. Modul ini dirancang dengan pendekatan praktis dan studi kasus nyata untuk meningkatkan relevansi dan keterlibatan peserta. Workshop tatap muka dihadiri oleh 80% staf dan manajemen. Peserta menunjukkan peningkatan pemahaman yang signifikan tentang konsep dasar manajemen risiko TI dan strategi mitigasi melalui penilaian pra dan pasca pelatihan. Modul e-learning diakses oleh 90% peserta yang terdaftar, dengan tingkat penyelesaian sebesar 85%. Kuis dan evaluasi online menunjukkan peningkatan rata-rata 40% dalam pemahaman peserta mengenai kebijakan dan prosedur keamanan. Survei pasca pelatihan menunjukkan tingkat kepuasan sebesar 85%, dengan banyak peserta merasa lebih siap dalam menghadapi risiko TI. Penilaian kinerja menunjukkan peningkatan dalam implementasi kebijakan keamanan dan pengurangan insiden keamanan yang dilaporkan. Berdasarkan umpan balik, beberapa modul pelatihan diperbarui untuk mencakup ancaman terbaru dan teknik mitigasi yang lebih efektif. Rencana pelatihan berkelanjutan disusun untuk memastikan bahwa staf tetap terinformasi

---

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license



Gambar 1.

Pelatihan Manajemen Resiko Teknologi Informasi

## KESIMPULAN

tentang perkembangan terbaru dalam keamanan TI. Pelatihan manajemen risiko TI ini berhasil mencapai tujuannya dalam meningkatkan kesadaran dan keterampilan staf dan manajemen lembaga pendidikan dalam mengelola risiko TI. Peningkatan pemahaman dan keterampilan ini tidak hanya membantu dalam melindungi data dan infrastruktur TI, tetapi juga meningkatkan efisiensi operasional secara keseluruhan. Dengan pelaksanaan pelatihan yang berkelanjutan dan penyesuaian berdasarkan umpan balik, lembaga pendidikan dapat membangun infrastruktur keamanan yang kuat dan efisien, memastikan bahwa mereka siap menghadapi tantangan keamanan TI di masa depan..

## UCAPAN TERIMA KASIH

Penulis ingin mengungkapkan ucapan terima kasih yang tulus kepada semua pihak yang telah memberikan dukungan dan kontribusinya dalam pelaksanaan pengabdian masyarakat ini. Pertama-tama, terima kasih kepada pimpinan Lembaga Pendidikan sekolah YPKS Padangsidempuan atas kesempatan dan dukungan penuh dalam pelaksanaan pelatihan manajemen risiko TI. Tanpa dukungan mereka, pengabdian masyarakat ini tidak akan terwujud. Penghargaan juga disampaikan kepada tim TI Lembaga Pendidikan YPKS Padangsidempuan yang telah berpartisipasi aktif dalam pelatihan dan berbagai pengetahuan serta pengalaman berharga. Terima kasih juga kepada rekan-rekan dosen yang telah memberikan kontribusinya dalam hal, masukan, saran dan dukungan moral selama proses pelaksanaan pelatihan maupun penulisan artikel ini. penulis menyampaikan penghargaan dan terima kasih kepada semua pihak yang telah berkontribusi. Semoga hasil pengabdian masyarakat ini bermanfaat dan dapat memberikan kontribusi positif bagi pengembangan manajemen risiko TI di lembaga pendidikan.

## DAFTAR PUSTAKA

- Sandy, S. dan Solihin, H. H. (2021) "Audit Keamanan dan Manajemen Risiko pada e-Learning Universitas Sangga Buana," *Jurnal Manajemen Informatika (JAMIKA)*, 11(1), hal. 1–14. doi: 10.34010/jamika.v11i1.3641.
- Sutomo, B. dan Saputra, M. A. (2017) "Perancangan Tata Kelola Teknologi Informasi Pada Perguruan Tinggi Dengan Menggunakan Framework Cobit 5 Studi Kasus : Stmik Dharma Wacana Metro," *International Research on Big-Data and Computer Technology: I-Robot*, 1(1), hal. 66–80. doi: 10.53514/ir.v1i1.7.
- Wijaya, A. R., Siregar, M. dan Kartika, D. (2023) "Perencanaan Strategis Sistem Informasi sebagai Pendukung Optimalisasi Layanan Pendidikan di Sekolah Dasar," *Dirasisi*, 1(1), hal. 1–18.
- Yusuf, M. et al. (2023) "Penggunaan Teknologi Internet of Things (Iot) Dalam Pengelolaan Fasilitas Dan Infrastruktur Lembaga Pendidikan Islam," *PROPHETIK Jurnal Kajian Keislaman*, 1(2), hal. 1–18.

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license



Yusuf, M. dan Kholik, A. (2023) "Inklusi Digital dalam Manajemen Perkantoran Lembaga Pendidikan Islam," *Toga Jurnal Keguruan dan Ilmu Pendidikan*, 1(1), hal. 1–10. Tersedia pada: <https://www.mendeley.com/reference-manager/reader-v2/9c63cbb5-db34-3569-8ef1-1665fbe97046/106ba641-0f67-81d5-6806-c852296adf1a>.