Author Author

Proposal for Final Project.edited

Turnitin

Document Details

Submission ID

trn:oid:::3618:120885275

Submission Date

Nov 11, 2025, 10:05 AM GMT+5

Download Date

Nov 11, 2025, 10:06 AM GMT+5

File Name

Proposal for Final Project.edited.docx

File Size

16.1 KB

4 Pages

337 Words

2,263 Characters

1% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography

Match Groups

1 Not Cited or Quoted 1%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

0%	Internet sources
0%	Publications
1%	Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

1 Not Cited or Quoted 1%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

0%	Internet sources
0%	Publications
1%	Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Submitted works	
Turku University of Applied Sciences on 2025-04-29		**1%**

Proposal for Final Project: AI/Quantum and Supply-Chain Governance in Cyber Risk

Student

Institution

Course

Instructor

Date

Proposal for Final Project: AI/Quantum and Supply-Chain Governance in Cyber Risk

Thesis Question

What can AI-driven supply-chain attacks and quantum decryption of vendor certificates do to the third-party cyber risk by 2027, and what governance-first controls (at the intersection of Units 6-8 (Executive Leadership and Organizational Dynamics)) do boards require all suppliers to prevent regulatory and financial meltdown?

Summary

This paper builds on Unit 14: Emerging Trends and Technologies to analyze AI automation of multi-tier supply-chain compromises (For example, deepfake CISO approvals) and quantum computing subverting PKI trust in Software Bills of Materials (SBOMs). With methods of Unit 4 risk quantification and How to Measure Anything in Cybersecurity Risk, it models the probability of breaches and financial losses in highly trusted industries and organizations (Boyens, 2021). The main thesis: the absence of board-stated supplier governance playbooks (according to A Leader Guide to Cybersecurity, Chapter 7) means that more than 60 percent of breaches in the future will be initiated outside of the perimeter defenses. This response would involve zero-trust vendor attestation, quantum-secure SBOM verification, and assigned incident delegation, which can be implemented by 2026 to remove the exasperatingly important gap of governance lag and ensure organizational resilience.

Research Plan

For baseline, use Research Plan, utilize the cases of Leverage Study.net, Units 2-3 risk labs, and Unit 12 GRC tools. The external sources will consist of 2025 industry reports about AI supply-chain sabotage and quantum vendor risk. The references verify trends, implications, leading indicators (For example, SBOM tampering spikes), and resource requirements (training).

Gaps (existing controls versus the controls required), benefits (40 percent reduction in risk), and tactical actions (rollout 2026) will be quantified through analysis and will pressurize the executive to take action, using cost-benefit models.

References

Boyens, J. (2021). *(Draft) Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. https://doi.org/10.6028/nist.sp.800-161r1-draft

ENISA *Threat Landscape 2025* – Vendor compromise scenarios. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

WEF, *Global Cybersecurity Outlook 2025* – “AI in Supply-Chain Sabotage” https://www.weforum.org/publications/global-cybersecurity-outlook-2025/