Flow-Constrained Risk Management for Operational Technology Security: A Multi-Criteria Framework for Critical Infrastructure

Vsevolod Shabad[a]

[a] Department of Computer Science, University of Liverpool, Liverpool L69 3DR, United Kingdom.

Corresponding author: Vsevolod Shabad, Department of Computer Science,
University of Liverpool, Liverpool L69 3DR, United Kingdom.
Email: v.shabad@liverpool.ac.uk
ORCID: https://orcid.org/0009-0001-9332-6688

Abstract

Critical infrastructure operators face unprecedented cybersecurity threats whilst operating under severe resource constraints that traditional security frameworks fail to address. This research presents a novel flow-constrained risk management framework that enables systematic improvement of operational technology security within realistic organisational limitations. Building on lean manufacturing optimisation principles, the framework constrains security improvements through work-in-progress limitations: exactly one major improvement per quarter per asset, plus a maximum of three minor improvements in parallel. The approach integrates progressive Annual Loss Exposure refinement with multi-criteria stakeholder decision-making to provide measurable progress without requiring lengthy strategic investment cycles. The framework addresses four critical implementation gaps: systematic underestimation of resource constraints, reliance on non-existent representative datasets, insufficient recognition of behavioural biases, and dependence on strategic approval processes mismatched to threat response timelines. Mathematical analysis examines the convergence properties of the progressive risk assessment methodology, whilst queuing theory validates the efficiency improvements of the flow-constrained approach. Implementation feasibility was demonstrated within a global conglomerate operating across energy, mining, and manufacturing sectors. The framework provides the theoretical foundation for achieving systematic security enhancement within practical constraints, enabling board-level visibility through consistent risk reduction trends whilst avoiding contentious resource allocation debates.

Keywords: operational technology security, critical infrastructure, risk management, resource allocation, bias management

1 Introduction

Critical infrastructure operators face unprecedented cybersecurity threats whilst operating under severe resource constraints that traditional security frameworks fail to address. State-sponsored Advanced Persistent Threat groups systematically target critical infrastructure networks, with ransomware attacks against industrial organisations increasing by 87% in 2024 (Dragos, 2025). This threat escalation occurs against systematic underfunding in resource-constrained critical infrastructure environments (Stouffer et al., 2023).

Existing operational technology security frameworks provide comprehensive technical guidance; however, they systematically fail to address implementation barriers that prevent effective security enhancements. Current approaches assume organisations can secure dedicated budgets and implement controls across all systems simultaneously. However, empirical research reveals systematic gaps between framework recommendations and actual implementation capabilities, with implementation failures persisting regardless of framework quality (Evripidou and Watson, 2024).

This research addresses implementation challenges that interact synergistically to create systematic failure patterns in operational technology security. While individual challenges - resource constraints, data scarcity, behavioural biases, and strategic approval process limitations - are recognised across research domains, their combined interaction creates reinforcing failure patterns that undermine even well-designed security programmes.

This work presents a flow-constrained risk management framework that acknowledges these implementation barriers as interconnected constraints requiring simultaneous rather than sequential treatment. Building on work-in-progress limitation principles from lean manufacturing optimisation (Anderson, 2010), the framework enables systematic security improvement through disciplined resource allocation whilst operating within existing organisational capacity.

2 Background and Related Work

The theoretical foundation was established by combining lean manufacturing flow optimisation principles from Kanban (Anderson, 2010) and Scaled Agile (Leffingwell, 2018) with OT security management methodologies (Stouffer et al., 2023).

The mathematical formulation drew on queuing theory (Little, 1961) and multi-criteria decision analysis (Freeman, 1984) to provide rigorous analytical foundations.

Validation employed case study methodology within critical infrastructure environments to demonstrate practical feasibility.

2.1 Existing OT Security Frameworks and Their Limitations

Current operational technology (OT) security frameworks provide comprehensive technical guidance but systematically fail to address implementation barriers that prevent effective security enhancement. ISA/IEC 62443 establishes security levels and controls, whilst NIST SP 800-82r3 provides control baselines, and the Industrial Internet Consortium's security framework (Industrial Internet Consortium, 2016) addresses threat modelling and risk assessment processes. However, all share common assumptions about organisational capacity that rarely hold in practice.

These frameworks assume organisations can secure dedicated security budgets through strategic investment processes, access reliable historical data for quantitative risk assessment, overcome psychological resistance through technical arguments, and implement comprehensive controls across all assets simultaneously. NIST SP 800-82r3 exemplifies this challenge, providing comprehensive technical guidance whilst explicitly acknowledging critical implementation constraints. The framework recognises that OT environments often cannot accommodate unplanned downtime since "outages must be planned and scheduled days or weeks in advance," that "the goals of safety and efficiency sometimes conflict with security in the design and operation of OT systems," and that many OT components are "designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities" (Stouffer et al., 2023). Despite acknowledging these as "resource-constrained systems that do not include typical contemporary IT security capabilities," the framework assumes organisations can implement recommended controls across all systems simultaneously.

Recent empirical research by Evripidou and Watson (2024) examined OT security implementation challenges through a qualitative study with 72 practitioners, revealing systematic gaps between framework recommendations and practical implementation capabilities. Their analysis identified stakeholder mindset factors and operational values prioritisation as primary barriers, with cybersecurity often clashing with established operational priorities such as availability and safety. Critically, their findings demonstrate that implementation gaps persist regardless of framework quality, suggesting fundamental rather than peripheral challenges.

2.2 Evolving Threat Landscape for Critical Infrastructure

Critical infrastructure operators face an unprecedented escalation in both threat sophistication and attack frequency, which fundamentally challenges traditional security investment approaches. State-sponsored APT groups have systematically targeted critical infrastructure networks. According to the NCSC, "China state-sponsored and Russia state-sponsored actors are among the attackers that have been observed living off the land on compromised critical infrastructure networks" (National Cyber Security Centre, 2024). These sophisticated attacks represent a qualitative shift from opportunistic cybercrime to strategic nation-state operations designed to establish persistent access to critical systems.

The velocity of vulnerability discovery has accelerated dramatically, creating continuous pressure for security responses that traditional strategic planning cycles cannot keep pace with. CISA's Known Exploited Vulnerabilities catalogue (Cybersecurity and Infrastructure Security Agency, n.d.) demonstrates this acceleration, with industrial control system vulnerabilities increasingly appearing in actively exploited threat intelligence. Yet, the average time from vulnerability disclosure to active exploitation has decreased significantly, compressing the window available for defensive responses.

This threat escalation occurs against systematic underfunding that has persisted for decades. The NCSC observes that commercial incentives within the UK's CNI "can take priority over investment in the secure operation of critical systems," and that organisations with less mature security may limit incident information-sharing, hampering national response efforts (National Cyber Security Centre, 2023, p. 35). There is broad recognition of long-term underinvestment in UK infrastructure. The House of Commons Library notes “there is a general acceptance that there has been under investment in UK infrastructure in recent decades” and highlights significant deficiencies identified by the National Infrastructure Commission (Keep et al., 2025, p.4). HM Treasury likewise refers to a “cycle of underinvestment and instability” affecting the UK’s infrastructure systems (HM Treasury, 2024). Current threat data indicate that ransomware attacks against industrial organisations increased by 87% in 2024, with 60% more ransomware groups impacting OT/ICS environments (Dragos, 2025).

2.3 Resource Constraints in OT Security Implementation

Manufacturing research demonstrates how resource constraints undermine implementation quality regardless of process design sophistication. Current operational technology security frameworks emphasise comprehensive technical controls but systematically underestimate how resource constraints shape practical implementation outcomes. While NIST provides a three-tier control baseline approach, achieving even the "low" baseline often proves impossible given underfunding.

The systematic nature of resource constraints means that approaches assuming unlimited implementation capacity will fail in practice, regardless of technical sophistication. NIST SP 800-82r3 provides a useful three-tier control baseline approach; however, achieving even the "low" baseline often proves impossible for operators facing chronic underfunding, a lack of enforcement mechanisms, and accumulated security debt from deferred maintenance. These frameworks provide comprehensive technical guidance, but they systematically underestimate the impact of resource constraints on actual implementation outcomes.

2.4 Data Scarcity in OT Risk Assessment

Cybersecurity economics literature documents the systematic absence of reliable data for risk quantification in OT environments. Unlike domains such as payment fraud, where high-frequency events enable statistical analysis, OT security must operate under conditions of fundamental data uncertainty where cyber-attacks represent "high-impact, low-frequency events" with insufficient datasets for reliable risk assessment (Cook et al., 2016).

Leading cybersecurity researchers have established a scholarly consensus that organisations "cannot rely on quantified threat assessments because representative incident datasets don't exist" for operational technology environments. Research demonstrates that "collecting data on cyberattacks is extremely difficult" with significant sampling bias where "ransomware victims do not disclose the full reality of their experiences" (Cremer et al., 2022). Even purpose-built academic datasets contain fundamental flaws, as acknowledged by (Morris, 2015), creator of widely-cited industrial control systems datasets: "These datasets have been found to contain some unintended patterns which cause machine learning algorithms to easily identify attacks versus non-attacks in unrealistic ways."

This data scarcity creates what Canbek et al. (2022) describe as "garbage in, garbage out" degradation in cybersecurity analysis workflows. Academic analysis of sophisticated frameworks like Factor Analysis of Information Risk reveals that algorithms restrict statistical distributions and model expandability when applied to operational technology environments lacking historical incident data (Wang et al., 2020). Anderson and Moore (2006) establish that "risks cannot be managed better until they can be measured better," yet the systematic absence of reliable OT incident data means traditional measurement approaches fail precisely when most needed.

2.5 Systematic Behavioural Biases in OT Security Investment

Behavioural economics research reveals consistent cognitive biases that affect technology investment decisions under uncertainty. Kahneman and Tversky's prospect theory demonstrates that decision-makers systematically deviate from rational choice models when facing uncertain outcomes with potential losses (Kahneman and Tversky, 1979). A recent analysis Korteling et al. (2023) shows that executives systematically discount future risks, prefer maintaining current systems, and rely on external validation when facing uncertainty.

Critical infrastructure organisations exhibit distinctive patterns, creating systematic resistance to security investment. Financially anchored executives demand quantitative ROI analysis, which data scarcity makes impossible. OT-anchored executives exhibit systematic scepticism toward threats they cannot directly observe, viewing security warnings as theoretical concerns. Key biases include: normalcy bias (underestimating adverse event likelihood), overconfidence bias (overestimating defensive capabilities), availability heuristic (recalling observed disruptions but struggling with cyber incident probabilities), anchoring bias (initial estimates unduly influencing decisions), and not-invented-here syndrome (rejecting externally originated ideas).

Even when external validation confirms threat reality and magnitude, executives continue attempting to reduce security resources for "operational efficiency." This creates requirements for sustained demonstration of security improvement progress through visible, measurable trends that maintain stakeholder confidence and resist budget erosion over time.

Recent research extends foundational cognitive bias theory to cybersecurity-specific contexts, with studies identifying an optimistic bias in cyber risk perception as a systematic factor affecting security investment decisions (Salzberger, 2025). This research demonstrates that executives systematically underestimate cyber risk likelihood whilst overestimating their organisation's defensive capabilities, patterns that align with the executive psychology challenges observed in critical infrastructure environments.

2.6 Strategic Investment Processes vs. Operational Agility Requirements

Operations research literature demonstrates how strategic planning cycles can create responsiveness barriers in dynamic threat environments. Traditional cybersecurity and OT security approaches assume organisations can secure dedicated security budgets through strategic planning and board-level approvals, creating fundamental temporal mismatches between investment approval cycles and threat response requirements. Strategic investment processes typically require months of business case development, stakeholder consultation, budget allocation, and board approval, whilst threat landscapes evolve continuously with exploitation timescales measured in days or weeks.

Multi-criteria decision-making applications in cybersecurity typically assume that decision-makers can evaluate an unlimited number of alternatives using detailed technical criteria (Wang, 2019). However, cognitive psychology research demonstrates that decision quality deteriorates when stakeholders face excessive alternatives without structured selection processes (Iyengar and Lepper, 2000). This challenge becomes acute when organisations attempt to develop comprehensive business cases for security improvements across multiple assets simultaneously, creating choice overload that paradoxically delays decision-making.

NIST SP 800-39 provides comprehensive guidance for iterative organisational risk management but offers limited practical direction for resource allocation when organisations cannot implement all recommended controls simultaneously whilst maintaining operational responsiveness (National Institute of Standards and Technology, 2011). The framework assumes organisations can pause operational security improvement whilst developing strategic investment cases, an assumption that conflicts with the continuous evolution of threats.

2.7 Research Gap and Integrated Approach Novelty

Existing literature treats implementation challenges as separate problems requiring independent solutions. Manufacturing research addresses resource constraints, cybersecurity economics documents data limitations, behavioural economics reveals cognitive biases, and operations research demonstrates agility barriers - but current approaches assume organisations can address each gap sequentially through implementing "continuous monitoring," conducting "regular risk assessments," and developing "incident response planning" without acknowledging how these challenges interact to prevent effective implementation.

Freeman's stakeholder theory offers frameworks for engaging diverse groups with conflicting priorities (Freeman, 1984), but existing stakeholder engagement approaches assume unlimited deliberation time and analytical resources. The Scaled Agile Framework provides portfolio management approaches that optimise resource allocation under uncertainty through work-in-progress limitations and iterative planning cycles (Leffingwell, 2018), but these principles have received limited attention in cybersecurity domains where strategic investment cycles predominate.

While these approaches address individual aspects of implementation challenges, existing literature lacks integrated frameworks that simultaneously address resource constraints, data limitations, behavioural biases, and agility requirements within operational technology security contexts. The need for integrated solutions that acknowledge these gaps as interconnected constraints requiring simultaneous rather than sequential treatment represents the fundamental research gap this work addresses.

2.8 Stakeholder Engagement Process Design

The framework addresses systematic behavioural biases through structured multi-criteria decision-making adapted from Hohmann's Innovation Games methodology (Hohmann, 2006). The "Buy the Feature" prioritisation game provides established procedures for collaborative decision-making under resource constraints, but requires modification to address resistance patterns specific to operational technology environments.

Evripidou and Watson (2024) conducted qualitative analysis with 72 OT cybersecurity practitioners, revealing that cybersecurity often clashes with established operational priorities such as availability and safety. Their findings demonstrate that implementation gaps persist regardless of framework quality, suggesting that stakeholder engagement challenges represent fundamental rather than peripheral barriers.

The process modifications specifically target the "not-invented-here syndrome," where individuals reject ideas originating from outside their group (Katz and Allen, 1982). By ensuring each expert feels they are co-authors of final decisions rather than having security measures imposed by headquarters, the process addresses systematic resistance to externally mandated security improvements.

Expert group composition is based on Freeman's stakeholder theory (Freeman, 1984), which provides a framework for engaging diverse groups with conflicting priorities in complex decision-making. The collaborative prioritisation process employs power-of-two voting cards rather than Fibonacci sequences to make priority differences highly visible, where discrepancies between individual priorities and collective rankings become readily apparent.

3 Methods

3.1 Research Design and Methodology

This research emerged from practical necessity when the author, operating within critical infrastructure environments, faced urgent requirements to strengthen OT security against active nation-state threat actors whilst constrained by limited resources and funding allocations. The enterprise assets under responsibility were directly threatened by state-sponsored APT groups actively targeting critical infrastructure networks, creating immediate OT security requirements that could not be met by traditional strategic investment cycles.

Initial attempts to apply established security frameworks and risk management approaches, well-documented in existing literature, proved inadequate for addressing the simultaneous pressures of active nation-state threats and severe resource limitations characteristic of critical infrastructure operators. Traditional approaches, assuming comprehensive security budgets and lengthy implementation timelines, were fundamentally mismatched to the operational reality of defending against sophisticated attackers with existing organisational capacity.

This practical challenge necessitated developing novel approaches that could achieve systematic security improvement within existing constraints, whilst providing demonstrable progress against documented threats. The research, therefore, employs design science methodology to develop and validate a flow-constrained risk management framework that addresses implementation barriers preventing effective operational technology security enhancement under active threat conditions.

Research Question Development: The primary research question emerged from this practical experience, combined with an analysis of implementation failures documented in the existing literature: ***How can critical infrastructure operators achieve systematic OT security improvements within existing resource constraints, while providing measurable progress for executive oversight?*** Supporting methodological questions address resource allocation approaches, risk assessment methodologies under data uncertainty, stakeholder engagement techniques, and progress measurement mechanisms.

Methodological Approach: The research follows a four-phase design science process addressing the fundamental challenge identified by Gordon and Loeb (2006) that, whilst economic models for security investment are theoretically valid, organisational acceptance remains limited due to practical implementation barriers that existing frameworks systematically underestimate.

3.2 Cross-Domain Literature Analysis Methodology

Literature analysis employed a methodology across five complementary domains to identify implementation barriers and solution approaches: **operational technology security** (technical foundations and implementation failures), **risk management** (quantitative assessment approaches and data uncertainty challenges), **behavioural economics** (decision-making biases affecting security investment), **lean manufacturing and agile methodologies** (resource constraint management and workflow optimisation), and **stakeholder management theory** (collaborative decision-making frameworks).

Analysis revealed that existing literature treats implementation challenges as separate problems requiring independent solutions, whereas their combined interaction creates reinforcing failure patterns preventing effective implementation. Four critical constraints requiring simultaneous treatment were identified: (1) resource limitations preventing comprehensive control deployment, (2) data scarcity undermining quantitative risk assessment, (3) psychological barriers impeding security investment decisions, and (4) temporal mismatches between strategic planning cycles and threat response requirements. These became fundamental design requirements, validated through practitioner feedback.

3.3 Component Development and Selection Methodology

The four critical constraints were translated into specific design requirements through structured analysis. Resource limitations required components functioning within existing capacity constraints, data scarcity required approaches operating without comprehensive historical datasets, psychological barriers required methods overcoming stakeholder resistance patterns, and temporal mismatches required approaches providing operational agility whilst maintaining strategic oversight.

Framework components were identified through evaluation of approaches from each domain against derived requirements using five selection criteria: multi-constraint capability, implementation feasibility, organisational acceptance, measurable progress demonstration, and theoretical rigour. Selected approaches required adaptation to address differences between source domains and OT security contexts through: theoretical foundation analysis, constraint mapping to OT security context, modification design addressing identified gaps, and preliminary validation through expert review.

Component integration evaluation employed interface analysis to identify potential theoretical conflicts between different domain approaches and dependency mapping, examining where solutions to one constraint might impact others, ensuring component compatibility assessment before implementation testing.

3.4 Mathematical Foundation Selection and Validation Methodology

Mathematical approach selection required evaluation because no single theoretical framework could simultaneously address all framework requirements. Evaluation assessed potential mathematical foundations across analytical capability, practical applicability within resource-constrained environments, and integration potential with other required approaches.

The research design combined queuing theory, multi-criteria decision analysis, and probability theory, following Lewis and Grimes (2005). Compatibility assessment procedures evaluated theoretical coherence between different mathematical approaches through formal analysis of underlying assumptions, parameter requirements, and output interpretation methods.

Mathematical validation required developing analytical approaches because traditional validation methods assume conditions that the framework explicitly addresses as constraints. Following convergence analysis methodology from operations research literature, procedures demonstrated theoretical validity under data uncertainty conditions through convergence analysis and sensitivity analysis, examining robustness across parameter variations. Mathematical validation employed formal proof techniques, mathematical modelling testing framework behaviour, and peer review processes with mathematical experts.

3.5 Empirical Validation Design and Implementation Methodology

Case Study Design Rationale and Approach: The single-case embedded design was selected after evaluating alternative empirical approaches following Yin (2018) case study methodology. Multi-case studies were rejected due to access limitations in critical infrastructure environments. Experimental designs were eliminated as neither feasible nor ethical in OT security contexts. Survey approaches were insufficient for assessing complex organisational change effects. The embedded approach provides multiple validation contexts within controlled organisational variables whilst maintaining practical implementation feasibility.

Longitudinal Study Design Methodology: Following Menard (2002), the multi-quarterly implementation design addressed specific validation requirements. Initial quarters assessed implementation feasibility and stakeholder acceptance. The middle quarters evaluated sustained engagement and adaptation capability. Final quarters measured cultural transformation effects and long-term sustainability. This temporal structure enabled assessment of both short-term effectiveness and long-term organisational change impacts.

Validity Threat Management and Research Rigour Design: Following Yin (2018), the research design addressed multiple validity threats through structured methodological choices. Internal validity protocols employed triangulation across multiple data sources, combined with member checking procedures. Construct validity methodology used multiple measurement indicators for each assessment criterion with convergent validity testing approaches. External validity enhancement employed comparison with documented implementation challenges in existing literature, enabling theoretical generalisation to similar contexts whilst acknowledging case study limitations.

Systematic Researcher Bias Management Approach: The author's dual role as researcher and practitioner required a comprehensive bias management research design following reflective practitioner methodology (Schön, 2016). Structured data collection approaches minimised subjective interpretation during evidence-gathering phases. Independent validation research procedures through stakeholder feedback sessions provided an external perspective on research findings and interpretations. Documentation approaches for design decisions enabled transparency and external scrutiny of all research choices, with a clear separation between practitioner insights and research analysis.

Evidence Collection Design and Analysis Framework: Following Creswell and Plano Clark (2018), data collection employed a triangulation methodology to ensure a comprehensive assessment whilst maintaining research rigour. Quantitative metrics were defined with specific measurement approaches and validation criteria. Qualitative evidence collection used structured approaches with analysis procedures. Mixed-methods analysis employed frameworks for integrating quantitative and qualitative findings whilst maintaining analytical rigour.

3.6 Ethical Considerations and Research Limitations

Ethical Research Design in Critical Infrastructure Contexts: Research design in critical infrastructure environments necessitates a systematic consideration of ethical implications and safety constraints, adhering to established ethical research guidelines for sensitive contexts. Ethical protocols ensured that research activities could not compromise the operational safety or security posture of participating assets. Research design explicitly excluded any interventions that might create new security vulnerabilities or operational risks. Informed consent procedures were developed to ensure all participants understood research objectives whilst maintaining confidentiality requirements for sensitive infrastructure information.

Research Design Limitations and Boundary Conditions: The research design acknowledges systematic limitations inherent in single-case embedded methodology within critical infrastructure contexts consistent with established case study limitations (Yin, 2018). Generalisation limitations were addressed through theoretical rather than statistical generalisation approaches. The research design explicitly acknowledges that organisational, cultural, and regulatory context variations may affect framework applicability across different critical infrastructure sectors. These limitations were systematically incorporated into research design choices and analysis methodology to ensure appropriate interpretation of findings.

Data Sensitivity and Confidentiality Research Protocols: Research design required systematic development of protocols for handling sensitive critical infrastructure security information. Data collection research procedures were designed to maintain participant anonymity whilst enabling systematic analysis. Storage and analysis protocols ensured compliance with both academic research standards and industrial security requirements. Research design included systematic procedures for ensuring that published findings could not compromise participant organisation security posture or reveal sensitive operational details.

3.7 Iterative Refinement and Quality Assurance Methodology

Framework Refinement Research Design: The iterative development process employed a systematic methodology to ensure research rigour whilst enabling practical adaptation. Each iteration cycle included structured feedback collection, systematic barrier identification, evidence-based design modification, and effectiveness validation before proceeding to subsequent iterations. This approach balanced research objectivity with practical improvement requirements.

Quality Control and Validation Checkpoints: Systematic quality assurance processes were embedded throughout the research design to maintain academic standards whilst addressing practical implementation requirements. Regular validation checkpoints assessed framework development against original research objectives. Expert review processes validated both theoretical foundations and practical applicability. Stakeholder feedback sessions ensured framework relevance whilst maintaining research independence.

Research Documentation and Traceability Protocol: Systematic documentation processes ensured research transparency and enabled external validation of methodological choices. Design decisions were documented with explicit rationale and supporting evidence. Alternative approaches were recorded with reasons for rejection. Iteration cycles were systematically tracked with clear criteria for modification decisions and effectiveness assessment outcomes.

4 Framework Specification

This research develops a flow-constrained risk management framework that addresses implementation barriers in operational technology security through a systematic methodology combining literature analysis, theoretical modelling, and iterative refinement through practical application. The approach focuses on creating innovative solutions that address identified problems whilst contributing to scientific knowledge through rigorous analytical foundations.

4.1 Architectural Overview

This framework addresses critical infrastructure security improvement through an integrated approach that operates within existing resource constraints, whilst providing measurable progress for board oversight. The framework integrates two core components that address the fundamental implementation barriers identified in existing approaches:

- **Flow-constrained portfolio management** governs resource allocation and improvement selection, applying manufacturing optimisation principles to prevent resource dilution whilst maintaining systematic progress.
- **Progressive Annual Loss Exposure refinement** provides increasingly accurate risk prioritisation without requiring comprehensive historical datasets, transitioning from external validation to internal evidence-based measurement.

The framework's integrated design addresses the implementation gap identified by Gordon and Loeb (2006): despite the economic validity of security investment models, organisational acceptance remains limited due to practical implementation barriers. Rather than assuming organisations can overcome these barriers through better economic analysis, the framework operates within realistic constraints whilst building credibility through demonstrated results.

4.2 Flow-Constrained Portfolio Management

Building on established manufacturing applications documented by Stadnicka et al. (2020), the framework adapts Kanban work-in-progress limitation principles to operational technology security improvement. The approach addresses cognitive biases identified by Kahneman and Tversky (1979), particularly the Planning Fallacy, where organisations systematically underestimate the time and effort required for complex tasks.

Scope Definition: The framework governs strategic security improvements requiring stakeholder coordination and oversight, distinct from routine daily operations. Strategic improvements include new security architecture implementations, control deployments, process redesigns, and technology upgrades requiring cross-functional coordination. Excluded are daily security monitoring, routine vulnerability patching, standard incident response, and regular maintenance activities.

Two-Layer Prioritisation Structure: The framework employs enterprise-wide asset prioritisation combined with asset-specific improvement selection to ensure systematic progress whilst preventing resource dilution.

- **Layer 1: Enterprise Asset Prioritisation** selects one enterprise asset (e.g., a mine, power generation station, or manufacturing facility) per quarter for focused security improvement based on Annual Loss Exposure ranking. This ensures systematic progress across the enterprise whilst preventing resource dilution across multiple assets simultaneously.
- **Layer 2: Asset-Specific Improvement Prioritisation** constrains strategic security improvements to one major improvement per quarter (completing within the quarter) plus a maximum of three minor improvements in parallel (each completing within one month). This enables up to nine minor improvements per quarter whilst maintaining work-in-progress limits that prevent resource overload.

The mathematical foundation draws on Little's Law:

$$T = W/L$$

where throughput (T) equals work-in-progress (W) divided by lead time (L). Applied to cybersecurity improvement, constraining concurrent initiatives achieves superior risk reduction compared to attempting multiple simultaneous improvements that exceed organisational capacity.

4.3 Progressive ALE Estimation Addressing Board Credibility Challenges

The framework uses Annual Loss Exposure (ALE) calculations as the primary metric for asset prioritisation and progress measurement. ALE represents the expected annual financial loss from all threats affecting a specific asset, calculated as ALE = ARO × SLE, where

Annual Rate of Occurrence (ARO) represents attack frequency and Single Loss Expectancy (SLE) represents impact magnitude (Chapple et al., 2024). Traditional ALE methodologies fail in OT environments due to executive psychology barriers and data limitations. This framework employs a progressive three-phase approach: (1) Initial ALE using insurance SLE estimates and conservative ARO baselines, (2) Validated ALE incorporating penetration testing results, and (3) Empirical ALE based on operational security control performance. Updated ARO calculations use: ARO = (Successful Incidents + Control-Prevented Attacks) / Measurement Period, where control-prevented attacks represent verified attempts stopped by non-redundant security controls.

Executive Psychology Challenge: The framework recognises that executives often distrust internal staff risk assessments due to systematic cognitive biases documented in behavioural economics research. These biases - including normalcy bias, overconfidence bias, and availability heuristic - lead to reliance on external authorities for credible evidence rather than internal security assessments.

The executive psychology challenges identified here align with systematic research on cognitive biases in complex decision-making environments (Korteling et al., 2023). Their analysis of sustainability challenges reveals similar patterns: executives systematically discount future risks, prefer maintaining current systems, and rely on external validation when facing uncertainty, precisely the challenges observed in operational technology security investment decisions.

Progressive Methodology: Rather than relying on static risk assessments, the framework employs a progressive approach where ALE accuracy improves through operational experience:

Phase 1: External Validation Foundation

- **SLE Source**: Worst-case scenario costs from insurance surveys
- **ARO Baseline**: Conservative estimates (0.1-0.5) reflecting high-impact, low-frequency nature of OT incidents
- **Purpose**: Establish a credible baseline using an external authority

Phase 2: Penetration Testing Validation

- **Reality Testing**: External penetration testing provides concrete evidence of vulnerability
- **Scenario Refinement**: Model actual operational impacts specific to demonstrated vulnerabilities
- **Executive Confidence**: External validation overcomes internal scepticism

Considering potential safety risks, penetration testing should aim to capture the management or signalling plane but not demonstrate the real harm that may result from this capture. The scenario analysis allows for a plausible estimation of such harm.

Phase 3: Empirical Performance Measurement

- **Control-Based ARO**: Measure actual attack prevention by non-redundant security controls

- **Operational Evidence**: Track successful security control activations that prevented attacks
- **Cultural Transformation**: Build internal credibility through demonstrated results

Limitations and Manual Adjustments for Critical Infrastructure: The ALE methodology acknowledges fundamental limitations when applied to critical infrastructure environments where certain consequences cannot be meaningfully quantified. Human safety impacts, environmental catastrophes, and erosion of societal trust represent categories of potential damage that resist monetary valuation (Aven, 2016). The framework incorporates a provision for manual adjustment of asset prioritisation when non-quantifiable risks significantly outweigh quantifiable ALE calculations. However, when organisational resources prove insufficient to address all assets with significant non-quantifiable risks simultaneously, the framework provides a transparent fallback to empirical ALE-based prioritisation, ensuring systematic progress within available capacity.

Due Care Documentation: The framework's systematic approach demonstrates due care - the reasonable steps an organisation takes to protect its information assets. In legal terms, due diligence is 'concerned with supplying a standard of care against which fault can be assessed,' with 'lack of due diligence giving rise to a breach of an international obligation, in the same way that negligence, or lack of reasonable care, entails a breach of a duty of care in many domestic legal systems' (Francesconi and Zanetti, 2021). Documented prioritisation processes provide legal protection against negligence claims by demonstrating that security decisions were made through defensible processes rather than arbitrary judgment.

However, relying solely on external validation creates ongoing dependency on third-party credibility and fails to address the fundamental challenge of building sustained executive confidence in internal security capabilities. While penetration testing and insurance surveys provide initial credibility, organisations must transition to empirical measurement that builds internal credibility through demonstrated results. This transition from external dependency to internal evidence represents the framework's core innovation for achieving sustainable security improvement.

4.4 Empirical Security Control Performance Measurement

The framework addresses the challenge of building sustained internal credibility by transitioning from external validation to empirical measurement based on operational security control performance. This approach not only provides concrete evidence of security improvement effectiveness but also creates the foundation for long-term cultural change within the organisation.

Control-Based ARO Measurement Methodology: In operational technology environments where security controls often lack redundancy, each successful security control activation that prevents an attack represents empirical evidence of a genuine threat attempt. The methodology distinguishes between **security events** (often noise) and **attack attempts** (security-relevant) by counting control activations that prevented successful attacks rather than the volume of security events generated.

Attack Attribution Logic: One attack campaign represents one ARO increment regardless of events generated. Multiple attack vectors may represent separate increments if different non-redundant controls stopped each vector. Only attacks stopped by sole-capable controls count toward the ARO measurement.

Example Application: When malware attempts lateral movement, simultaneous blocking by both endpoint detection and network access controls represents **redundant protection** and should **NOT** contribute to the ARO count. However, if endpoint detection alone prevents malware execution with no other capable controls, this constitutes **non-redundant protection** where the organisation was "one control failure away" from a successful incident, contributing **+1** to the empirical ARO measurement.

Post-Implementation Validation and Improvement Tracking: Following security improvements, the methodology continues measuring control-prevented attacks to demonstrate actual risk reduction. Security improvements may reduce either attack magnitude (through better containment) or frequency (through earlier detection), tracked through:

- **Enhanced Control Redundancy**: Implementing outbound NACLs alongside endpoint detection creates defence-in-depth, where malware may still be detected but cannot communicate with command servers.
- **Attack Vector Mitigation**: Email sandboxing shifts detection from endpoint to gateway level, stopping attacks earlier in the kill chain.
- **Threat Sophistication Evolution**: Attackers resort to more sophisticated techniques, demonstrating that basic vectors have been eliminated.

Progress is measured as a percentage ALE reduction:

(Baseline ALE - Current ALE) / Baseline ALE.

SLE Refinement Through Operational Impact Modelling: Updated SLE calculations incorporate scenario analysis based on penetration testing results showing actual operational impacts specific to OT systems. When penetration testing successfully demonstrates control over critical operational systems, scenario modelling estimates operational disruption duration, equipment damage costs, and production downtime costs until human intervention or automatic safety systems activate.

Conversely, when penetration testing fails to compromise OT systems following security improvements, this provides clear evidence that the asset's risk profile has been sufficiently reduced, enabling the organisation to shift improvement focus to the next highest-priority asset in the enterprise portfolio. However, to maintain vigilance against evolving threats, successfully defended assets should be enrolled in bug bounty programmes that provide early notification of newly discovered vulnerabilities. This approach ensures that if new attack vectors emerge against previously secured assets, the organisation can rapidly redirect improvement efforts back to those assets based on empirical evidence of renewed risk rather than theoretical assessments.

This dual validation approach - unsuccessful penetration testing indicating readiness to move forward, and bug bounty programmes providing ongoing surveillance for regression - resonates with agile iterative development principles of continuous feedback and adaptive prioritisation.

Progressive Credibility Enhancement and Sustainable Cultural Transformation: This systematic progression from external authoritative sources (insurance estimates) to internal evidence (penetration testing) to operational reality (empirical control performance) represents more than a measurement methodology - it creates fundamental cultural transformation within the organisation. As executives develop trust in internal security experts through consistent demonstration of measurable results, the framework achieves its ultimate goal: shifting organisational psychology from external dependency to internal confidence. When security teams can present concrete evidence of threat frequency, control effectiveness, and quantifiable risk reduction, executives gain genuine confidence in internal assessments. This cultural shift embodies the Kanban principle of "Improve Collaboratively, Evolve Experimentally" (Anderson, 2010), where a collaborative, healthy atmosphere is grounded in demonstrable, sustainable flow of successful improvements rather than theoretical promises. The resulting psychological transformation creates self-reinforcing positive feedback loops that enhance operational technology security effectiveness through improved communication, shared understanding of risks, and sustained commitment to security investment, ultimately making the framework self-sustaining rather than dependent on continued external validation.

4.5 Expert Co-Authoring Process for OT Personnel Engagement

The framework adapts the "Buy the Feature" prioritisation game from Hohmann's Innovation Games methodology (Hohmann, 2006), incorporating psychological modifications to overcome typical resistance from OT personnel, where operational availability and safety are prioritised over security concerns (Evripidou and Watson, 2024).

Expert Group Composition: For each selected asset, the expert group includes OT managers, industrial safety specialists, OT security specialists, IT specialists, and cybersecurity specialists (both HQ and asset-level), with all participants having equal voting weight regardless of hierarchy.

Improvement Identification Process:

1. **Brainstorming**: Inventory potential vulnerabilities and improvements of security controls (preventive, detective, and reactive)
2. **Decomposition**: Break improvements into the smallest components based on implementation timeframes.
    - **Minor**: Completable within one month.
    - **Major**: More than one month but within one quarter.
    - **Excluded**: Requiring more than one quarter (to maintain flow constraints).
3. **Feasibility Filtering**: Remove any remaining improvements that exceed available resource constraints or conflict with operational requirements.

Collaborative Prioritisation:

- **Voting Method**: Power-of-two cards (instead of Fibonacci) to make priority differences highly visible, creating natural transparency where significant discrepancies between individual high-priority votes and collective rankings become

readily apparent, addressing anchoring bias where initial estimates unduly influence subsequent decisions (Tversky and Kahneman, 1974).
- **Blocking Analysis**: Check for technical dependencies, resource unavailability, regulatory requirements, or budget constraints.
- **Substitution Process**: Replace blocked top-priority improvements with lower-priority alternatives fitting the same constraints.

Psychological Design for Resistance Reduction:

The process ensures each expert feels they are co-authors of the final decision rather than having security measures imposed by headquarters, addressing the not-invented-here syndrome (Katz and Allen, 1982).

Enhanced Priority Discrimination Through Power-of-Two Voting:

The framework employs power-of-two voting cards (1, 2, 4, 8, 16) rather than Fibonacci sequences to enhance priority discrimination among cybersecurity experts. The exponential progression creates sharper distinctions between importance levels compared to Fibonacci's more gradual increases (1, 2, 3, 5, 8, 13). This design addresses the cognitive challenge where security experts must differentiate between vulnerabilities with potentially similar risk profiles.

The mathematical advantage lies in the clear multiplicative relationship: each priority level represents exactly double the importance of the previous level, eliminating the ambiguous middle values present in Fibonacci sequences. This binary progression forces experts to make decisive priority judgments rather than selecting intermediate values that may mask genuine disagreement about risk severity. The resulting priority transparency enables rapid identification of consensus versus divergent expert opinions on security improvement importance.

4.6 Implementation and Progress Management

Quarterly Asset Selection: Enterprise selects the asset with the highest current ALE for focused improvement, shifting to the next highest-ALE asset following successful risk reduction.

Monthly Expert Group Reviews:

- Track quarterly initiative advancement, identify and resolve blockers
- Assess completed minor improvements and select up to three new ones (maintaining WIP limit of 3)
- Adjust priorities based on operational learning and changing threat landscape

Example Quarter Timeline:

- **Month 1**: Major improvement begins + 3 minor improvements in parallel
- **Month 2**: Major continues + assess completed minors + start 3 new minors
- **Month 3**: Major completes + assess completed minors + start final 3 minor improvements

- **Result**: 1 major + up to 9 minor improvements completed per quarter, with never more than 3 minor improvements active simultaneously

Enterprise Progress Tracking: Monitor aggregate enterprise ALE reduction quarterly, providing board-level visibility without requiring detailed technical discussions. When penetration testing becomes unsuccessful following improvements, ALE can be reduced significantly, demonstrating measurable progress.

Validation Cycle: Periodically re-run penetration testing to validate the effectiveness of the improvement. Successful defence allows ALE reduction; new vulnerabilities require updated scenario analysis and continued improvement cycles. This methodology provides executives with concrete evidence of security improvement effectiveness, addressing the sunk cost fallacy (Arkes and Blumer, 1985).

Ongoing Threat Intelligence Integration: The framework also incorporates systematic monitoring of CISA's Known Exploited Vulnerabilities (KEV) catalogue may trigger re-evaluation of previously secured assets. When CISA publishes a KEV relevant to a "good enough" asset, the organisation must carefully verify whether at least two redundant controls adequately cover the specific attack vector described in the KEV. The relatively low velocity of KEV publications (typically fewer than 10 new entries per month) allows for thorough analysis of each vulnerability without creating operational urgency, enabling methodical assessment of whether additional security improvements are warranted for previously secured assets.

This structure provides substantial improvement capacity whilst maintaining flow constraints that prevent resource dilution and coordination overhead, allowing teams to balance strategic improvements with ongoing operational security responsibilities.

4.7 Technical Implementation Considerations

Attack Attribution Methodology: The framework employs a three-tier validation process to distinguish genuine attacks from false positives in ARO calculations:

- **Tier 1: Automated Initial Classification**
  - Security controls log activation events with contextual metadata like source IP, attack vector, and payload characteristics.
  - Automated correlation engine identifies patterns consistent with known attack signatures.
  - Events failing basic plausibility checks (e.g., internal system maintenance, legitimate user behaviour) are automatically excluded.

- **Tier 2: SOC Analyst Review**
  - Human analysts examine automated classifications using established incident response procedures.
  - Evidence requirements include but are not limited to: malicious payload detection, unauthorised access attempts, exploitation of known vulnerabilities, suspicious network communications, anomalous system behaviour, or other indicators consistent with malicious intent.

  - Analysts document decision rationale and supporting evidence for audit trails.

- **Tier 3: Peer Review Validation**

  - Complex cases undergo secondary review by the SOC manager.
  - Monthly calibration sessions ensure consistency across analyst teams.
  - Disputed classifications require consensus between at least two analysts and the SOC manager.

Evidence Threshold for Attack Attribution: Sufficient evidence for attack attribution requires documented satisfaction of at least two of the following criteria (non-exhaustive list):

- **Technical Evidence:**

  - Malicious code or payload detected by endpoint security tools with confirmed threat intelligence correlation.
  - Network traffic patterns consistent with known attack frameworks (MITRE ATT&CK techniques).
  - Exploitation attempts against specific CVE-identified vulnerabilities.
  - Other technical indicators of malicious activity, as identified by security tools or analyst expertise.

- **Behavioural Evidence:**

  - Unauthorised authentication attempts exceeding normal failure thresholds.
  - Data exfiltration patterns or unusual network communications to external command infrastructure.
  - Privilege escalation attempts or lateral movement across network segments.
  - Anomalous user or system behaviour patterns indicating potential compromise.
  - Other behavioural anomalies consistent with malicious activity.

- **Contextual Evidence:**

  - Timing correlation with known threat campaigns or vulnerability disclosure timelines
  - Geographic origin consistent with active threat actor infrastructure
  - Attack vector alignment with organisation-specific threat intelligence
  - Additional contextual factors supporting malicious intent determination

  This framework remains adaptable to emerging attack vectors and novel threat techniques through regular methodology reviews and analyst training updates.

Statistical Limitations Acknowledgement:

- **Inherent Analytical Constraints:**

  - ARO calculation methodology acknowledges fundamental limitations in low-frequency, high-impact event analysis.
  - Cybersecurity events occur infrequently compared to high-volume domains, creating challenges for statistical baseline establishment.

  - Sample size limitations prevent traditional confidence interval calculations in many operational contexts.

- **Minimum Data Collection Requirements:**

  - Organisations should maintain a minimum 3-month observation period before establishing baseline estimates.
  - Initial implementation phases require extended data collection to capture sufficient event diversity.
  - Seasonal threat variations necessitate longer observation windows for trend identification.

- **Measurement Expression Guidelines:**

  - Measurements should be expressed as ranges rather than point estimates when sample sizes are insufficient.
  - Range-based reporting provides an honest representation of measurement uncertainty.
  - Documentation of confidence limitations is required when statistical thresholds cannot be met.

- **Precision vs. Practical Value Framework:**

  - The framework prioritises consistent improvement direction over precise quantification.
  - Demonstrable security enhancement trends provide more operational value than statistically precise measurements.
  - Directional improvement indicators are sufficient for strategic decision-making in resource-constrained environments.
  - Systematic comparative assessment is more valuable than absolute statistical characterisation of threat frequencies.

4.8 Implementation Experience

This framework methodology has been developed and tested through application within a global conglomerate with diverse energy, mining, and refining operations, including assets classified as critical infrastructure. The practical implementation provided insights into the effectiveness of stakeholder engagement and resource constraint management, informing the refinements presented here.

However, broader empirical validation across different industries and organisational contexts represents an important direction for future research.

5 Theoretical Analysis

5.1 Mathematical Validation

The framework integrates established mathematical principles from three domains: queuing theory, multi-criteria decision analysis, and probability theory. This section validates the mathematical coherence of these applications within the operational technology security context.

Queuing Theory Foundation

The framework applies Little's Law, which states:

$$\text{Throughput } (\text{T}) = \text{Work-in-Progress } (\text{W}) \,/\, \text{Lead Time } (\text{L})$$

This proven relationship (Little, 1961) constrains W to specific limits: one major improvement per quarter, plus a maximum of three minor improvements in parallel.

The mathematical validity depends on maintaining system stability through WIP constraints, preventing the resource contention that causes lead time degradation in unconstrained systems.

Multi-Criteria Decision Analysis Structure

The stakeholder prioritisation employs power-of-two voting (1, 2, 4, 8, 16) rather than Fibonacci sequences. The mathematical structure creates exponential separation between priority levels:

$$\text{Priority Score} = \Sigma(\text{stakeholder\_votes} \times 2\text{\textasciicircum preference\_level})$$

This weighting system ensures that high-priority consensus cannot be mathematically overridden by numerous low-priority votes, preserving expert judgment in the decision process.

Probability Theory Application

The progressive ALE methodology transitions through external estimates, validated scenarios, and empirical measurement phases.

The approach maintains probabilistic coherence while acknowledging fundamental limitations in estimating P(threat) for high-impact, low-frequency events where representative datasets do not exist.

5.2 Convergence Properties

Progressive ALE Refinement Convergence

The framework's progressive ALE methodology exhibits convergence properties through its three-phase transition from external validation to internal measurement capability, whilst acknowledging that absolute ALE reduction cannot be guaranteed due to evolving threat landscapes.

Phase 1 establishes baseline estimates using reputable insurance survey data, providing initial ALE calculations with known uncertainty bounds. These insurance-based scenarios often encompass broad operational disruptions (fires, natural disasters, equipment failures) that may be disconnected from IT/OT security specifics, typically providing more pessimistic SLE estimates than cybersecurity-specific scenarios warrant.

Phase 2 introduces penetration testing validation focused on cybersecurity vulnerabilities within the OT environment. This phase develops realistic scenario analysis based on demonstrated attack vectors and their operational impacts, typically yielding more accurate and often lower SLE estimates than broader operational disruption scenarios.

Phase 3 develops empirical measurements based on observed security control performance and actual prevented attack attempts.

Convergence emerges from replacing broad estimated parameters with cybersecurity-specific measured values. As organisations accumulate operational evidence of attack frequencies and control effectiveness, ALE calculations incorporate progressively more empirical data and fewer external estimates, typically revealing lower actual risk levels than initial insurance projections.

Critically, this convergence toward measurement accuracy does not guarantee sustained ALE reduction. New threats and vulnerabilities may emerge at a velocity exceeding an organisation's improvement capacity. The framework's value lies in ensuring focus on the highest-priority risks at any given time, rather than promising absolute risk reduction across all assets simultaneously.

Stakeholder Consensus Convergence

The expert co-authoring process demonstrates convergence properties through iterative priority refinement. Initial stakeholder voting often reveals significant disagreement, reflected in wide variance across individual priority rankings. The structured discussion process following initial voting systematically addresses the sources of disagreement.

The power-of-two voting structure makes priority differences mathematically explicit, forcing resolution of conflicting assessments rather than averaging them. Subsequent voting rounds typically show reduced variance as stakeholders converge on a shared understanding of improvement priorities and resource constraints.

Work-in-Progress Optimisation Convergence

The flow-constrained approach exhibits convergence toward optimal resource utilisation through learning effects. Organisations initially struggle with accurately estimating effort for both major and minor improvements. Over multiple quarterly cycles, estimation accuracy improves as teams develop a better understanding of actual resource requirements.

The WIP constraints prevent system overload that would mask learning signals, enabling teams to observe actual completion times and adjust planning accordingly. This creates a feedback loop where adherence to constraints facilitates improved estimation, which in turn enhances the effectiveness of future constraints.

The mathematical basis for convergence lies in bounded system behaviour: constraining concurrent work prevents the exponential complexity growth that occurs in unlimited parallel processing, maintaining system stability required for learning and optimisation.

5.3 Mathematical Limitations and Assumptions

While drawing on Little's Law ($T = W/L$), cybersecurity environments violate stability assumptions required for strict mathematical validity. In practical implementation, the arrival rate of new vulnerabilities and threats consistently exceeds the departure rate of resolved security issues, as threat discovery and sophistication typically outpace organisational remediation capacity. Rather than achieving mathematical equilibrium, the framework's value lies in allocating resources toward the highest-priority threats within this inherently unstable environment.

Similarly, whilst our progressive ALE methodology demonstrates improving measurement accuracy through operational experience, rigorous mathematical convergence proof with defined error bounds requires future theoretical analysis.

5.4 Comparative Framework Analysis

Comparison with NIST SP 800-82r3

While NIST SP 800-82r3 provides comprehensive technical guidance and control baselines, it assumes organisations can implement recommended controls across all systems simultaneously and secure dedicated security budgets through strategic planning processes.

The flow-constrained framework addresses implementation barriers that NIST SP 800-82r3 acknowledges but does not resolve. NIST explicitly recognises that OT environments are often "resource-constrained systems that do not include typical contemporary IT security capabilities" where "adding resources or features may not be possible" (Stouffer et al., 2023). The flow-constrained approach operates within these acknowledged constraints rather than assuming they can be overcome.

Where NIST provides comprehensive control catalogues, the flow-constrained framework provides systematic resource allocation and prioritisation mechanisms that enable progressive implementation of those controls within realistic organisational capacity.

Comparison with ISA/IEC 62443

ISA/IEC 62443 establishes security levels (SL-1 through SL-4) and provides detailed technical specifications for industrial automation and control systems security. The standard assumes organisations can conduct comprehensive risk assessments and implement appropriate security levels based on systematic analysis.

The flow-constrained framework complements ISA/IEC 62443 by providing a practical implementation methodology when organisations cannot address all identified security level requirements simultaneously. Rather than replacing the technical specifications of ISA/IEC 62443, the framework provides portfolio management approaches that enable systematic progression toward compliance with appropriate security levels.

Comparison with NIST SP 800-39

NIST SP 800-39 provides comprehensive guidance for organisational risk management, establishing a three-tier approach (organisational, mission/business process, and information system levels) with iterative risk management processes (National Institute of Standards and Technology, 2011). The framework assumes organisations can conduct enterprise-wide risk assessments, develop comprehensive risk management strategies, and implement coordinated responses across all organisational levels.

The flow-constrained framework addresses practical implementation challenges that NIST SP 800-39 acknowledges but does not resolve. While NIST SP 800-39 recommends "continuous monitoring" and "regular risk assessments," it provides limited guidance for resource allocation when organisations cannot implement all recommended risk responses simultaneously.

Where NIST SP 800-39 establishes the theoretical foundation for organisational risk management, the flow-constrained framework provides practical portfolio management mechanisms that enable systematic risk reduction within realistic resource constraints whilst maintaining the iterative improvement principles that NIST SP 800-39 advocates.

Implementation Feasibility Comparison

The key differentiator lies in the feasibility of implementation under real-world constraints. Existing frameworks provide technically sound guidance but require organisational capabilities that critical infrastructure operators often lack. The flow-constrained framework operates within documented constraints rather than assuming they can be overcome, enabling systematic security improvement through practical resource allocation and stakeholder engagement mechanisms.

6 Discussion

6.1 Practical Implications for Security Managers

The framework provides security managers with practical approaches to achieving security improvement within realistic organisational constraints. By working within existing budget frameworks and organisational capacity, security programmes can demonstrate measurable progress whilst building capability and stakeholder support.

The emphasis on win-win solutions that provide operational benefits alongside security improvements offers guidance for building sustainable stakeholder support. Visual management techniques provide proven approaches to communicating complex progress to non-technical stakeholders whilst maintaining transparency.

6.2 Theoretical Contributions

The research contributes novel integration of flow optimisation with cybersecurity risk management, demonstrating how manufacturing principles can enhance security portfolio management. The mathematical treatment of work-in-progress constraints provides operational research foundations for systematic security improvement under uncertainty.

The framework's integration of behavioural insights with technical analysis addresses cognitive limitations that affect security decision-making whilst maintaining analytical rigour appropriate to available data and organisational capabilities.

6.3 Limitations and Boundary Conditions

The framework's effectiveness depends on organisational maturity for collaborative decision-making and sufficient stakeholder availability for structured engagement processes. Data quality requirements for meaningful Annual Loss Exposure calculations may exceed capabilities in some operational technology environments.

Technical domain constraints may affect applicability when cybersecurity improvements cannot be meaningfully decomposed into discrete initiatives with measurable risk reduction effects. Some regulatory environments may require specific analytical rigour that conflicts with the framework's simplified approach.

6.4 Empirical Validation Limitations

The empirical validation acknowledges significant methodological limitations that constrain the generalisation of findings. The single-case embedded design, although appropriate for exploratory research in sensitive critical infrastructure environments, cannot support broad claims about the universal applicability of a framework. The participating organisation, whilst operating across diverse industrial sectors, represents a convenience sample that may not accurately reflect the full range of organisational cultures, regulatory requirements, and resource constraints encountered across different critical infrastructure operators.

The research design lacks control groups, which prevents a systematic comparison with alternative security improvement approaches. This methodological limitation means claims about the framework's relative effectiveness remain unvalidated through controlled empirical analysis. Additionally, several key success metrics rely on qualitative stakeholder feedback rather than standardised quantitative measurements, limiting reproducibility and cross-study comparison.

These limitations suggest the framework should be viewed as a promising approach requiring broader empirical validation rather than a definitively proven methodology for all critical infrastructure contexts.

6.5 Future Research Directions

Future research should examine framework adaptation across different industrial sectors and organisational contexts whilst investigating integration with threat intelligence feeds and machine learning applications. Longitudinal studies could assess framework performance over extended implementation periods whilst exploring organisational learning effects.

Investigating integration approaches with enterprise risk management systems could enhance organisational alignment whilst maintaining cybersecurity-specific analytical capabilities. Dynamic priority adjustment mechanisms could enable more responsive adaptation to changing threat conditions.

Specific research priorities include controlled comparative studies evaluating the framework against traditional security investment approaches to validate relative effectiveness claims. Multi-case studies across telecommunications, nuclear treatment, and transportation sectors would enable systematic analysis of sector-specific adaptation requirements whilst maintaining theoretical generalisability. Additionally, empirical research examining the framework's performance during actual cyber incidents would provide critical validation of the progressive ALE methodology under real-world stress conditions.

7 Conclusions

The mathematical foundation provides defensible justification for security resource allocation decisions whilst acknowledging analytical limitations that characterise operational technology environments. This practical orientation makes systematic security improvement accessible to organisations that might otherwise lack resources for sophisticated quantitative analysis.

The framework's emphasis on collaborative stakeholder engagement addresses critical implementation challenges that purely technical approaches often overlook. By involving operational personnel in security decision-making whilst providing structured analytical processes, organisations can build sustainable security programmes that gain stakeholder support rather than resistance.

The framework's successful application within a diversified conglomerate spanning energy, mining, and manufacturing operations provides reasonable confidence in its universal applicability across critical infrastructure sectors. Future implementation within the telecommunications industry will enable analysis of sector-specific adaptation requirements whilst validating the framework's cross-industry effectiveness. This planned expansion will contribute to understanding how flow-constrained approaches can enhance cybersecurity resilience across diverse critical infrastructure domains, potentially informing broader policy approaches to national infrastructure protection.

For critical infrastructure operators, the framework offers practical guidance for achieving systematic security improvement without requiring comprehensive organisational transformation or strategic investment commitments that may prove politically or financially infeasible. The approach demonstrates how operational research principles can enhance cybersecurity effectiveness whilst respecting practical constraints.

8 Declaration of Generative AI and AI-assisted Technologies in the Writing Process

During the preparation of this work, the author used Claude (Anthropic) in order to improve readability and language quality as a non-native English speaker. After using this tool, the author reviewed and edited the content as needed and takes full responsibility for the content of the publication.

9 Data Availability Statement

Due to the sensitive nature of critical infrastructure security implementation and confidentiality agreements with the participating organisation, raw data cannot be made publicly available. General implementation insights and anonymised methodological details are available from the corresponding author upon reasonable request.

10 Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

11 Declaration of Competing Interest

The author declares no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

12 References

Anderson, D.J. Kanban: Successful evolutionary change for your technology business. Sequim, WA: Blue Hole Press; 2010.

Anderson, R., Moore, T. The economics of information security. Science (American Association for the Advancement of Science) 2006;314(5799):610–3 https://doi.org/10.1126/science.1130992.

Arkes, H.R., Blumer, C. The psychology of sunk cost. Organizational Behavior and Human Decision Processes 1985;35(1):124–40 https://doi.org/10.1016/0749-5978(85)90049-4.

Aven, T. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research 2016;253(1):1–13 https://doi.org/10.1016/j.ejor.2016.03.055.

Canbek, G., Temizel, T.T., Sagiroglu, S. Gaining insights in datasets in the shade of "garbage in, garbage out" rationale: Feature space distribution fitting. WIREs Data Mining and Knowledge Discovery 2022;12(3):e1456 https://doi.org/10.1002/widm.1456.

Chapple, M., Stewart, J.M., Gibson, D. ISC2 CISSP certified information systems security professional official study guide. 10th edn ed. Chichester: Sybex; 2024.

Cook, A., Smith, R., Maglaras, L., Janicke, H. Measuring the risk of cyber attack in industrial control systems. 4th International Symposium for ICS & SCADA Cyber Security Research 2016. Swindon: BCS Learning & Development; 2016. p. 103–13. 10.14236/ewic/ics2016.12: 10.14236/ewic/ics2016.12. Available from: https://dx.doi.org/10.14236/ewic/ics2016.12.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F., et al. Cyber risk and cybersecurity: A systematic review of data availability. Geneva papers on risk and insurance Issues and practice 2022;47(3):698–736 https://doi.org/10.1057/s41288-022-00266-6.

Creswell, J.W., Plano Clark, V.L. Designing and conducting mixed methods research. 3rd ed. Thousand Oaks, California: SAGE; 2018.

Cybersecurity and Infrastructure Security Agency. Known exploited vulnerabilities catalog; n.d. Available from: https://www.cisa.gov/known-exploited-vulnerabilities-catalog. [Accessed Aug 09 2025].

Dragos. OT/ICS cybersecurity report: 8th annual year in review 2025. Hanover, MD2025. Available from: https://hub.dragos.com/hubfs/312-Year-in-Review/2025/Dragos-2025-OT-Cybersecurity-Report-A-Year-in-Review.pdf.

Evripidou, S., Watson, J.D.M. Understanding operational technology personnel's mindsets and their effect on cybersecurity perceptions: A qualitative study with operational technology cybersecurity practitioners. 2024 European Symposium on Usable Security2024. p. 137–54. 10.1145/3688459.3688472: 10.1145/3688459.3688472. Available from: https://dl.acm.org/doi/10.1145/3688459.3688472.

Francesconi, F., Zanetti, M. 'Cyber due diligence': A patchwork of protective obligations in international law. European Journal of International Law 2021;32(3):771–99 https://doi.org/10.1093/ejil/chab042.

Freeman, R.E. Strategic management: A stakeholder approach. Cambridge: Cambridge University Press; 1984.

Gordon, L.A., Loeb, M.P. Budgeting process for information security expenditures. Communications of the ACM 2006;49(1):121–5 https://doi.org/10.1145/1107458.1107465.

HM Treasury. New body to "get a grip" on infrastructure delays. GOV.UK; 2024. Available from: https://www.gov.uk/government/news/new-body-to-get-a-grip-on-infrastructure-delays.

Hohmann, L. Innovation games: Creating breakthrough products through collaborative play. Boston: Addison-Wesley Professional; 2006.

Industrial Internet Consortium. Industrial internet of things volume g4: Security framework. 2016. Available from: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf.

Iyengar, S.S., Lepper, M. When choice is demotivating: Can one desire too much of a good thing? Journal of Personality and Social Psychology 2000;79(6):995–1006 https://doi.org/10.1037/0022-3514.79.6.995.

Kahneman, D., Tversky, A. Prospect theory: An analysis of decision under risk. Econometrica 1979;47(2):263–91 https://doi.org/10.2307/1914185.

Katz, R., Allen, T.J. Investigating the not invented here (NIH) syndrome: A look at the performance, tenure, and communication patterns of 50 R&D project groups. R&D Management 1982;12(1):7–19 https://doi.org/10.1111/j.1467-9310.1982.tb00478.x.

Keep, M., Hutton, G., Lewis, S. Infrastructure in the UK. London: House of Commons Library; 2025. Available from: https://researchbriefings.files.parliament.uk/documents/SN06594/SN06594.pdf.

Korteling, J.E., Paradies, G.L., Sassen-van Meer, J.P. Cognitive bias and how to improve sustainable decision making. Frontiers in Psychology 2023;14:Article 1129835 https://doi.org/10.3389/fpsyg.2023.1129835.

Leffingwell, D. SAFe 4.5 reference guide: Scaled Agile framework for lean enterprises. Boston: Addison-Wesley Professional; 2018.

Lewis, M.W., Grimes, A.J. Metatriangulation: Building theory from multiple paradigms. Revista de administração de emprêsas 2005;45(1):72–91.

Little, J.D.C. A proof for the queuing formula: L = λw. Operations Research 1961;9(3):383–7 https://doi.org/10.1287/opre.9.3.383.

Menard, S.W. Longitudinal research. 2 ed. Thousand Oaks, Calif: Sage Publications; 2002. viii–viii p.

Morris, T. Industrial control system (ICS) cyber attack datasets. 2015. Available from: https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets.

National Cyber Security Centre. NCSC annual review 2023. London: National Cyber Security Centre; 2023. Available from: https://www.ncsc.gov.uk/pdfs/reports/Annual_Review_2023.pdf.

National Cyber Security Centre. NCSC and partners issue warning about state-sponsored cyber attackers hiding on critical infrastructure networks. London: National Cyber Security Centre; 2024. Available from: https://www.ncsc.gov.uk/pdfs/news/ncsc-and-partners-issue-warning-about-state-sponsored-cyber-attackers-hiding-on-critical-infrastructure-networks.pdf.

National Institute of Standards and Technology. NIST SP 800-39: Managing information security risk, organization, mission, and information system view. Gaithersburg, MD: U.S. Department of Commerce; 2011. Available from: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf.

Salzberger, A. The optimistic bias in cyber risk perception of german enterprises: Do organizational and personal moderators matter? Organizational Cybersecurity Journal: Practice, Process and People 2025. Available from: https://dx.doi.org/10.1108/ocj-02-2024-0003 https://doi.org/10.1108/ocj-02-2024-0003.

Schön, D.A. The reflective practitioner how professionals think in action. Abingdon, Oxon: Routledge, an imprint of the Taylor & Francis Group; 2016.

Stadnicka, D., Bonci, A., Lorenzoni, E., Dec, G., Pirani, M. Symbiotic cyber-physical Kanban 4.0: An approach for SMEs. 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)2020. p. 140–7. 10.1109/ETFA46521.2020.9212073: 10.1109/ETFA46521.2020.9212073. Available from:

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., et al. NIST SP 800-82r3: Guide to operational technology (OT) security. Gaithersburg, MD: National Institute of Standards and Technology (U.S.); 2023. 10.6028/nist.sp.800-82r3: 10.6028/nist.sp.800-82r3. Available from: https://dx.doi.org/10.6028/nist.sp.800-82r3.

Tversky, A., Kahneman, D. Judgment under uncertainty: Heuristics and biases. Science 1974;185(4157):1124–31 https://doi.org/10.1126/science.185.4157.1124.

Wang, J., Neil, M., Fenton, N. A bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. Computers & Security 2020;89:101659. Available from: https://dx.doi.org/10.1016/j.cose.2019.101659 https://doi.org/10.1016/j.cose.2019.101659.

Wang, Y. Multi-criteria optimization for cybersecurity investment planning in industrial control systems. Computers & Chemical Engineering 2019;126:224–37 https://doi.org/10.1016/j.compchemeng.2019.04.018.

Yin, R.K. Case study research and applications: Design and methods. Sixth edition. ed. Los Angeles: SAGE; 2018.

Vitae

Vsevolod Shabad, CISSP, CCSP, is a Principal Enterprise Architect at BT Group and a Fellow of BCS, The Chartered Institute for IT. He holds an MEng in Applied Mathematics and a PGDip in Information Security, and is currently pursuing an MSc in Cybersecurity at the University of Liverpool. His research interests include enterprise architecture, operational technology security, and risk-driven decision-making in critical infrastructure.