From Crisis to Control - A Retrospective Enterprise Architecture Analysis of Cybersecurity Transformation

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

Purpose: This study analyses the cybersecurity transformation of a large regulated financial institution in Kazakhstan during 2021, applying a retrospective enterprise architecture (EA) perspective - viewed through the updated 2025 EA lens - to evaluate strategic, operational, and human-factor changes.

Design/methodology/approach: Using a case study approach, the analysis integrates incident management metrics, regulatory requirements, and EA frameworks, supported by internal operational data and external literature.

Findings: Over a five-month transformation period, incident resolution times improved dramatically, with the 90th percentile reduced from near the 30-day internal compliance limit to one day. This was achieved through a Kanban-based operational redesign, expanded analyst capabilities, and clearer separation of incident and problem management. Stakeholder confidence improved, though challenges with informal expectations and workload balance persisted.

Practical implications: The findings demonstrate how EA principles can be applied in highly regulated operational contexts to balance rapid tactical response with sustained strategic improvement.

Originality: This study contributes to integrating operational practice with EA theory in the cybersecurity domain, analysed through the updated 2025 EA lens. The four-year gap between the transformation and this retrospective analysis helped to minimise researcher bias, allowing for a more objective evaluation of outcomes. It offers a replicable framework for systematic security improvement in regulated industries, tested in a challenging regulatory environment, and grounded in proven techniques that balance tactical agility with strategic capability development.

Keywords: Enterprise architecture; Cybersecurity operations; Kanban; Incident management; Security operations centre; Regulated industry; Workflow optimisation; Process improvement; Cognitive bias; Value streams

Introduction: Practical Implementation Guide

In early 2021, a security operations centre (SOC) at one of Kazakhstan's large banks faced escalating incident resolution times, approaching a critical 30-day constraint. This deadline was not directly regulatory but emerged from internal compliance operational requirements. Typical payment card dispute resolution procedures required customer complaints to be investigated and resolved within thirty calendar days - see, for example, Halyk Bank Kazakhstan (2022, Section 13.3, 30 days from complaint receipt) or Kaspi Bank (2024, Section 50, 30 days from the transaction date). The compliance team needed assurance that cybersecurity investigations would be completed within this timeframe as standard practice. This enabled the compliance team to rely on comprehensive cybersecurity findings when responding to customer disputes, regardless of whether specific incidents were initially suspected to be cyber-related.

The timing was particularly challenging, as Kazakhstan's banking sector faced unprecedented pressure for digital transformation following the COVID-19 pandemic. The National Bank of Kazakhstan reported that non-cash card transactions in the first half of 2021 were 2.5 times higher than the same period in 2020, whilst their total value was 2.3 times greater (National Bank of Kazakhstan, 2021). This surge in digital payments occurred alongside increasingly demanding cybersecurity regulatory requirements Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market (2021, Resolution No. 48 as amended by No. 34, 2021), creating operational pressure as complex cybersecurity incidents approached the 30-day limit imposed by the compliance team.

The deteriorating performance shown in Figure 1 below (January-February 2021) created urgent pressure that drove the March 2021 transformation initiative. Five months later, the organisation consistently resolved 90% of cyber incidents within one day whilst maintaining quality and stakeholder satisfaction. This dramatic improvement came not from new technology or additional staff, but from systematically implementing Kanban workflow management principles that inadvertently aligned with enterprise architecture best practices.

Research Objectives:

- Analyse how the Kanban methodology inadvertently implemented enterprise architecture principles in cybersecurity operations within the banking sector’s constraints.
- Examine the role of cognitive biases in the design of operational processes.
- Offer practical guidance for security leaders navigating similar workflow challenges in the financial services sector.
- Demonstrate the connection between operational excellence and strategic business outcomes in regulated environments.

Research Contribution: This study provides tested solutions based on actual implementation in a challenging regulatory environment, with clear explanations of underlying principles that enable adaptation to different organisational contexts. The integration of operational practice with enterprise architecture theory provides a replicable framework for systematic security improvement in regulated industries, offering actionable insights for both practitioners and academics, and aligning with the journal's focus on practical applications in cybersecurity operations.

Literature Review

Enterprise Architecture and Value Stream Design

Enterprise architecture provides systematic approaches to connecting business strategy with operational execution (Kotter, 1996). In terms of ArchiMate (The Open Group, 2022), effective architecture requires alignment between the business layer (regulatory compliance, stakeholder value and analyst roles/capabilities), the application layer (incident-management systems and other application services that support the SOC process), and the technology layer (platforms and infrastructure that host and run these applications and controls, including identity and access enforcement).

Value stream design principles emphasise end-to-end flow optimisation rather than local functional efficiency. The disconnection between these layers creates organisational inefficiencies that fragment value delivery across departmental boundaries rather than flowing continuously toward customer value realisation. Enterprise architecture frameworks should address layer alignment to prevent fragmentation and ensure value streams run smoothly from end to end.

Kanban Methodology in Operational Contexts

Anderson (2010) Kanban methodology emphasises evolutionary change through visualising work, limiting work-in-progress, and managing flow. The STATIK (Systems Thinking Approach to Introducing Kanban) methodology offers a systematic approach to understanding demand patterns and stakeholder requirements before implementing process changes. Work-in-progress limits function as architectural constraints that force alignment between capacity and demand, creating productive tension that drives innovation rather than accepting delays.

Organisational Change and Motivation Theory

Pink (2010) identifies three pillars of intrinsic motivation: autonomy, mastery, and purpose. Kotter (1996) describes classic organisational change failures as attempting technological solutions without addressing underlying structural and cultural barriers. Heath & Heath (2010) identify directing the rider (clear process), motivating the elephant (intrinsic motivation), and shaping the path (systematic constraints) as critical elements of successful change. The absence of these elements creates what Meadows (2008) are identified as leverage points in system design that treat symptoms rather than changing system structure and paradigm.

Cognitive Bias and Process Design

Kahneman & Tversky (1979) describe loss aversion behaviour where teams become increasingly risk-averse about process changes due to fear of negative outcomes. Tversky & Kahneman (1974) identify the availability heuristic where decision-makers overweight vivid, recent information whilst underestimating the cumulative impact of routine activities. These cognitive biases require what behavioural economists call "choice architecture" – a systematic design that makes beneficial decisions easier and harmful decisions more difficult (Thaler & Sunstein, 2008).

Site Reliability Engineering and Measurement

Beyer et al. (2016) establish Site Reliability Engineering principles that separate different service capabilities with distinct Service Level Indicators (SLI), Service Level Objectives (SLO), and Service Level Agreements (SLA). This approach enables different measurement and improvement cycles aligned with different strategic time horizons, preventing the conflation of urgent operational restoration with important strategic improvement activities.

Research Methodology

Research Approach and Framework

This study employs a retrospective case study methodology examining a cybersecurity transformation in Kazakhstan's banking sector during 2021. The research applies a dual-perspective analytical framework, combining the practical implementation experience with theoretical enterprise architecture analysis conducted using contemporary EA frameworks and professional knowledge acquired subsequently.

The dual-perspective approach leverages the author's professional development as an enterprise architect following the 2021 implementation and access to evolved EA frameworks, particularly ArchiMate 3.2 (The Open Group, 2022) and contemporary value stream design principles. During the 2021 transformation, the team operated from operational necessity without formal EA frameworks or theoretical guidance. The retrospective analysis applies systematic EA principles - including layer alignment, value stream mapping, and constraint-based governance - that provide a theoretical understanding of why certain operational interventions succeeded whilst others required adjustment.

This methodology addresses the challenge that operational practitioners often lack theoretical frameworks to understand why certain interventions succeed, whilst enterprise architecture theory may lack concrete implementation examples. The approach enables examination of how operational necessity can inadvertently align with EA principles, providing both practical implementation guidance and theoretical validation of EA frameworks in operational contexts.

Data Sources and Limitations

The analysis draws from systematic measurement data collected from January 2021 onwards, including baseline performance metrics that demonstrated the need for intervention and subsequent transformation outcomes through September 2021. The collected data included incident resolution metrics, workflow analysis, and team performance indicators. The retrospective analysis applies enterprise architecture frameworks, motivation theory, and cognitive psychology literature to understand the underlying success factors that were invisible during the 2021 implementation.

The single case study approach limits generalisability, though the regulatory environment and digital transformation pressures are common across financial services globally. The retrospective analysis benefits from temporal distance but may be subject to hindsight bias. The dual-perspective methodology aims to mitigate this limitation by clearly separating contemporary understanding from theoretical retrospection.

Researcher Bias and Limitations

The analysis acknowledges potential researcher bias inherent in the dual role of practitioner and retrospective analyst. The author was directly involved in the 2021 transformation as a security operations practitioner, which provides insider access to implementation details but may introduce subjective interpretation of events and outcomes.

To mitigate this bias, the study relies primarily on systematic measurement data collected during the transformation period rather than subjective recollections. The retrospective enterprise architecture analysis is conducted using established theoretical frameworks applied independently of the original implementation experience. Where practitioner insights inform the analysis, these are explicitly identified and clearly distinguished from objective measurement data and theoretical interpretation. The four-year temporal separation between implementation (2021) and analysis (2025) provides additional distance that helps distinguish between immediate operational concerns and broader architectural insights. The systematic measurement approach and established theoretical frameworks provide an objective analytical structure that helps separate empirical findings from subjective interpretation, ensuring academic rigour whilst leveraging practitioner insights.

The single case study approach and retrospective methodology limits generalisability, though the regulatory environment and operational pressures examined are representative of financial services globally.

Case Context and Background

Organisational and Regulatory Setting

The SOC operated within Kazakhstan's banking sector during a period of accelerated digital transformation following the COVID-19 pandemic. Enhanced regulatory oversight requirements (Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market, 2021) mandated not only incident notification but comprehensive investigation reports, root cause analysis, and remediation evidence within prescribed timeframes. Complex cybersecurity incidents were approaching the 30-day internal compliance limit, broadly comparable to a service-level commitment, creating cascading pressure: compliance risks, operational stress, and mounting stakeholder urgency that threatened organisational stability.

Initial Operational Challenges and Stakeholder Analysis

The SOC operated with a traditional two-tier analyst model where L1 analysts handled simple cases and escalated complex incidents to L2 specialists. However, the L2 team had become the constraining factor in the system. While L1 analysts could resolve straightforward incidents efficiently, they lacked the knowledge and access rights to handle complex cases, forcing escalation to an overburdened L2 team whose high individual expertise could not overcome the systematic capacity constraint. This created a systematic bottleneck where complex incidents would queue for L2 attention, with waiting time often consuming more days than the actual investigation and resolution work.

The STATIK stakeholder mapping focused on understanding actual consumption patterns rather than established practices. Business units required immediate confirmation of containment and system safety status within hours, as well as comprehensive impact analysis and preventive measures within weeks. Compliance teams needed evidence that appropriate response procedures had been followed according to internal compliance requirements within the 30-day deadline. Legal teams needed sufficient documentation for potential law enforcement cooperation immediately, but a comprehensive forensics analysis could be delivered later. IT teams needed immediate confirmation of containment and tactical remediation guidance to restore service availability within hours. These represented distinct service level objectives rather than conflicting requirements.

Case Analysis

Kanban Implementation and Process Redesign

Process Mapping and Demand Analysis: The stakeholder analysis deliberately followed the STATIK methodology Anderson (2010). The critical finding was that stakeholders required both tactical and strategic information, but with fundamentally different timeframes and Service Level Objectives (SLOs). L1 analysts were spending considerable time on root cause analysis activities during active incident response, when stakeholders actually needed this strategic analysis delivered through different SLOs in the problem management timeframe. This conflated two distinct activities that ITIL 4 best practices recommend separating: incident management (restoring service quickly) and problem management (identifying and eliminating root causes of incidents) AXELOS (2019). The transformation implemented this separation, enabling L1 analysts to close incidents rapidly once immediate threats were contained and systems were restored, regardless of whether comprehensive root cause analysis was complete.

Most significantly, L2 teams were running advanced forensics investigations that were not actually in demand by subsequent pieces of the value stream chain. In many cases, L1 analysts could identify incidents involving the exploitation of known vulnerabilities that remained in the security improvement backlog due to organisational resource constraints. Although the root cause was evident and well-documented, established internal practices still required comprehensive forensic reports from L2 specialists. L2 specialists would spend days conducting exhaustive digital forensics and attack vector reconstruction that consumed significant time, whilst downstream stakeholders actually required only basic impact assessment and remediation guidance to proceed with their decision-making processes.

The timing analysis revealed that the L2 bottleneck was not primarily caused by the duration of forensic investigations themselves, but by queue waiting times. Whilst L2 specialists might complete their analysis within hours or days, incidents would often wait weeks in the L2 queue before receiving attention. This created a systematic bottleneck where the constraint was L2 capacity allocation rather than L2 technical capability. The cross-functional team approach eliminated this queuing delay by enabling L1 analysts to handle complex incidents directly, supported by L2 expertise when needed, rather than forcing all complex cases through the L2 queue. This shift was supported by expanding L1 analysts' system access rights and providing targeted skills development, enabling them to participate in complex investigations as part of cross-functional incident teams in line with Kanban principles.

This created a counterintuitive but powerful dynamic: despite L1 analysts being significantly less skilled than L2 specialists and requiring considerably more time to complete complex analysis, the overall incident resolution time was dramatically faster. An L1 analyst might spend several hours investigating an incident that an L2 specialist could resolve in 30 minutes. Still, since the L1 analyst could begin quite immediately, whilst the L2 queue had weeks of waiting time, the end-to-end flow time was substantially reduced. This demonstrated a fundamental systems thinking principle: optimising flow is more important than optimising individual efficiency when bottlenecks exist in the system.

Cross-functional Teams and WIP Limits: The cross-functional approach reflected Hackman (2002) research on high-performing teams that combine diverse expertise with clear shared objectives. Instead of maintaining separate L1 and L2 teams with rigid boundaries, flexible incident response teams are formed around specific incidents based on complexity and stakeholder requirements. Each of these informal teams combined L1 investigative capacity, L2 technical expertise, and business stakeholder representation appropriate to the incident's potential impact.

WIP limits forced difficult prioritisation conversations that had previously been avoided. When teams could only work on a limited number of incidents simultaneously, they had to make explicit trade-offs between regulatory urgency, business impact, and technical complexity. The implementation of separate Definition-of-Done (DoD) criteria for incident management and problem management enabled L1 analysts to close incidents rapidly once immediate threats were contained and systems were restored, regardless of whether comprehensive root cause analysis was complete.

Systematic Measurement Implementation: The measurement system moved beyond simple throughput metrics to flow-based metrics that provided transparent and valuable information for stakeholders, whilst being challenging to manipulate. The key breakthrough was implementing 90th percentile incident resolution time as the primary performance indicator, which proved to be the most fair and transparent metric for stakeholders, whilst being difficult to cheat compared to easily manipulated measures like "incidents closed per day."

All incidents were processed through the same class and the same queue for incident management, ensuring consistent response times and avoiding the complexity of classification decisions during time-critical response activities. Although regulatory requirements No. 48 Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market (2021) mandated detailed incident attribution and categorisation for reporting purposes - including comprehensive analysis of attack vectors, affected systems, and damage assessment - this regulatory classification did not influence the operational class of service or response priorities. A detailed forensic analysis, required for regulatory compliance, was performed separately from the operational incident response process, ensuring that regulatory requirements did not impact restoration times.

After achieving the fastest possible containment and restoration, incidents were placed into a separate problem management queue for subsequent grouping and analysis, including the detailed regulatory reporting requirements.

Critical Incident Analysis: Cognitive Bias and Process Deviation

The September 2nd issue: The transformation started in March 2021, and by early September - about five months later - stakeholders were used to seeing steady improvements in how quickly incidents were resolved. On 2nd September, the weekly review showed a sharp rise in the cybersecurity incident SLI. The formal internal compliance limit of 30 days was still met; however, because resolution times had been significantly faster for months, we had agreed on a shorter, informal SLO with stakeholders. This new expectation was missed, which caused disappointment even though we stayed within the formal limit. The spike happened because a technically interesting incident came up the week before. With the regular workload being heavy, this unusual case caught the attention of many SOC analysts. Using their new freedom and encouraged teamwork, several analysts chose to work together on this single case for two days instead of following the oldest-first policy for the queue.

As expected, while too many people focused on the new case, older incidents waited, and overall progress slowed down. This showed that well-meant changes - like more freedom, teamwork, and pull-based work - can cause problems when people understand HOW to follow the process but not WHY certain rules are in place. More importantly, the 2nd September spike broke the informal SLO and shook stakeholder confidence in the improvement trend.

Cognitive Bias Analysis: The September 2nd incident exemplified (Tversky & Kahneman, 1974) availability heuristic - SOC analysts overestimated the importance of the vivid, new incident whilst underestimating the cumulative impact of delayed routine incidents. The incident demonstrated what behavioural economists recognise as novelty bias, where decision-makers systematically overweight new or unusual information relative to routine but important baseline activities (Kahneman, 2011).

The planning fallacy (Kahneman & Tversky, 1979) compounded the availability heuristic as analysts consistently underestimated the time required for comprehensive analysis, whilst overestimating their ability to simultaneously manage multiple incidents effectively. From a systems thinking perspective, the bias represented what (Senge, 1993) was identified as "fixing that fails" - interventions that address symptoms whilst creating unintended consequences that worsen overall system performance.

Enterprise Architecture Retrospective Analysis

Architectural Layer Disconnection: From the enterprise architecture perspective, informed by formal EA training and ArchiMate 3.2 framework, the 2021 problems represented classic architectural anti-patterns that disconnected business strategy from operational execution.

The L1-L2 escalation model created what enterprise architects recognise as a "handoff anti-pattern" - value streams were artificially fragmented across organisational boundaries rather than flowing end-to-end from incident detection to resolution.

The missing enterprise architecture perspective meant that capabilities were defined by organisational hierarchy rather than value delivery requirements. L1 analysts possessed the time and motivation to develop deeper investigation skills, but organisational design prevented this capability development. Meanwhile, L2 specialists became a shared service bottleneck, violating the architectural principle that critical path activities should have dedicated capacity.

Inadvertent Architectural Coherence: The Kanban implementation succeeded because it accidentally addressed fundamental layer disconnections that had been invisible to operational management. The visual board created what enterprise architects call "value stream transparency" - making work flow visible across organisational boundaries and enabling end-to-end optimisation rather than local optimisation.

WIP limits served as architectural constraints, aligning available platform/infrastructure capacity (technology layer) with operational demand (business layer). This represented an architectural shift from hierarchical capability design to flow-based capability design, where skills were developed in response to value delivery requirements rather than organisational structure.

Findings and Discussion

Performance Improvements and Strategic Value

The transformation delivered measurable improvements across all key performance indicators. The 90th percentile incident resolution time improved from approaching the 30-day internal compliance deadline to consistently achieving resolution within one day for 90% of incidents. This dramatic improvement represented a 30x performance enhancement that exceeded initial expectations and demonstrated the power of systematic flow optimisation over resource-based approaches.

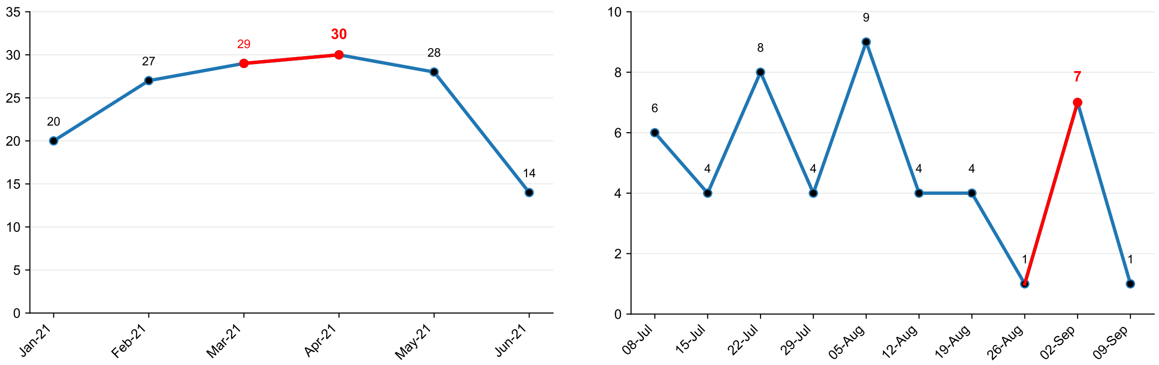

Figure 1. 90th percentile incident resolution times (in days) for all cybersecurity incidents handled by SOC between January and mid-September 2021. The left panel shows monthly measurements used in the initial analysis phase (Jan-Jun 2021); the right panel shows weekly measurements introduced from July 2021 as part of the operational redesign. The Kanban-

based transformation began in March 2021, with an initial rise in April reflecting process inertia, followed by a sharp and sustained decrease in resolution times as the new approach took effect. The deteriorating trend in January-February 2021 provided the catalyst for the March transformation initiative

Regulatory compliance became consistently achievable without overtime or emergency measures. The separation of incident management and problem management eliminated the time pressure that had previously forced teams into unsustainable heroic efforts to meet compliance deadlines. Most significantly, the systematic measurement revealed consistent performance rather than sporadic heroic achievements.

The transformation's most significant achievement was establishing a direct line of sight between daily technical work and strategic business outcomes. The systematic approach demonstrated that security operations could be predictable and measurable rather than heroic and unpredictable. This shift enabled security teams to participate in business planning processes as reliable capability providers rather than unpredictable cost centres.

Enterprise Architecture and Human Factors Insights

The transformation succeeded because it addressed what Heath & Heath (2010) identify as the three critical elements of change: directing the rider (clear process), motivating the elephant (intrinsic motivation), and shaping the path (systematic constraints). However, the deeper success factors align with enterprise architecture principles that connect business strategy with operational execution.

The separation of incident and problem management addressed the lack of proper temporal architecture design - ensuring that the architectural layers (business, application, technology) are synchronised for different time horizons and relevant short-term and long-term objectives.

The team exhibited symptoms of what Pink (2010) identifies as motivation improvements: autonomy through transparency into work priorities, mastery through capability development opportunities, and purpose through connection between daily incident work and business outcomes. The elimination of obviously wasted work had a dramatic impact on team dynamics, with positive atmosphere, increased creativity, and improved individual performance.

Bias-Resistant Process Design Principles

The September 2nd issue revealed fundamental principles for designing bias-resistant operational systems. The oldest-first policy represented what enterprise architects call "constraint-based governance" - systematic rules that prevent local optimisation from degrading system performance. However, the policy implementation failed because it relied on individual discipline rather than systematic enforcement mechanisms.

Enterprise architecture principles for bias-resistant systems require what behavioural economists call "choice architecture" - systematic design that makes beneficial decisions easier and harmful decisions more difficult. The incident demonstrated the need for what enterprise architects recognise as "cognitive load management" in operational processes, requiring systematic constraints that maintain flow performance regardless of individual decision-making quality during high-stress situations.

Implications for Practice

Guidance for Security Leaders

Security leaders facing similar challenges should recognise that organisational change is fundamentally about psychological transitions, not just process modifications. The critical lesson is distinguishing between **education** (HOW to follow processes) and **awareness** (WHY processes matter for business outcomes). Teams require an understanding of flow principles and business impact before they can effectively exercise autonomy within systematic constraints.

Implementation should begin with systematic measurement that reveals current performance patterns before attempting process changes. The 90th percentile approach provides transparent, manipulation-resistant metrics that create accountability whilst avoiding the gaming behaviours that simple throughput metrics encourage. Most importantly, security leaders must recognise that sustainable improvement requires addressing human factors and cognitive biases through process design rather than assuming that policy compliance will overcome psychological tendencies.

Enterprise Architecture Integration Opportunities

Enterprise architects should recognise security operations as a critical business capability that requires systematic design principles rather than ad-hoc operational approaches. The retrospective analysis demonstrates that security operations benefit from the same architectural thinking applied to other business capabilities: clear value stream design, appropriate Service Level Objectives for different business outcomes, and systematic measurement that connects operational performance to business value delivery.

The separation of incident and problem management exemplifies the enterprise architecture principle of temporal capability design - different business capabilities optimised for different time horizons and success criteria. Current EA practitioners can apply value stream mapping techniques to security operations, identifying waste in handoffs between functional silos and implementing flow-based organisation design that optimises for business outcome delivery rather than functional efficiency.

The transformation demonstrates significant opportunities for integrating enterprise architecture thinking into security operations design. Enterprise architects can provide systematic approaches to understanding demand patterns through STATIK methodology, ensuring that security capabilities are right-sized according to business consumption rather than technical capability. Most significantly, enterprise architecture principles of systematic measurement and continuous improvement provide frameworks for security operations maturity that go beyond compliance checklists to create sustainable competitive advantage through operational excellence.

Conclusion

Research Contributions and Broader Implications

This retrospective analysis validates the principle that understanding purpose before method - starting with WHY rather than HOW - creates more sustainable organisational change. The transformation succeeded because it inadvertently addressed fundamental enterprise architecture principles that connected business strategy with operational execution, demonstrating that operational necessity can force adherence to systematic design principles even when theoretical frameworks are not explicitly applied.

The dual-perspective approach reveals patterns that are invisible from either viewpoint alone. The integration of operational practice with enterprise architecture theory provides actionable insights for both operational leaders facing immediate challenges and enterprise architects designing systematic capability improvements.

The transformation demonstrates that enterprise architecture principles provide powerful analytical frameworks for understanding operational success beyond specific methodologies or technologies. The systematic approach to value stream design, constraint management, and measurement-driven improvement creates replicable frameworks for operational excellence that transcend individual technical domains.

Future Research Directions

Most significantly, the retrospective reveals that sustainable operational improvement requires addressing human factors and cognitive biases through systematic design rather than assuming that process compliance will overcome psychological tendencies. Enterprise architecture thinking provides frameworks for bias-resistant system design that account for predictable human behaviour patterns whilst maintaining operational effectiveness.

Future research should explore the systematic application of enterprise architecture principles to other operational domains, particularly investigating how temporal capability design principles can address the common pattern of forcing strategic analysis into tactical timeframes. Additionally, research into bias-resistant process design could provide systematic approaches to operational improvement that account for cognitive limitations whilst supporting human autonomy and creativity within systematic constraints.

The integration of EA principles with operational security provides a model for other technical domains facing similar challenges of connecting technical excellence with business value delivery through systematic, sustainable approaches to organisational capability development.

References

Agency of the Republic of Kazakhstan for Regulation and Development of the Financial Market (2021) "On approval of the Requirements for ensuring information security of banks, branches of non-resident banks of the Republic of Kazakhstan, and organisations conducting certain types of banking operations, rules and terms for providing information on information security Incidents, including data on violations and failures in information systems" Resolution No. 48 dated March 27, 2018; as amended by Resolution No. 34 dated February 17, 2021, available at: https://adilet.zan.kz/rus/archive/docs/V1800016772/17.02.2021 [Accessed 12 Aug 2025].

Anderson, D. J. (2010) Kanban: Successful evolutionary change for your technology business. Sequim, WA, USA, Blue Hole Press. ISBN: 978-0-9845214-0-1.

AXELOS (2019) ITIL® Foundation: ITIL 4 Edition. Norwich, UK, The Stationery Office Ltd. ISBN: 9780113316076.

Beyer, B., Jones, C., Petoff, J. & Murphy, N. R. (2016) Site reliability engineering: how Google runs production systems. Beijing, China, O'Reilly. ISBN: 149192912X.

Hackman, J. R. (2002) Leading Teams: Setting the Stage for Great Performances. Boston, MA, USA, Harvard Business Review Press. ISBN: 978-1578512331.

Halyk Bank Kazakhstan (2022) "Rules for Using Bank Cards (Halyk Bank Kazakhstan)", available at: https://halykbank.kz/storage/app/media/Card/RUS_pravila_card.pdf [Accessed 12 Aug 2025].

Heath, C. & Heath, D. (2010) Switch: How to Change Things When Change Is Hard. New York, NY, USA, Crown Business. ISBN: 978-0385528757.

Kahneman, D. (2011) Thinking, Fast and Slow. New York, NY, USA, Farrar, Straus and Giroux. ISBN: 9780141918921.

Kahneman, D. & Tversky, A. (1979) Prospect theory: An analysis of decision under risk. *Econometrica*. 47 (2), 263–291. doi: 10.2307/1914185.

Kaspi Bank (2024) "Rules for issuance, distribution and servicing of prepaid payment cards', Kaspi.kz", available at: https://guide.kaspi.kz/client/ru/gold/documents/pravila_vypuska_pasprostraneniya_i_obslujivaniya_platejnoi_karty_2024 [Accessed 12 Aug 2025].

Kotter, J. P. (1996) Leading change. Boston, MA, USA, Harvard Business School Press. ISBN: 0875847471.

Meadows, D. H. (2008) Leverage Points - Places to Intervene in a System. White River Junction, VT, USA, Chelsea Green Publishing. ISBN: 978-1-60358-055-7.

National Bank of Kazakhstan (2021) *Residents of Kazakhstan Conducted 2.6 Billion Cashless Transactions in H1 2021*. https://nationalbank.kz/en/news/informacionnye-soobshcheniya/11915. [Accessed 12 Aug 2025]

Pink, D. H. (2010) Drive the surprising truth about what motivates us. Edinburgh, UK, Canongate. ISBN: 1-84767-888-2.

Senge, P. M. (1993) The fifth discipline: the art and practice of the learning organization. London, UK, Century. ISBN: 1-4070-6000-7.

Thaler, R. H. & Sunstein, C. R. (2008) Nudge: Improving Decisions About Health, Wealth, and Happiness. New Haven, CT, USA, Yale University Press. ISBN: 9780300122237.

The Open Group (2022) *ArchiMate® 3.2 Specification*. https://publications.opengroup.org/standards/archimate/specifications/c226 [Accessed 14 Aug].

Tversky, A. & Kahneman, D. (1974) Judgment under uncertainty: Heuristics and biases. *Science*. 185 (4157), 1124–1131. doi: 10.1126/science.185.4157.1124.

Adilet.zan.kz is the official legal information system of the Republic of Kazakhstan, maintained by the Ministry of Justice.

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

During the preparation of this manuscript, the author used Claude Sonnet 4.0 (Anthropic) exclusively for grammar correction and language refinement as a non-native English speaker, in accordance with Emerald's policy permitting copy-editing with AI tools. The tool was not used for content generation, analysis, research design, or conceptual development. All research methodology, findings, and intellectual contributions are the sole work of the author, who has reviewed all content and accepts full responsibility for its accuracy and integrity.