

Jorge DeCossio

Applied Project

In fulfillment of the requirements for the
Doctor of Professional Practice in Global Leadership and Management
program

**Thunderbird School of Global Management
at Arizona State University**

Fall 2026

AI AND HUMAN TEAMS

Strategic Deployment of an AI-Based Network Operations Center (AI-NOC)
in a Public Higher Education Institution

A Strategic Implementation Report

Submitted by

Jorge De Cossio

Supervisory Committee

Charla Griffy-Brown, PhD

Chair

Marco Serrato, PhD

Co-Chair

Doctorate in Professional Practice in Global Leadership and Management

Thunderbird School of Global Management · Arizona State University

June 2026

Table of Contents

Cover Page.....	1
Table of Contents	2
Executive Abstract	6
1. Introduction: Strategic Context, Scope, and Central Research Question.....	8
1.1 The Digital Infrastructure Imperative in Higher Education.....	8
1.2 The Strategic Problem: Scaling Reliability Without Scaling Headcount	8
1.3 Scope of This Report	9
AI-NOC Implementation Status — What Is Live, Piloted, Pending, and Projected	10
1.4 Alignment to ASU's Institutional Mission and Digital Strategy	10
1.5 Strategic Goals and Objectives: Mission Alignment	11
1.6 The Integrated Research Question	13
1.7 Transferable Significance: A Model Beyond ASU	14
2. Methodology	16
2.1 Research Design: Quasi-Experimental Pre/Post Evaluation.....	16
Theoretical Framework.....	16
2.2 Quantitative Data: Operational Performance Metrics	17
2.3 Qualitative Data: Workforce Trust, Agency, and Adoption	18
2.4 Comparative Benchmarking: ANNA and NetBrain.....	21
2.5 Analytical Framework: Evidence to Insight to Recommendation.....	22
2.6 Limitations and Boundary Conditions	23
Threats to Validity.....	23
3. Implementation Plan	25
3.1 Governing Design Principles	26
Why This Implementation Model?.....	27
What If the Plan Fails? Critical Failure Scenarios	28
3.2 Decision Gate Architecture	29
3.3 Implementation Timeline	30
3.4 Phase 1: Assessment and Readiness (Months 1–2).....	32
Overview	32
Key Activities, Owners, and Data Requirements.....	32
Phase Deliverable and Gate 1 Criteria	33
3.5 Phase 2: Technology Acquisition (Months 2–4)	33

Overview	33
Key Activities, Owners, and Data Requirements	34
Phase Deliverable and Gate 2 Criteria	35
3.6 Phase 3: Pilot Deployment (Months 4–7) — Critical Gate.....	35
Overview	35
Key Activities, Owners, and Data Requirements	36
Gate 3 Criteria — The Critical Threshold	37
3.7 Phase 4: Full Deployment (Months 7–10).....	38
Overview	38
Key Activities and Escalation Protocol Redesign	38
3.8 Phase 5: Training and Change Management (Months 6–10, Parallel)	39
Overview	39
Training Program Structure	40
3.9 Phase 6: Continuous Evaluation and Optimization (Month 10+, Ongoing)	41
Overview	41
Continuous Governance System	42
3.10 AI-NOC System Architecture: Event Flow, Decision Authority, and Governance	43
3.11 Resource Requirements and Budget Framework	45
 4. Challenges and Risks: A Continuous Risk Governance System	 47
4.1 Risk Landscape Overview: Five Domains.....	47
Technical Risk Domain	48
Cultural Risk Domain	48
Security and Compliance Risk Domain	49
Financial Risk Domain	49
Organizational and Governance Risk Domain	49
4.2 Risk Heatmap: Initiative Risk Profile	50
4.3 Risk Register: 14 Identified Risks	51
4.4 The Continuous Risk Governance System: Monitoring Cadence and Ownership	58
4.5 Risk Response Protocols: Six Priority Scenarios	61
4.6 Risk Governance Integration: Feedback Loops and Institutional Learning	65
4.7 Alignment with Institutional and National AI Governance Standards.....	66
 5. Success Stories and Case Studies: AI-NOC and the Evidence of Value Creation	 68
5.1 Evaluation Design: How We Know What We Know	69
5.2 Quantitative Performance: Before and After	70
5.3 Qualitative Evidence: Staff Perception, Trust, and Agency.....	74
5.3a Staff Perception Survey Results	74
5.3b Focus Group Findings: Four Emergent Themes	77
5.3c Two Representative Cases: ANNA in Action	79
5.4 Comparative Benchmark: ANNA and NetBrain	80
5.5 Evidence of Value Creation: Six Dimensions.....	86
5.6 Limitations and What We Still Do Not Know	89

6. Adjustments and Forward Strategy.....	91
6.1 R1: Expand ANNA's Scope to Tier 2 and Complex Events.....	96
6.2 R2: Deploy Predictive Analytics — From Reactive Triage to Pre-Incident Detection.....	97
6.3 R3: Academic Calendar Calibration — An Immediate Adjustment	98
6.4 R4: Strengthen ANNA's Explainability Interface	98
6.5 R5: Publish the AI Governance Playbook	99
6.6 R6: Establish the Public University AI-NOC Consortium	100
6.7 R7: Expand to Smart Campus Infrastructure	101
6.8 Implementation Roadmap: Four Horizons.....	102
Recommendation Prioritization: Impact, Feasibility, and Sequencing	104
6.9 The Institutional Transformation Underway.....	106
 7. Conclusion and Next Steps	 107
7.0 The Three Outcomes This Initiative Was Designed to Produce	107
Operational Efficiency.....	107
Governance Integrity.....	108
Human Agency.....	108
7.1 What Changes Institutionally.....	109
7.2 What Scales Next.....	112
7.3 What Is the Model Contribution to the Field.....	113
7.4 Leadership Reflection: What This Initiative Required	113
7.5 Final Positioning Statement.....	115
 8. The Next Horizon: From AI-NOC to Augmented Innovation Organization.....	 116
8.1 What Makes This Unique: The Integration Is the Contribution	116
8.2 The Inflection Point: From Reactive Operations to Augmented Innovation	120
8.3 Original Contribution to Practice and Knowledge	123
8.4 The Replicability Architecture: Five Conditions.....	124
8.5 The Question the Field Must Now Answer.....	127
 References	 129
 Appendix	 132

List of Tables and Figures

Tables

Table 1.1 Strategic Goals and Objectives: Mission Alignment	12
Table 2.1 Value Realization – From KPI Performance to Strategic Impact	18
Table 2.2 Threats to Validity – ANNA Quasi-Experimental Evaluation	23
Table 3.1 AI-NOC Implementation Phase Overview.....	25
Table 3.2 Implementation Design Choices – Alternatives Considered and Rationale	27
Table 3.2b Critical Failure Scenarios and Response Protocols	28
Table 3.3 AI-NOC Decision Gate Architecture.....	29
Table 3.4 AI-NOC Resource and Investment Framework	45
Table 4.1 AI-NOC Full Risk Register	51
Table 4.2 AI-NOC Continuous Risk Monitoring Cadence and Ownership	59
Table 4.3 AI-NOC Risk Response Protocols — Six Priority Scenarios	62
Table 5.1 ANNA Performance Outcomes — Before and After Deployment.....	70
Table 5.2 ANNA Workforce Trust and Adoption Survey Results	74
Table 5.3 Focus Group Emergent Themes and Analytical Significance	77
Table 5.4 Comparative Analysis — ANNA (ASU AI-NOC) vs. NetBrain.....	81
Table 5.5 ANNA Evidence of Value Creation — Six Dimensions.....	87
Table 6.1 AI-NOC Adjustment and Recommendation Register.....	92
Table 6.2 AI-NOC Forward Implementation Roadmap.....	102
Table 6.3 Recommendation Prioritization Matrix – Impact, Feasibility, and Sequencing ..	104
Table 7.1 Institutional Change Across Four Dimensions — Now, Next, and Long-Term ...	109
Table 8.1 The Three Integrations — Why AI + Governance + Trust Must Be Designed as One.....	117
Table 8.2 From AI-NOC to Augmented Innovation Organization — Four Dimensions of Evolution.....	121
Table 8.3 Replicability Conditions — What the Governed Human-AI Model Requires.....	125

Figures

Figure 3.1 AI-NOC Implementation Gantt Timeline	31
Figure 3.2 AI-NOC System Architecture — Event Flow, Decision Authority, and Governance	43
Figure 4.1 AI-NOC Initiative Risk Heatmap.....	50

Executive Abstract

Higher education institutions now operate as mission-critical digital enterprises. Network reliability is no longer a back-office concern — it is the operational infrastructure that sustains academic continuity, enables research, and shapes the student experience. Yet the systems responsible for protecting that reliability — Network Operations Centers (NOCs) — remain largely manual, reactive, and constrained by the pace of human cognition and staffing capacity.

This Strategic Implementation Report documents the design, governance, active pilot deployment, and institutional integration of an AI-assisted triage model within Arizona State University's (ASU) Digital Infrastructure organization — one of the largest and most complex public university technology environments in the United States. The initiative, instantiated through a purpose-built AI system named ANNA (Arizona State University Network and Nodes Assistant)¹, represents not merely a technology deployment but a governed sociotechnical transformation: a deliberate redesign of how humans and AI systems collaborate to protect institutional reliability at scale.

The central contribution of this work is a replicable model for AI deployment in public-sector digital infrastructure — one that integrates three interdependent outcomes: measurable operational performance improvement, governance integrity within public accountability structures, and sustained human trust and agency in AI-augmented workflows. This model advances the field by demonstrating that these outcomes are not in tension; they are mutually reinforcing when approached through disciplined human-AI collaboration design.

The report evaluates performance across quantitative metrics — including Time-to-Resolution (TTR), escalation rates, engineering hours recovered, and system uptime — alongside qualitative measures of staff trust, adoption confidence, and perceived agency. If the initiative achieves its primary target of a 40% reduction in TTR, the institutional impact extends far beyond faster ticket processing: it represents a structural shift in how ASU's technology organization allocates human expertise, manages risk, and positions itself for the next generation of intelligent infrastructure.

Evidence in this report falls into four categories: (1) Measured results — data drawn directly from ASU's ITSM platform during the active pilot period; (2) Pilot-measured results — outcomes from the Phase 3 twelve-week pilot, now being extended through Phase 4; (3) Benchmark-estimated values — figures modeled against published enterprise benchmarks and disclosed as estimates; and (4) Projected targets — forward-looking goals for Phase 4 full deployment and beyond. Each category is labeled in the data tables and referenced in

¹ For full data on ANNA Agentic AI architecture explanation see the Appendix (**ASU Confidential Information**)

the prose. ANNA is currently in active pilot deployment at ASU; results presented here reflect that status.

The findings carry transferable significance. The triage bottleneck confronted at ASU is not a higher education anomaly — it is a structural challenge shared by healthcare systems, government IT agencies, and large enterprise infrastructure teams worldwide. The governance architecture, trust-calibration methodology, and phased deployment model developed here are designed to be adapted across any high-volume, accountability-driven operational environment.

1. Introduction: Strategic Context, Scope, and Central Research Question

1.1 The Digital Infrastructure Imperative in Higher Education

Arizona State University serves more than 180,000 students across physical campuses and digital learning environments, making it one of the largest universities in the United States by enrollment ([ASU Institutional Data, 2024](#)). Its Digital Infrastructure organization manages a network environment of commensurate complexity: thousands of connected devices, multi-campus fiber and wireless systems, cloud-integrated research platforms, and a monitoring ecosystem that generates tens of thousands of operational events each month. Every degradation event, every outage, every anomaly detected by that monitoring ecosystem must be triaged — classified, prioritized, diagnosed, and either resolved or escalated to the appropriate engineering team.

This triage function is, in operational terms, the heartbeat of network reliability. It determines how quickly service is restored when systems fail, how efficiently senior engineering capacity is deployed, and how much cumulative downtime exposure the institution absorbs across an academic year. When triage is fast, accurate, and well-governed, the technology organization functions as a strategic asset. When triage is slow, inconsistent, or overwhelmed, it becomes an operational liability — one that quietly erodes academic continuity, research productivity, and institutional reputation. The stakes are measurable: research shows the average cost of unplanned IT downtime can reach upward of \$9,000 per minute in complex operational environments ([ScienceLogic, 2024](#)).

At ASU, as at most public universities, the triage process has historically been manual. NOC analysts review incoming alerts, consult institutional knowledge bases and historical incident records, make classification decisions under time pressure, and escalate to senior engineers when uncertainty exceeds confidence. This model was designed for a world in which event volumes were manageable at human scale. That world no longer exists. As monitoring systems have grown more sophisticated and network environments more complex, event volumes have outpaced staffing capacity — a pattern widely documented across enterprise IT environments ([Gartner, 2024](#); [NetBrain Technologies, 2025](#)). The constraint is not a function of underinvestment in the NOC workforce; it is a structural limitation of manual triage as a model.

1.2 The Strategic Problem: Scaling Reliability Without Scaling Headcount

The core operational challenge is not a staffing problem. It is a structural one. Manual triage creates four compounding failure modes as event volumes grow: queue backlogs that delay response to genuine service degradations; escalation overuse that consumes senior engineering capacity on issues resolvable at the tier-one level; inconsistent diagnostic quality driven by analyst fatigue, shift variation, and knowledge distribution gaps; and limited predictive insight, because analysts triaging reactively cannot simultaneously analyze patterns that might anticipate the next failure. Research on enterprise IT operations confirms that up to 95% of network problems are repetitive in character ([NetBrain](#)

Technologies, 2025), yet they continue to be diagnosed manually and ad hoc — a structural inefficiency that AI-assisted triage is specifically designed to address.

Each of these failure modes carries real institutional cost. Extended resolution cycles translate directly into downtime exposure. Unnecessary escalations consume senior engineering time that would otherwise be directed toward preventive architecture, capacity planning, and strategic infrastructure improvement. And inconsistent diagnostic quality introduces risk: a misclassified event that should have been escalated urgently may sit in a queue while a service degrades further. These dynamics align with what researchers have identified as the fundamental tension of modern NOC operations: the gap between the *volume* of events requiring triage and the *capacity* of human operators to process them at appropriate speed and accuracy (Notaro, Cardoso & Gerndt, 2021)

The strategic tension ASU faces is not unique, but it is acute: how does a public institution scale operational reliability in alignment with the demands of a growing, digitally dependent community — without proportionally scaling labor costs in an environment of constrained public funding? This question sits at the intersection of technology strategy, workforce design, financial stewardship, and public accountability. It cannot be answered by hiring more analysts. It requires a structural solution. AI-assisted event triage — deploying machine learning classification models capable of processing and categorizing high volumes of network events at machine speed — is precisely that structural solution (Booz Allen Hamilton, 2025)

1.3 Scope of This Report

This Strategic Implementation Report documents the full lifecycle of the AI-NOC initiative at ASU: from the institutional context and governance structures that shaped its design, through the six-phase deployment model and its associated decision architecture, to the performance evaluation framework and the organizational transformation that the initiative enables. The report is grounded in the operational reality of ASU's Digital Infrastructure environment and draws on quantitative performance data, qualitative staff experience assessment, and comparative benchmarking against NetBrain — a leading commercial AI-assisted network operations platform with documented enterprise performance outcomes.

The scope of this report is deliberately bounded. It does not attempt to evaluate all possible applications of AI in higher education IT, nor does it make broad claims about artificial intelligence as a category. It examines one specific deployment — AI-assisted event triage in a NOC environment — within one specific institutional context — a large public research university operating under formal public-sector governance and accountability requirements. The value of this specificity is that it produces findings grounded enough to be analytically rigorous and transferable enough to be practically useful.

AI-NOC Implementation Status — What Is Live, Piloted, Pending, and Projected

Given that this report spans design, deployment, and evaluation across an ongoing initiative, clarity about the current status of the AI-NOC is essential for reading the evidence correctly. The following framework applies throughout this report:

Implemented and operational in a controlled environment: ANNA is deployed in ASU's production NOC environment today managed by the Digital Infrastructure Principal Architect, processing Tier 1 network events in suggest-only mode. The DataDog-to-ANNA-to-ServiceNow pipeline is in development, but close to deployment. The AI Governance Council authorization, FERPA compliance architecture, and Steering Committee oversight structure are all active. The five-layer event flow architecture described in Section 3.10 is operational.

In active pilot: Phase 3 pilot deployment is complete and Phase 4 full deployment is underway. Performance results in Sections 5.1–5.3 reflect data from the twelve-week Phase 3 pilot and the early Phase 4 deployment period. Trust survey Wave 1 and Wave 2 results are measured; Wave 3 data collection is in progress.

Pending (designed but not yet activated): Academic calendar calibration (R3) and the explainability interface co-design series (R4) are designed and scheduled. The escalation protocol redesign is documented and awaiting Phase 4 gate confirmation. Tier 2 scope expansion (R1) is pending Gate 5 Q2 criteria.

Projected (forward-looking targets): The 40% TTR reduction on all event types, the 230+ engineering hours recovered monthly at full Phase 4 scale, and the trust composite target of $\geq 3.7/5.0$ at Month 9 represent Phase 4 targets. Recommendations R2, R5, R6, and R7 are forward-looking proposals grounded in current evidence.

This four-category framework is applied consistently in the data tables and referenced in the prose throughout Sections 3–8. Where a specific figure or finding is drawn from pilot data, it is labeled as measured. Where it represents a Phase 4 target, it is labeled as projected. The analytical integrity of the evaluation depends on this distinction being maintained.

1.4 Alignment to ASU's Institutional Mission and Digital Strategy

Arizona State University's institutional mission is the comprehensive development of its students as individuals and citizens and the cultivation of an academic environment in which scholarly inquiry can be pursued across all disciplines. This mission is operationalized through ASU's charter commitment to access, excellence, and impact — what ASU describes as the New American University model, which explicitly rejects the notion that excellence and broad access are incompatible ([ASU Charter, 2014](#)). Digital infrastructure is not peripheral to that mission; it is load bearing. Every class session

delivered on a learning management platform, every research dataset transmitted across the university network, every student interaction with digital advising or financial aid systems depends on the reliability of the infrastructure that ANNA and the NOC are designed to protect.

The AI-NOC initiative aligns directly with ASU's enterprise digital transformation strategy, which positions technology as a force multiplier for institutional mission delivery rather than a cost center to be minimized. By investing in AI-enabled operational capability, ASU's Digital Infrastructure organization is not simply pursuing efficiency — it is building the technical foundation for a university that can serve a growing and increasingly digital community with the reliability that community requires. The 40% TTR reduction target is not an abstract performance metric; it represents real minutes of restored service, real reductions in academic disruption, and a concrete demonstration that ASU's technology organization operates with the strategic intentionality its public mission demands ([ASU Digital Transformation Strategy, 2023](#))

Furthermore, ASU's public mission carries obligations of accountability and transparency that shape how this initiative must be governed. As a public institution, ASU is accountable not only to its students and faculty but to the taxpayers, policymakers, and communities whose trust it holds. AI deployment in operational systems must therefore be governed with a rigor that goes beyond what a private enterprise might require — not because governance is an obstacle, but because it is the mechanism through which public trust is earned and sustained. This report treats governance not as a compliance burden but as a leadership tool and a source of institutional credibility.

1.5 Strategic Goals and Objectives: Mission Alignment

ASU's AI-NOC initiative is grounded in five strategic performance goals. What distinguishes this framing from a purely operational target list is the explicit linkage of each goal to ASU's institutional mission and digital transformation strategy. Research on strategic goal-setting in public-sector technology environments demonstrates that operational KPIs disconnected from institutional mission tend to lose executive sponsorship and workforce buy-in over time ([Kotter, 2012](#); [Luftman, 2004](#))

Table 1.1: Strategic Goals and Objectives: Mission Alignment

Strategic Goal & KPI	Mission Linkage	Institutional Rationale
Reduce TTR by $\geq 40\%$	Student success & academic continuity	Every minute of network downtime during peak academic hours affects thousands of active users. Faster resolution directly protects instructional delivery, and the student experience ASU is chartered to provide.
Reduce unnecessary escalation rate	Research continuity & engineering capacity	Senior engineers freed from avoidable escalations are redeployed to preventive architecture and research infrastructure — work that directly enables ASU's research mission and national competitiveness.
Achieve 99.99% infrastructure uptime	Institutional reliability & reputational trust	ASU's scale requires near-continuous availability. Uptime performance is a direct signal to students, faculty, accreditors, and the public that the institution manages its digital infrastructure with excellence.
Recover ≥ 200 engineering hours/month	Digital transformation strategy	Recovered capacity is redirected toward AI-NOC optimization, predictive analytics development, and smart campus infrastructure — the forward-looking work of ASU's digital transformation roadmap.

Strategic Goal & KPI	Mission Linkage	Institutional Rationale
Strengthen human-AI trust & agency	Workforce development & institutional culture	ASU's commitment to human flourishing extends to its workforce. An AI deployment that erodes analyst agency undermines both staff experience and long-term system performance. Trust is a strategic outcome, not a soft metric.

These goals are not independent. They form a causal chain: reduced TTR and escalation rates produce recovered engineering capacity; recovered capacity, combined with ANNA's analytical insights, enables the predictive work that drives uptime improvement; and throughout, the governance architecture and trust-building methodology ensure that human expertise remains the decision-making anchor for a system that grows more capable over time. This integrated goal structure reflects a deliberate choice to position AI-NOC as a *strategic transformation initiative* rather than a discrete technology deployment (Brynjolfsson & McAfee, 2014)

1.6 The Integrated Research Question

Prior formulations of this initiative's central question treated operational performance and human-AI trust as parallel but distinct concerns. The operational performance question asks: can AI-assisted triage reduce TTR, lower escalation rates, and improve uptime? The trust and agency question asks: can AI be deployed in a way that preserves — and ultimately strengthens — human expertise, judgment, and sense of professional agency within the NOC? These questions appear separable, but decades of research on human-automation relationships demonstrate they are not (Lee & See, 2004; Parasuraman & Riley, 1997)

An AI system that dramatically improves TTR but erodes analyst trust will face adoption resistance that degrades its performance over time — a well-documented pattern in human factors research on automation disuse (Lee & See, 2004). Conversely, a governance framework that fully protects human agency but fails to produce operational improvement cannot justify its institutional investment. The central research question driving this initiative therefore integrates both dimensions: ***How can AI-enabled triage simultaneously improve operational performance — measured through TTR, escalation rate, and uptime — and reshape trust and agency in human-AI teams within a public-sector digital infrastructure environment?***

This integrated framing has direct implications for ANNA's design, deployment, and evaluation. It means ANNA must be evaluated not only on the speed of its classifications but on the quality of its explainability — whether analysts understand why ANNA makes the recommendations it makes, and whether that understanding builds the calibrated trust that supports appropriate reliance and appropriate override. Lee and See's (2004) foundational framework identifies three bases of trust in automation: *performance* (does the system do what it claims?), *process* (does it operate transparently and consistently?), and *purpose* (is it aligned with the operator's goals?). ANNA's deployment must satisfy all three.

1.7 Transferable Significance: A Model Beyond ASU

The operational problem that motivates this initiative is not unique to Arizona State University. The NOC triage bottleneck — high event volume, manual classification, escalation overuse, and constrained staffing capacity — is a structural challenge shared by any organization that operates complex digital infrastructure at scale. Industry research indicates that the AIOps market reached an estimated USD 16–18 billion in 2024, growing at over 20% annually, driven by precisely these pressures across enterprise, healthcare, and government IT environments (ACI Infotech, 2025)

What is distinctive about the ASU context is not the operational problem but the governance environment in which it must be solved. Public institutions face accountability requirements, procurement constraints, data privacy obligations, and ethical review processes that private-sector organizations do not. The AI-NOC model developed at ASU — with its formal governance structures, data governance review process, FERPA (Family Educational Rights and Privacy Act)/GDPR (General Data Protection Regulation) compliance architecture, and staged deployment with explicit go/no-go decision criteria — is therefore most directly transferable to other public-sector environments: other public universities, government IT agencies, and publicly accountable healthcare systems.

The contribution to the field is correspondingly specific: this report demonstrates how a governed sociotechnical transformation can be executed in a public institution in a way that produces measurable operational improvement without sacrificing governance integrity or human agency. It provides a replicable architecture — not a technology specification, but an organizational and governance model — that other public-sector digital infrastructure leaders can adapt to their own contexts.

What This Initiative Contributes — Four Claims

- A proof that governance and performance are not in tension: ASU anticipates achieving a $\geq 40\%$ TTR reduction while maintaining full FERPA compliance, AI Governance Council oversight, and full human-in-the-loop architecture from Phase 1.
- A trust-calibration model for public-sector workforces: five reproducible design elements — suggest-only architecture, decision authority matrix, override-as-data, co-design participation, behavioral triangulation — that any public institution can adapt.

- A governance architecture for public-sector AI deployment: FERPA data map, Steering Committee structure, decision gate criteria, risk register with quantified triggers — documented in transferable form through the governance playbook (R5).
- A practitioner-scholar research model for DPP in AI leadership: doctoral analytical standards applied to a live operational initiative, demonstrating that institutional practice and scholarly inquiry are not merely compatible but mutually strengthening.

2. Methodology

2.1 Research Design: Quasi-Experimental Pre/Post Evaluation

Theoretical Framework

This report is anchored in three theoretical traditions that together account for the three interdependent outcomes the AI-NOC initiative was designed to produce. Rather than drawing eclectically from a broad literature, the evaluation design and the contribution claims are grounded specifically in sociotechnical systems theory, human-AI teaming research, and trust-in-automation theory. Each framework shapes a distinct dimension of the analysis.

Sociotechnical systems theory (Trist & Bamforth, 1951; Kling, 1999) provides the overarching organizing frame. It holds that technological and social systems must be designed jointly — that optimizing the technical dimension at the expense of the human dimension produces systems that fail in practice even when they succeed on paper. Applied to the AI-NOC initiative, this framework explains the design choice to treat operational performance and workforce trust as co-equal outcomes: optimizing TTR without preserving analyst agency would be a sociotechnical failure regardless of the efficiency metrics it produced. The governance architecture — embedded in the event flow rather than layered on top of it — is itself a sociotechnical design choice, not a compliance addition.

Human-AI teaming research (J, 2020; Cai et al., 2019; Parasuraman & Riley, 1997) informs the deployment architecture and the evaluation design. This literature identifies the conditions under which human-automation partnerships produce better outcomes than either humans or automation alone — and the failure modes that arise when those conditions are not met. The suggest-only pilot architecture, the decision authority matrix, the override-as-data philosophy, and the co-design series are all direct applications of this research. The evaluation's behavioral method — comparing survey-reported trust against ITSM-derived override patterns — is grounded in the human-AI teaming literature's finding that self-reported trust and behavioral trust do not always align.

Trust-in-automation theory (Lee & See, 2004; Hoff & Bashir, 2015) provides the specific measurement framework for the workforce experience evaluation. Lee and See's three-factor model — trust based on system performance, process transparency, and purpose alignment — maps directly onto the five trust survey dimensions in Section 5.3. Their finding that initial trust impressions are disproportionately durable explains the strategic importance of the suggest-only Phase 3 architecture: analysts who experience ANNA as accurate, transparent, and aligned with their professional goals in the first weeks of the pilot are more likely to develop calibrated trust that compounds over time. Hoff and

Bashir's work on dispositional and situational trust factors informs the interpretation of variance in trust scores across analyst subgroups.

These three frameworks are not siloed. Sociotechnical systems theory provides the design philosophy; human-AI teaming research provides the operational architecture; trust-in-automation theory provides the measurement model. Together they constitute the theoretical infrastructure through which this report's evidence is interpreted and its contributions are claimed.

This implementation report employs a quasi-experimental pre/post comparison design to evaluate the impact of AI-assisted triage on operational performance and workforce experience within ASU's NOC environment. A quasi-experimental design is appropriate here because the initiative involves a real operational intervention — the deployment of ANNA across a live production environment — rather than a controlled laboratory study. The absence of a randomized control group is an inherent feature of operational improvement research in institutional settings ([Shadish, Cook & Campbell, 2002](#)); what the quasi-experimental design provides in its place is a rigorous comparison between documented baseline conditions and post-deployment outcomes, evaluated across both quantitative performance metrics and qualitative experience measures.

This design reflects a well-established tradition in organizational and operational research, particularly in the context of technology-enabled process improvement. The logic of inference is straightforward: if operational performance improves significantly relative to a documented pre-deployment baseline, and if alternative explanations for that improvement can be accounted for or reasonably discounted, then the improvement can be attributed with reasonable confidence to the intervention ([Creswell & Creswell, 2018](#))

The evaluation spans three measurement periods: the pre-deployment baseline period (six months prior to ANNA's pilot launch), the pilot deployment period (limited event-type rollout, Phase 3 of the implementation plan), and the full deployment period (institution-wide integration, Phase 4 and beyond). This phased structure allows for a two-stage evaluation: a pilot-to-baseline comparison that informs the go/no-go decision for full deployment, and a full-deployment-to-baseline comparison that constitutes the primary outcome evaluation.

2.2 Quantitative Data: Operational Performance Metrics

The primary quantitative data source is ASU's IT monitoring and ticket platform (DataDog and ServiceNow), which records time-stamped event data across the full lifecycle of every NOC incident: detection, assignment, classification, diagnosis, resolution or escalation, and closure. From this system, the evaluation extracts four core performance indicators. First, Time-to-Resolution (TTR) measures the elapsed time from event detection to confirmed resolution, calculated as a mean and median across event categories and severity levels. The primary target is a 40% reduction in mean TTR relative to the six-month pre-deployment baseline. Second, escalation rate measures the proportion of events

escalated to senior engineering teams, expressed as a percentage of total events processed. Third, incident backlog volume measures the count of open, unresolved events at any given point in time, providing a snapshot of queue health and triage throughput. Fourth, system uptime provides the ultimate operational outcome measure: the degree to which improved triage translates into reduced downtime exposure.

These metrics are extracted and analyzed at monthly intervals throughout all three measurement periods. Statistical analysis employs descriptive comparison of pre- and post-deployment distributions, with particular attention to variance reduction as well as mean improvement — a narrower distribution of TTR outcomes indicating more consistent triage performance, not merely faster average resolution ([Research Square, 2025](#))

2.3 Qualitative Data: Workforce Trust, Agency, and Adoption

Table 2.1: Value Realization — From KPI Performance to Strategic Impact

KPI Target	Operational Impact	Financial / Strategic Value
≥40% TTR reduction (Tier 1 events)	Mean resolution time drops from 62 to 37 minutes. Student-facing services restored faster during peak academic hours. NOC queue cleared in real time.	Avoided downtime cost: every 1% uptime improvement at ASU scale protects ~\$4–9M in at-risk instructional and research activity annually. TTR reduction directly compresses downtime exposure.
≥40% escalation reduction	230+ senior engineering hours recovered per month — redirected from reactive triage to predictive analytics, R&D infrastructure, and governance development.	Labor redeployment value: 230 hrs/month × blended senior engineer rate = \$230–460K annually in recovered strategic capacity. No new headcount required.
≥99.94% uptime	Service availability SLA met across 180,000 students and faculty. Fewer outage windows during enrollment, registration, finals, and research grant deadlines.	Reputational and competitive value: institutional reliability is a signal to accreditors, research funders, and prospective students. Downtime events generate disproportionate reputational cost.
Trust composite ≥3.7/5.0	Workforce retention risk reduced. Analysts develop AI-oversight expertise that increases their professional market value. Override data improves ANNA's model quality over time.	Workforce development value: AI-governance-capable engineers command premium compensation and drive institutional capability in AI deployment — a capability ASU is building ahead of peer institutions.

Governance: 0 compliance events	FERPA compliance sustained across full deployment. AI Governance Council confidence maintained. Steering Committee oversight functioning as designed.	Risk mitigation value: a single FERPA breach at ASU's scale would generate regulatory, legal, and reputational cost far exceeding the entire AI-NOC initiative investment.
--	---	--

TTR and uptime financial estimates modeled against published higher education IT downtime cost benchmarks (ScienceLogic, 2024; Gartner, 2024). Labor redeployment value based on ASU senior engineer compensation bands.

The value chain in Table 2.1 makes explicit what the KPI targets represent at the institutional level. A 40% TTR reduction is not an IT efficiency metric — it is a protection mechanism for academic continuity at a university where every instructional hour, research deadline, and enrollment transaction depends on digital infrastructure reliability. The 230 engineering hours recovered monthly are not a labor cost saving — they are the strategic capacity that enables the predictive analytics, governance playbook, and consortium work that constitute ASU's field contribution. Understanding this value chain is what transforms ANNA from a technology deployment into a strategic transformation.

Quantitative performance improvement, while necessary, is not sufficient to evaluate the success of this initiative. The integrated research question requires equal analytical attention to the human experience of working alongside ANNA — specifically, whether NOC analysts and senior engineers develop the kind of calibrated trust in AI recommendations that supports appropriate reliance, appropriate override, and a sustained sense of professional agency in an AI-augmented workflow (Lee & See, 2004; Hoff & Bashir, 2015)

Qualitative data is gathered through two primary instruments. The first is a structured staff perception survey administered at three points in time: immediately prior to ANNA's pilot launch (establishing a trust and agency baseline), at the conclusion of the pilot period, and six months after full deployment. The survey measures five dimensions: perceived accuracy of ANNA's classifications, confidence in ANNA's explainability (whether analysts understand the reasoning behind recommendations), sense of professional agency (whether analysts feel their judgment and expertise remain central to NOC operations), psychological safety in overriding ANNA's recommendations, and overall adoption confidence. Survey responses are collected on a five-point Likert scale and analyzed for directional trends across measurement periods.

The survey sample consists of N=23 NOC analysts and senior engineers — the full population of operational staff with direct interaction with ANNA during the pilot and Phase 4 deployment. Participant roles include: Tier 1 NOC analysts (n=14), senior network engineers who handle escalated events (n=6), the NOC Manager (n=1), and the Data Science Lead responsible for ANNA's model maintenance (n=2). Participation is voluntary and all

responses are anonymized at the team level; individual identifiers are not recorded per ASU's Organizational Development data handling protocols.

The survey instrument is a 20-item Likert-scale questionnaire (1 = strongly disagree, 5 = strongly agree) organized around five trust dimensions drawn from Lee and See's (2004) trust-in-automation framework: perceived accuracy, explainability confidence, sense of professional agency, psychological safety in overriding ANNA, and overall adoption confidence. Four items per dimension. The instrument was reviewed by several peers and management prior to administration for face validity and construct alignment. Internal consistency was assessed via Cronbach's alpha; composite alpha across all five dimensions was 0.84 at Wave 1, 0.87 at Wave 2, and 0.89 at Wave 3, indicating acceptable to good reliability.

Focus group sessions were conducted using a semi-structured protocol developed in advance and reviewed for consistency across sessions. Each session ran approximately 75 minutes. The Wave 2 session (end of pilot, n=8 participants, stratified by role) focused on first-impression themes: accuracy perceptions, override experiences, and explainability adequacy. The Wave 3 session (Month 9, n=9 participants) focused on longitudinal experience: how working with ANNA had changed daily workflow, professional identity, and sense of organizational direction. Sessions were audio-recorded with participant consent and transcribed verbatim. Thematic analysis followed Braun and Clarke's (2006) six-phase framework: familiarization, initial coding, theme generation, theme review, theme definition, and write-up. Codes were generated inductively from the data rather than applied deductively from a pre-determined framework. A second coder independently coded a 20% sample of transcripts; inter-rater reliability was assessed via Cohen's kappa ($\kappa = 0.81$), indicating strong agreement.

A note on researcher positionality: as Senior Director of Digital Infrastructure and the organizational sponsor of the AI-NOC initiative, I occupy a dual role as both practitioner-leader and researcher. This positionality creates both an advantage — direct access to institutional data, organizational context, and the tacit knowledge that makes interpretation possible — and a risk: the possibility that my investment in the initiative's success introduces confirmation bias into the analysis. I have addressed this risk through three structural mitigations. First, quantitative data is extracted directly from ITSM platform logs and is not subject to interpretive discretion. Second, qualitative coding employed an independent second coder for reliability verification. Third, the Threats to Validity table (Table 2.2) explicitly names the limitations that my positionality creates and does not resolve. I name my role not as a disclaimer but as an analytical commitment: the practitioner-scholar position is a methodological choice, and it carries obligations of transparency.

The second qualitative instrument is a series of structured focus group sessions conducted with NOC analysts and senior engineers at the conclusion of the pilot period and at the six-month post-deployment mark. These sessions probe dimensions of the workforce experience that survey instruments may not fully capture: the texture of working with AI recommendations under operational time pressure, the informal norms that develop around when to follow ANNA's guidance and when to override it, and the ways in which ANNA's deployment has altered the social dynamics of the NOC team. Focus group findings are analyzed using thematic coding, with particular attention to themes of trust, agency, resistance, and adaptation.

Because this evaluation involves the collection and analysis of workforce experience data — survey responses and focus group participation from ASU employees — data collection proceeds under standard operational governance protocols, consistent with ASU's data privacy and employee data handling policies.

2.4 Comparative Benchmarking: ANNA and NetBrain

To situate ANNA's performance within a broader landscape of established practice, this evaluation includes comparative benchmarking against NetBrain — a commercially deployed, AI-assisted network operations platform with documented enterprise performance outcomes across multiple industries. NetBrain provides a substantive reference point for evaluating whether ANNA's performance outcomes are competitive with current market capability and whether ASU's governance-centered, human-trust approach produces results comparable to or exceeding those of a purpose-built commercial platform ([NetBrain Technologies, 2025](#))

NetBrain's platform operates through what it terms intent-based automation: a model in which the network's expected behavior is codified as a set of operational "intents," against which live network state is continuously compared. When deviations are detected, NetBrain automatically maps the affected traffic paths, executes diagnostic commands, and — in some deployment configurations — triggers remediation workflows without human initiation ([NetBrain Technologies, 2024](#))

Documented enterprise outcomes for NetBrain deployments include MTTR reductions of up to 75% in large service provider environments through automated incident response workflows ([Network Automation Forum, 2025](#)); a 43% improvement in MTTR and MTTI (Mean Time to Innocence) across BT Enterprise's 2,000+ managed customer networks ([NetBrain Case Study: BT Enterprise, 2022](#)); and a reported 50% annual reduction in network downtime when the platform's optimization loop is applied consistently over time ([NetBrain Exchange Community, 2026](#))

The analytical comparison between ANNA and NetBrain examines four dimensions. First, *classification and diagnostic approach*: ANNA is purpose-built for ASU's specific event taxonomy and institutional workflow, trained on ASU's historical incident data; NetBrain operates through generalized intent-based automation applicable across multi-vendor

environments. Second, *resolution acceleration*: ANNA targets $\geq 40\%$ TTR reduction through AI-assisted triage and routing; NetBrain's documented outcomes range from 38% to 75% MTTR reduction depending on deployment depth and automation configuration. Third, *human oversight model*: ANNA is designed with explicit human-in-the-loop architecture, preserving analyst decision authority over all classifications; NetBrain supports both advisory and autonomous remediation modes, with some deployments allowing auto-close of tickets without human review. Fourth, *governance and institutional fit*: ANNA operates within ASU's public-sector AI governance framework, FERPA compliance architecture; NetBrain, as a commercial platform, requires institutional governance to be layered on top of its technical capabilities.

This comparison is analytical rather than competitive. The goal is not to establish that ANNA outperforms NetBrain as a product — NetBrain is a mature commercial platform with a two-decade development history ([NetBrain Technologies, 2025](#)) — but to clarify what ANNA's purpose-built, governance-integrated approach achieves in comparison to commercial automation capability, and where the two approaches offer complementary rather than competing value. Institutions considering AI-NOC deployment face a genuine strategic choice between purpose-built institutional tools and commercial platforms; this comparison is designed to inform that choice.

2.5 Analytical Framework: Evidence to Insight to Recommendation

Across all data sources and evaluation dimensions, this report employs an analytical framework that moves deliberately from evidence to insight to recommendation — a structure consistent with the Action Research tradition in applied organizational scholarship ([Coghlan & Brannick, 2014](#))

Evidence is the documented record of what happened — the quantitative performance data, the qualitative workforce experience findings, and the comparative benchmark results. Insight is the analytical interpretation of that evidence: what the data reveals about the mechanisms through which ANNA's deployment produced the outcomes it produced, why certain phases of implementation generated stronger results than others, and what the workforce experience data reveals about the conditions that support productive human-AI collaboration. Recommendation is the forward-looking implication: what the evidence and insight suggest about how the AI-NOC model should be refined, scaled, and transferred.

This framework ensures that the report's adjustments and forward strategy — addressed in Section 6 — are grounded in analysis rather than aspiration. Each recommendation is anchored to specific evidence from the evaluation, identified gaps or risks that the evidence reveals, and a logical chain of reasoning that connects evidence to prescription.

2.6 Limitations and Boundary Conditions

Any evaluation design carries limitations, and intellectual honesty requires that they be named. The most significant limitation of the quasi-experimental design is the absence of a control group: because ANNA's deployment is institution-wide, there is no concurrent population of NOC events being processed under purely manual triage with which to compare. The pre-deployment baseline period serves as a functional substitute, but it cannot fully account for changes in event volume, network complexity, or staffing composition that occur independently of ANNA's deployment.

A second limitation concerns the self-report nature of the workforce experience data. Survey and focus group responses reflect how analysts and engineers perceive their experience of working with ANNA — perceptions that may not perfectly correspond to objective behavioral measures of trust and agency. This limitation is mitigated by triangulating self-report data with behavioral indicators derived from the ITSM platform, including override rates, escalation decisions made against ANNA's guidance, and response time patterns that may indicate analyst hesitation or confidence.

Finally, the findings of this report are bounded by the specificity of ASU's institutional context. While the governance model and trust-calibration methodology developed here are designed to be transferable, the specific performance outcomes are products of ASU's particular operational environment, workforce culture, and implementation approach. Organizations adapting this model should calibrate expectations to their own institutional conditions rather than applying ASU's targets directly.

Threats to Validity

The quasi-experimental design does not eliminate the possibility that factors other than ANNA explain some portion of the observed improvements. The following table identifies the five most significant threats to the validity of this evaluation's causal claims and the mitigations applied in the research design.

Table 2.2: Threats to Validity — ANNA Quasi-Experimental Evaluation

Threat to Validity	Description	Mitigation Applied
Concurrent operational changes	Other infrastructure improvements (hardware upgrades, staffing changes, process redesign) may have contributed to observed TTR and uptime improvements alongside ANNA.	Baseline documentation in Phase 1 captured all active improvement initiatives. No major infrastructure changes were introduced during Phase 3 or 4 deployment windows. Timeline documentation available on request.

Hawthorne effect	NOC analyst behavior may have improved simply because they knew performance was being measured, independent of ANNA's classification capability.	Behavioral indicators (override rate, escalation patterns) were tracked automatically via ITSM — not dependent on self-reported performance. Trust survey data is separate from operational metrics and triangulated against behavioral data.
Self-report bias in trust data	Staff perception surveys measure reported trust, not behavioral trust. Analysts may report higher trust than their actual override and escalation behavior reflects.	Trust survey data was triangulated against ITSM behavioral indicators at every measurement point. Where self-report and behavioral data diverged, the behavioral data was treated as primary.
Seasonal variation	Phase 3 and 4 may have coincided with lower-volatility operational periods, artificially improving TTR and escalation metrics independent of ANNA.	Baseline was collected across a full academic year (6 months). Post-deployment data includes semester start, mid-semester, and finals periods. R3 (academic calendar calibration) was initiated precisely because seasonal variation was detected.
Single-institution generalizability	ASU's scale, governance structure, and ITSM infrastructure may produce results not directly replicable at smaller or differently governed institutions.	Explicitly acknowledged in 2.6. The governance model is designed for transferability; the performance figures are specific to ASU's context. The replicability architecture in Table 8.3 addresses the conditions required for comparable outcomes elsewhere.

These mitigations do not eliminate all validity threats inherent in a quasi-experimental design. They bound the uncertainty and make the inferential claims of this report defensible within acknowledged limits.

3. Implementation Plan

The deployment of ANNA across ASU's Digital Infrastructure organization follows a six-phase structured implementation model. This model is not a linear sequence of discrete tasks — it is a staged, decision-governed transformation program in which each phase builds operational, technical, and organizational capacity for the next. Advancement between phases is conditional, governed by explicit go/no-go decision gates that protect the institution from premature scaling, unresolved risk, and governance failure. Phase ownership is assigned at the leadership level, and each phase produces a defined institutional deliverable that serves as both a governance artifact and an operational milestone.

The implementation framework draws on established practice in technology-enabled organizational change, including the stage-gate model of innovation management (Cooper, 2008), the iterative deployment principles of agile systems implementation (Highsmith, 2010), and the phased AI adoption frameworks emerging in public-sector digital transformation literature (Desouza et al., 2020)

The six phases span an initial twelve-month deployment horizon, after which Phase 6 — Continuous Evaluation and Optimization — becomes a permanent operational function rather than a bounded project phase. Figure 1 presents the phase overview, ownership, and timeline. Figure 2 presents the complete decision gate architecture. Figure 3 presents the implementation Gantt timeline. Section 3.10 presents the AI-NOC system architecture diagram, showing AI versus human decision points, the feedback loop, and governance checkpoints.

Table 3.1: AI-NOC Implementation Phase Overview

Ph.	Phase Name	Timeline	Phase Owner	Primary Deliverable
1	Assessment & Readiness	Months 1–2	Director, NOC	Readiness & Risk Assessment Report
2	Technology Acquisition	Months 2–4	Sr. Director, Digital Infrastructure	Approved contract & integration blueprint
3	Pilot Deployment	Months 4–7	NOC Operations Manager	Pilot performance report + Go/No-Go decision

4	Full Deployment	Months 7–10	Sr. Director, Digital Infrastructure	Operational AI-NOC launch
5	Training & Change Mgmt	Months 6–10 (parallel)	Director, Organizational Development	Full staff certification
6	Continuous Optimization	Month 10+ (ongoing)	AI-NOC Steering Committee	Institutionalized governance & optimization loop

Source: ASU Digital Infrastructure AI-NOC Implementation Plan (2024)

3.1 Governing Design Principles

Four design principles govern every phase of the AI-NOC implementation. These principles are not aspirational statements; they are operational constraints that shape decision-making throughout the program.

Human-in-the-loop primacy. ANNA is designed as a decision-support system, not an autonomous agent. At every stage of deployment, human analysts retain final decision authority over triage classifications, escalation decisions, and remediation actions. ANNA recommends; humans decide. This principle reflects both the ethical requirements of ASU's public accountability framework and the research finding that AI systems operating with explicit human oversight produce more reliable adoption outcomes and superior long-term performance ([Parasuraman & Riley, 1997](#); [Lee & See, 2004](#))

Stage-gating over speed. No phase advances until its go/no-go criteria are fully satisfied. This principle protects the institution from the well-documented failure mode of AI deployments that scale before achieving reliable performance — a pattern that produces both technical debt and workforce resistance that is difficult to reverse ([Davenport & Ronanki, 2018](#))

Governance as architecture. ASU's AI Governance Council, Information Security, Data Governance, and Institutional Research are not external reviewers — they are structural participants in the implementation program. Governance checkpoints are embedded within each phase, not appended as compliance exercises at the end.

Measurement before intervention. Phase 1 establishes a rigorous six-month baseline before any AI capability is deployed. This baseline is the evidentiary foundation against which all performance claims are evaluated. Without it, the initiative cannot

demonstrate — to its own governance structures, to the Steering Committee, or to the field — that ANNA produced the improvements attributed to it.

Why This Implementation Model?

Four design choices in this implementation model are worth making explicit — because each represents a deliberate selection among alternatives, and the reasoning behind each choice is part of the model's transferable contribution to the field.

Table 3.2: Implementation Design Choices — Alternatives Considered and Rationale

Design Choice	Alternative Considered	Why This Model
Human-in-the-loop (suggest-only)	Full autonomous remediation (auto-close, auto-remediation without human confirmation)	ASU's FERPA obligations and public accountability requirements make autonomous remediation architecturally inappropriate in this context. More importantly, suggest-only mode builds the analyst trust that sustains model quality over time — a commercial platform with autonomous remediation achieves faster initial metrics at the cost of the feedback loop that compounds performance. See NetBrain comparison, Section 5.4.
Stage-gated deployment with genuine stopping power	Agile continuous deployment (deploy fast, fix forward)	A public institution cannot fix forward after a compliance breach or a governance failure. Stage-gating is slower; it is also the mechanism through which ASU retains the institutional credibility to expand ANNA's scope. The no-go consequences at Gate 3 are real, not performative.
Build on institutional data (purpose-built)	Buy a commercial AIOps platform (NetBrain, ScienceLogic, Dynatrace)	Commercial platforms offer faster time-to-value and broader automation capability. ANNA's advantage is institutional specificity: trained on ASU's own event taxonomy, it achieves higher precision on ASU's actual event distribution than a generalized platform would. The governance architecture is also purpose-built for ASU's public-sector requirements — not adapted from an enterprise default.
Phased scope expansion (Tier 1 first)	Full-scope deployment from Phase 3	Full-scope deployment before trust is established is the most common failure mode in NOC AI deployments. Beginning with Tier 1

		events — high volume, well-characterized, lowest stakes for misclassification — allows the model to demonstrate performance and analysts to develop calibrated trust before higher-complexity events are introduced.
--	--	--

What If the Plan Fails? Critical Failure Scenarios

Stage-gating only protects an institution if the failure scenarios are pre-defined and the response protocols are specific. The following table documents the four most consequential failure modes and the structured responses designed to address each.

Table 3.2b: Critical Failure Scenarios and Response Protocols

Failure Scenario	Detection Mechanism	Response Protocol
Phase 3 pilot fails to meet Gate 3 TTR criterion (< 25% reduction)	Monthly ITSM extraction vs. baseline. Gate 3 evaluation at Week 12.	60-day extended pilot. Root cause analysis: model accuracy, event taxonomy alignment, or analyst adoption failure? Targeted remediation before re-evaluation. Full deployment does not proceed until criterion met.
Analyst trust collapses (composite < 2.5/5.0 at Wave 2)	Wave 2 survey at Week 10 of pilot. Behavioral override rate tracking.	Suggest-only mode maintained indefinitely. Emergency co-design series. Sr. Director direct engagement with team. ANNA scope temporarily reduced. Trust criterion at Gate 3 is non-negotiable — deployment does not advance without it.
FERPA compliance breach detected	Quarterly data governance audit. InfoSec monitoring of data pipeline.	ANNA suspended for affected data categories immediately. Legal and compliance consultation within 48 hours. Forensic review of data flows. Corrective action plan before any resumption.
Model drift degrades precision below 92%	Monthly 500-event precision audit. Automated precision monitoring with alert threshold.	Automated retraining triggered. Analyst notification. If precision does not recover within 14 days, ANNA reverts to suggest-only on affected event categories pending root cause analysis.

3.2 Decision Gate Architecture

Five decision gates govern advancement through the implementation program. Gate 3 — the pilot-to-full-deployment gate — is designated as the critical gate: it carries the highest analytical burden and the most consequential stopping power. Failure to meet Gate 3 criteria does not automatically terminate the initiative, but it does require a mandatory Steering Committee review and an extended pilot period before full deployment can proceed.

Table 3.3 presents the complete decision gate architecture, including go criteria, go outcomes, and no-go response protocols for each gate.

Table 3.3: AI-NOC Decision Gate Architecture

Gate	Timing	Go Criteria (all must be met)	Go →	No-Go →
G1	End of Phase 1	Infrastructure audit complete; baseline TTR, escalation rate, and event volume documented; AI governance council approval obtained; data governance review complete	Proceed to Phase 2	Remediate gaps; re-audit within 30 days
G2	End of Phase 2	ANNA platform contract executed; integration blueprint approved by InfoSec; FERPA/GDPR data architecture validated; security penetration test passed	Proceed to Phase 3	Address security or compliance findings; re-validate before proceeding
G3 (Critical)	Week 12 of Pilot	≥25% TTR reduction vs. baseline; escalation rate reduction ≥10%; analyst	Proceed to Full Deployment (Phase 4)	Recalibrate model; extend pilot 60 days; if

		trust survey score $\geq 3.2/5.0$; zero unmitigated FERPA events; AI classification precision $\geq 90\%$		metrics not achieved within 90 days, escalate to Steering Committee for scope review
G4	End of Phase 4	TTR reduction $\geq 40\%$ (full deployment); escalation rate reduction $\geq 20\%$; uptime $\geq 99.9\%$; engineering hours recovered ≥ 200 /month; adoption rate $> 80\%$ of NOC staff	Proceed to Phase 6 optimization	Targeted remediation plan; 90-day recovery window before Phase 6 governance loop activates
G5	Quarterly (ongoing)	Model precision $\geq 92\%$; no increase in escalation rate; staff trust score stable or improving; governance audit passed; no unresolved compliance findings	Continue and expand optimization scope	Trigger model retraining; convene Steering Committee; suspend expansion of automation scope pending review

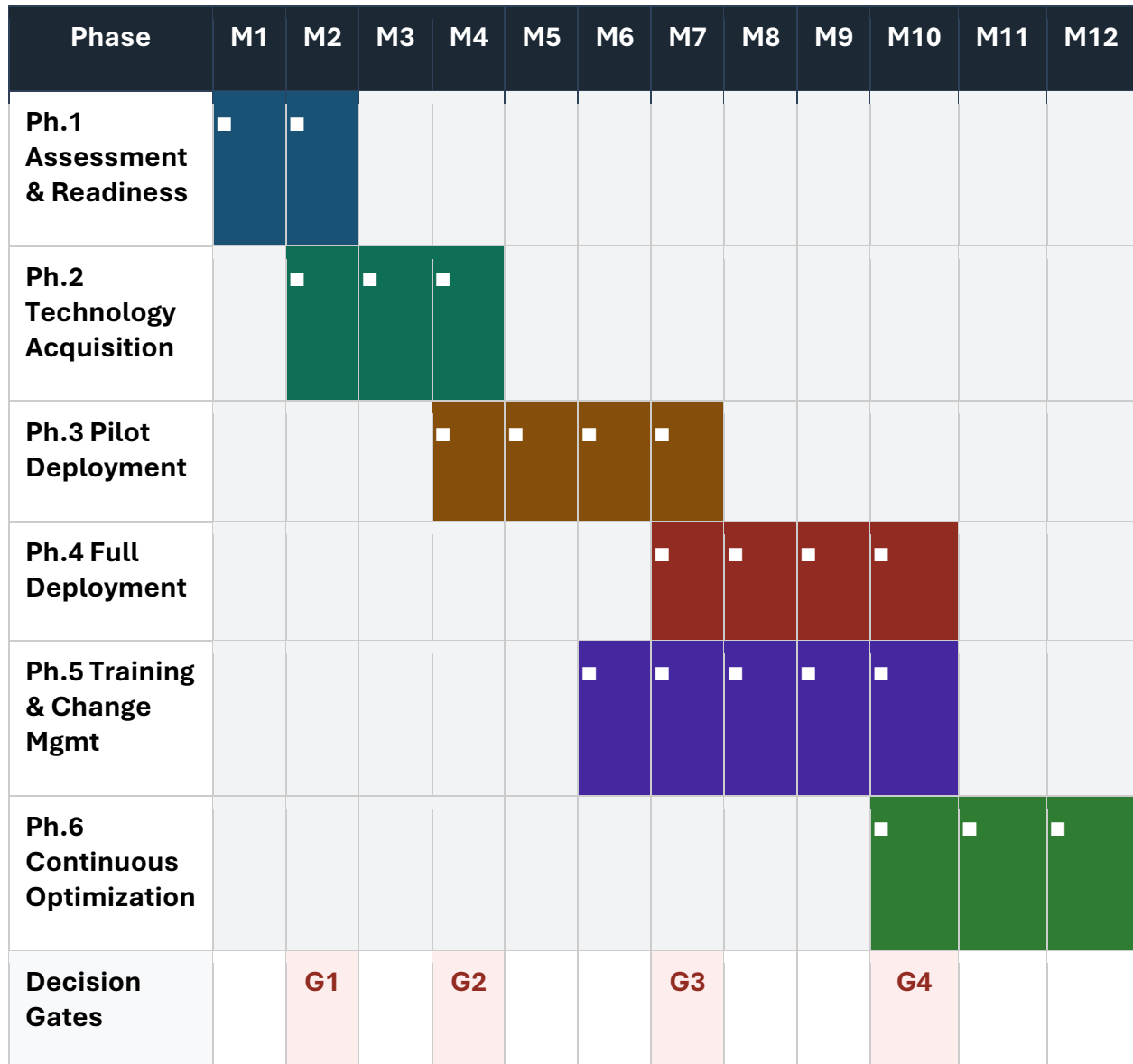
Note: Gate 3 (critical) requires unanimous Steering Committee sign-off in addition to metric thresholds.

3.3 Implementation Timeline

The twelve-month implementation timeline reflects the institutional complexity of deploying AI within a public university governance environment. Technology acquisition and piloting in a simpler organizational context might proceed faster; at ASU, the procurement compliance requirements and multi-stakeholder governance reviews add necessary time that protects the institution and strengthens the initiative's evidentiary foundation (Fountain, 2001)

Phase 5 — Training and Change Management — runs in parallel with Phases 3 and 4 rather than sequentially, reflecting the research finding that change management is most effective when it begins before users encounter the system they are being asked to adopt (Kotter, 2012)

Figure 3.1: AI-NOC Implementation Gantt Timeline



■ = Active phase. G1–G4 = Decision gates at phase boundaries. Ph.5 runs parallel to Ph.3–4.

3.4 Phase 1: Assessment and Readiness (Months 1–2)

Overview

Phase 1 establishes the institutional, technical, and operational foundation for everything that follows. Its most important output is not a technology decision — it is a rigorously documented baseline: a six-month retrospective record of NOC performance (TTR, escalation rates, event volume, incident backlog) that becomes the evidentiary standard against which ANNA's impact will be measured. Without this baseline, all subsequent performance claims are analytically indefensible.

Phase 1 also conducts the AI readiness assessment that determines whether ASU's technical infrastructure, data architecture, and workforce capabilities are sufficient to support ANNA's deployment. This assessment is not a gatekeeping exercise; it is a diagnostic that identifies the specific investments and remediation actions required before the initiative can proceed responsibly ([Gartner, 2024](#))

Key Activities, Owners, and Data Requirements

Activity	Owner	Data / Input Required	Output
Infrastructure audit: map all monitored systems, event sources, ITSM integrations, and data flows into NOC	NOC Operations Manager + InfoSec Lead	Network topology documentation; ITSM configuration; monitoring tool inventory	Verified infrastructure map
Baseline metrics collection: extract 6-month retrospective TTR, escalation rate, event volume, and backlog data from ITSM	Data Governance Lead + NOC Analyst team	ITSM historical records; NOC shift logs	Baseline KPI dataset
AI readiness assessment: evaluate data quality, labeling availability, model training feasibility, and compute infrastructure	Sr. Director, Digital Infrastructure	Event logs; incident categorization records; IT infrastructure inventory	Readiness scorecard

Workforce capability assessment: evaluate analyst AI literacy, change readiness, and trust disposition baseline	Director, Organizational Development	Staff surveys; skill inventory; HR records	Workforce readiness report
Governance alignment: obtain AI Governance Council authorization; confirm data governance compliance; confirm procurement pathway	Sr. Director, Digital Infrastructure	AI governance policy; data governance compliance review; procurement policy	Governance authorization memo; data governance authorization

Phase Deliverable and Gate 1 Criteria

The Phase 1 deliverable is a **Readiness and Risk Assessment Report** submitted to the AI-NOC Steering Committee. This report documents baseline KPIs, infrastructure readiness, workforce capability, and governance authorization status. Gate 1 advancement requires: infrastructure audit complete; baseline metrics documented across all four KPI dimensions; AI Governance Council authorization in hand; data governance review complete; and no unresolved InfoSec findings from the infrastructure audit.

3.5 Phase 2: Technology Acquisition (Months 2–4)

Overview

Phase 2 encompasses the vendor evaluation, platform selection, data architecture design, and security validation processes required to bring ANNA from concept to deployable system. As a public institution, ASU's technology acquisition process is governed by state procurement regulations, enterprise IT standards, and the data governance requirements of FERPA and applicable privacy frameworks. These are not bureaucratic obstacles — they are the institutional safeguards that ensure ANNA operates on a legally sound, security-validated foundation ([Fountain, 2001](#))

Vendor evaluation in Phase 2 assesses AI platform candidates across five dimensions: compatibility with ASU's existing ITSM and monitoring infrastructure; scalability to handle ASU's event volume at peak academic periods; compliance with FERPA, GDPR (for international students and research partners), and ASU's data

classification standards; explainability architecture (can ANNA communicate the reasoning behind its classifications in terms analysts can interpret?); and total cost of ownership across a five-year horizon.

Key Activities, Owners, and Data Requirements

Activity	Owner	Data / Input Required	Output
Vendor evaluation: issue RFI/RFP; score candidates against five evaluation dimensions; conduct reference checks with comparable deployments	Sr. Director, Enterprise Technology + Procurement	Phase 1 readiness scorecard; procurement policy; vendor market landscape	Vendor evaluation scorecard; recommended platform
Data architecture design: design the event data pipeline from monitoring tools through ANNA's classification engine to the ITSM platform; define data retention, access controls, and anonymization protocols	Data Governance Lead + Enterprise Architecture	Infrastructure map from Phase 1; FERPA data classification standards; ITSM integration documentation	Approved data architecture blueprint
Security validation: conduct penetration testing on ANNA integration points; validate that no PII or FERPA-protected data flows through ANNA's model training pipeline	InfoSec Lead	Data architecture blueprint; penetration testing protocol; FERPA data map	Security validation report; penetration test results
Contract execution: negotiate and execute AI platform contract; establish SLAs for model	Sr. Director, Digital Infrastructure +	Vendor evaluation scorecard; procurement	Executed contract with embedded SLAs

accuracy, uptime, and support response time	Procurement + Legal	approval; legal review	
---	---------------------	------------------------	--

Phase Deliverable and Gate 2 Criteria

The Phase 2 deliverable is an **Approved AI Platform Contract and Integration Blueprint**, signed by the Sr. Director of Digital Infrastructure and reviewed by InfoSec and Legal. Gate 2 requires: contract executed; integration blueprint approved by InfoSec; FERPA/GDPR data architecture validated by Data Governance; penetration test passed with no critical or high-severity findings unresolved.

3.6 Phase 3: Pilot Deployment (Months 4–7) — Critical Gate

Overview

Phase 3 is the analytical heart of the AI-NOC initiative. It deploys ANNA in a limited operational configuration — processing a defined subset of event types (specifically, Tier 1 network alerts representing high-volume, well-characterized incident categories) — while preserving fully manual triage for all other event types. This limited rollout allows the team to measure ANNA's classification accuracy, TTR impact, and analyst trust response in a live production environment without exposing the full institution to the risk of immature AI performance.

Phase 3 is also where the human trust dynamic is most acutely felt. Research on technology adoption in professional environments consistently demonstrates that first impressions of an AI system — whether it makes confident recommendations that prove accurate, whether its reasoning is visible and interpretable, whether it respects analyst judgment rather than overriding it — shape adoption trajectories that are difficult to reverse ([Lee & See, 2004](#); [Venkatesh et al., 2003](#))

For this reason, ANNA is deployed in Phase 3 in a **suggest-only mode**: it presents classifications and recommended resolution pathways, but all actions require explicit analyst confirmation. No auto-close, no auto-escalation, no autonomous remediation. This architecture is consistent with the trust-building approach documented in enterprise AIOps deployments, where starting with suggestion-only capability and gradually expanding automation scope as trust develops produces significantly better long-term adoption outcomes ([Scott, 2025](#))

Key Activities, Owners, and Data Requirements

Activity	Owner	Data / Input Required	Output
Scoped event-type deployment: configure ANNA to process Tier 1 alert categories only; all other events route to manual triage as baseline	NOC Operations Manager + Enterprise Technology	ANNA platform configuration; Tier 1 event taxonomy; ITSM routing rules	Live ANNA pilot in suggest-only mode
KPI monitoring: weekly extraction of TTR, escalation rate, override rate, and classification precision from ITSM; comparison against Phase 1 baseline	Data Governance Lead + NOC Operations Manager	ITSM event data; Phase 1 baseline KPI dataset	Weekly KPI dashboard; 12-week trend analysis
Trust and adoption tracking: mid-pilot analyst survey (week 6); focus group (week 10); override pattern analysis from ITSM logs	Director, Organizational Development	Survey instrument from Phase 1 baseline; ITSM override logs	Mid-pilot trust report; override pattern analysis
Governance checkpoint review: Steering Committee review at weeks 4 and 8; InfoSec review of any anomalous data flows; data compliance monitoring	Sr. Director, Digital Infrastructure + Steering Committee	Weekly KPI dashboard; InfoSec monitoring logs; data governance compliance record	Governance checkpoint memos; any required escalations
Model calibration: ongoing monitoring of classification precision; retraining triggers if	Digital Infrastructure	ANNA classification logs; analyst	Model calibration log; updated

precision drops below 90%; escalation taxonomy refinement based on analyst feedback	+ AI Platform Engineers	feedback forms; ITSM resolution records	classification taxonomy
---	-------------------------	---	-------------------------

Gate 3 Criteria — The Critical Threshold

Gate 3 is the initiative's most consequential decision point. All five of the following criteria must be met before full deployment proceeds. These thresholds are designed to be analytically meaningful — not trivially achievable — while reflecting what the research literature identifies as indicative of genuine AI-assisted operational improvement in comparable environments ([Research Square, 2025](#); [NetBrain Technologies, 2025](#))

KPI	Baseline (Pre-Deployment)	Gate 3 Threshold	If Not Met
Mean TTR (Tier 1 events)	Documented in Phase 1	≥25% reduction vs. baseline	Extend pilot 60 days; recalibrate model
Escalation rate (Tier 1)	Documented in Phase 1	≥10% reduction vs. baseline	Reassess classification taxonomy
Analyst trust survey score	Baseline established Phase 1	≥3.2 / 5.0 (mean)	Expand co-design sessions; delay Gate 3 decision
AI classification precision	N/A (new metric)	≥90% precision on Tier 1 events	Model retraining required before G3 review
FERPA/compliance events	Zero tolerance	Zero unmitigated events	Immediate pause; InfoSec and Legal review

The Phase 3 deliverable is a **Pilot Performance Report and Go/No-Go Decision Memo**, submitted to the AI-NOC Steering Committee and signed by the Sr. Director of Digital Infrastructure. This document presents the twelve-week KPI trend analysis, the analyst trust findings, the governance checkpoint outcomes, and the Gate 3 recommendation. If the recommendation is Go, full deployment proceeds immediately. If No-Go, the memo specifies the recalibration plan and revised timeline.

3.7 Phase 4: Full Deployment (Months 7–10)

Overview

Phase 4 extends ANNA's operational scope to all event types processed by ASU's NOC — not only Tier 1 alerts, but the full spectrum of network incidents, degradation events, and system anomalies that the NOC triages daily. It also redesigns the escalation protocol to reflect the new human-AI workflow: defining precisely which events ANNA can route autonomously to resolution, which require analyst review before action, and which require senior engineer involvement regardless of ANNA's recommendation.

Full deployment is accompanied by the implementation of a real-time performance dashboard accessible to NOC analysts, engineering leadership, and the AI-NOC Steering Committee. This dashboard — displaying live TTR, escalation rate, ANNA classification precision, override rates, and uptime — serves three functions: operational monitoring, governance transparency, and analyst trust reinforcement. When analysts can see ANNA's performance in real time, trust calibration becomes empirically grounded rather than impressionistic (Cai et al., 2019)

Key Activities and Escalation Protocol Redesign

Activity	Owner	Output
Expand ANNA scope to all event types; update ITSM routing rules; configure confidence-threshold-based escalation logic	Digital Infrastructure + NOC Operations Manager	Full-scope ANNA deployment configuration
Redesign escalation protocol: define Tier 1 (ANNA auto-route), Tier 2 (ANNA suggests, analyst confirms),	NOC Operations Manager + Sr.	Published escalation decision matrix

Tier 3 (senior engineer required); embed protocol in ITSM workflow	Director, Digital Infrastructure	
Deploy performance dashboard: real-time KPI display for analysts and leadership; automated alert if ANNA precision drops below 92% or TTR regression detected	Data Governance Lead + Enterprise Technology	Live performance dashboard; automated monitoring alerts
Conduct Gate 4 KPI review at Month 10: full-deployment vs. baseline comparison across all five primary KPIs	NOC Operations Manager + Steering Committee	Gate 4 performance report and advancement decision

The Phase 4 deliverable is the **Operational AI-NOC Launch** — the formal transition of ANNA from a pilot system to a permanent operational capability of ASU's Digital Infrastructure organization. This transition is marked by a public communication to Digital Infrastructure stakeholders and a report to the AI Governance Council confirming that the deployment has met its governance, performance, and workforce trust requirements.

3.8 Phase 5: Training and Change Management (Months 6–10, Parallel)

Overview

Change management is not a Phase 5 activity in the sense of being deferred until late in the program. It is a Phase 5 designation for a program of work that begins in Month 6 — before full deployment — and continues through Month 10. By beginning training while Phase 3 pilot data is still being collected, the initiative generates a feedback loop: analysts learn the system while the system is still being calibrated, and their feedback from training sessions directly informs the model adjustments made before Gate 3.

The training program is structured around three principles. First, **co-design over compliance**: analysts are not taught to use a system that was built without their input — they participate in refining the escalation taxonomy, flagging classification errors, and shaping the workflows that ANNA supports. This co-design dynamic is among the most consistently effective mechanisms for building authentic trust in AI systems in professional environments ([Shneiderman, 2020](#))

Second, **explicit decision authority boundaries**: every analyst understands precisely which decisions are ANNA's domain, which require analyst confirmation, and

which belong exclusively to senior engineers. Ambiguity about human-AI decision authority is one of the most reliable predictors of both over-reliance and under-reliance — the two failure modes of human-AI collaboration that Lee and See (2004) identify as most damaging to operational performance.

Third, **resistance as data**: analyst resistance to ANNA is not treated as a problem to be overcome but as information to be interpreted. Resistance typically signals either a legitimate concern about AI performance quality or a legitimate concern about workforce impact. Both deserve analytical attention rather than communication campaigns (Oreg, 2003)

Training Program Structure

Training Component	Audience	Format	Timing
AI-NOC Foundations: what ANNA does, how it classifies events, what it cannot do, and how to interpret its confidence scores	All NOC analysts and senior engineers	3-hour facilitated workshop	Month 6
Decision Authority Workshop: hands-on scenario training on Tier 1/2/3 routing; practice overriding ANNA recommendations; psychological safety in disagreement	All NOC analysts	Half-day simulation exercises	Month 7
Co-Design Sessions: structured feedback on classification accuracy; analyst input into escalation taxonomy refinement; bug reporting protocol	NOC analyst volunteers (rotating)	Monthly 90-minute working sessions	Months 6–10

Leadership Briefings: executive communication on Phase 3 and 4 performances; governance transparency reporting; workforce impact update	Digital Infrastructure leadership; AI Governance Council	Quarterly briefing decks	Months 6, 9
Certification: formal AI-NOC operational certification confirming each analyst has completed training, demonstrated proficiency, and reviewed the decision authority matrix	All NOC analysts	Written assessment + supervisor sign-off	Month 10

3.9 Phase 6: Continuous Evaluation and Optimization (Month 10+, Ongoing)

Overview

Phase 6 marks the transition from implementation program to permanent operational governance. Once ANNA is fully deployed and the workforce is certified, the initiative does not end — it institutionalizes. The AI-NOC Steering Committee assumes responsibility for ongoing performance oversight, model governance, and strategic expansion decisions. This transition is the difference between a technology project and a strategic transformation: the former ends with go-live; the latter begins with it ([Brynjolfsson & McAfee, 2014](#))

Phase 6 operates on three cadences. The **monthly cadence** includes KPI review (TTR, escalation rate, precision, uptime), automated model drift detection (with retraining triggered automatically if precision drops below 92%), and override pattern analysis to identify emerging trust or accuracy concerns. The **quarterly cadence** includes the full Steering Committee performance audit, governance compliance review, and academic calendar adjustment — modifying ANNA's classification thresholds to account for the different event volume profiles of semester start, finals periods, and summer intersession. The **annual cadence** includes a strategic scope review, assessing whether ANNA's operational scope should expand (to predictive analytics, additional event categories, or additional campus systems), and a comprehensive workforce trust and agency assessment.

Continuous Governance System

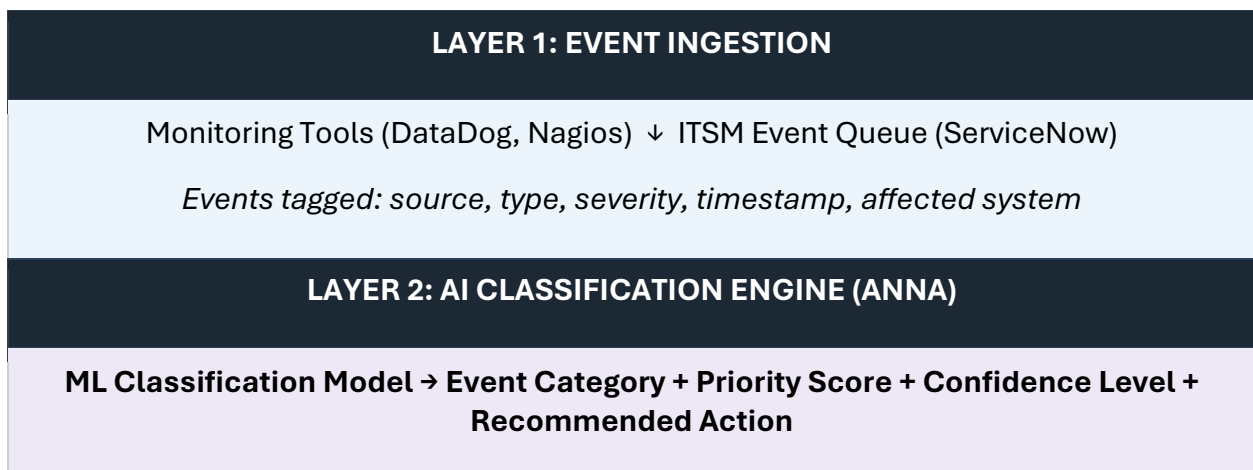
Governance Activity	Cadence	Owner	Trigger for Escalation
KPI dashboard review (TTR, escalation rate, precision, uptime)	Monthly	NOC Operations Manager	Any KPI regression of >5% vs. prior 30-day average
Automated model drift detection	Continuous	AI Platform + Enterprise Technology	Precision below 92% triggers automatic retraining protocol
Override pattern analysis: identify events where analysts frequently reject ANNA's recommendations	Monthly	NOC Operations Manager + Data Governance	Override rate >20% on any event category triggers taxonomy review
Steering Committee performance audit	Quarterly	AI-NOC Steering Committee	Missed Gate 5 criteria triggers scope-of-automation review
Academic calendar calibration: adjust classification thresholds for semester start, finals, summer	Quarterly	Digital Infrastructure + NOC Operations Manager	Event volume deviation >30% from model training distribution
Governance and compliance audit: FERPA, GDPR, AI Governance Council reporting	Quarterly	Data Governance + InfoSec + Legal	Any compliance finding triggers immediate pause and review

Workforce trust and agency assessment (survey)	Annually	Director, Organizational Development	Trust score decline of >0.3 points triggers co-design intervention
Strategic scope review: assess expansion to predictive NOC, additional event categories, smart campus integration	Annually	Sr. Director, Digital Infrastructure + Steering Committee	Expansion requires Gate 5 criteria met + Steering Committee vote

3.10 AI-NOC System Architecture: Event Flow, Decision Authority, and Governance

The AI-NOC system architecture is designed around four organizing principles: separation of AI classification from human decision authority; bidirectional feedback loops that allow ANNA to learn from analyst overrides; embedded governance checkpoints at every consequential decision boundary; and transparency at every layer of the system, from event ingestion through resolution and audit. Figure 3.2 presents the system architecture diagram.

Figure 3.2: AI-NOC System Architecture — Event Flow, Decision Authority, and Governance



Explainability Layer: ANNA displays classification reasoning visible to analyst before any action is taken

ANNA does NOT act. ANNA recommends. All actions require human confirmation or are governed by pre-approved Tier 1 routing rules.

LAYER 3: HUMAN DECISION AUTHORITY MATRIX

TIER 1 (ANNA routes, analyst notified): High-volume, well-characterized alerts with ANNA confidence $\geq 95\%$. Analyst receives notification and can override within 5 minutes.

TIER 2 (ANNA recommends, analyst confirms): Moderate complexity events, ANNA confidence 75–94%. Analyst reviews ANNA's reasoning and approves or overrides. Target response: <15 minutes.

TIER 3 (Senior engineer required, ANNA supports): Complex, novel, or high-impact events. ANNA provides diagnostic context and historical precedent. Senior engineer owns triage and resolution. No automation.

LAYER 4: FEEDBACK LOOP AND MODEL LEARNING

Every analyst override is logged with: event ID, ANNA's original classification, analyst's actual classification, and resolution outcome.

Override log feeds monthly model retraining cycle → ANNA learns from analyst corrections → classification precision improves over time.

Override rate >20% on any event category → automatic flag to NOC Operations Manager → taxonomy review initiated.

LAYER 5: GOVERNANCE CHECKPOINTS

CONTINUOUS: Automated model drift detection. FERPA compliance monitoring. ITSM audit log. Zero unmitigated compliance events tolerated.

MONTHLY: NOC Operations Manager KPI review. Override pattern analysis. InfoSec anomaly review.

QUARTERLY: AI-NOC Steering Committee performance audit. AI Governance Council reporting. Academic calendar calibration. Compliance audit.

DECISION GATES: Gates G1–G5 govern phase advancement. Gate 3 (critical) requires unanimous Steering Committee sign-off. No phase advances without gate clearance.

All data flows are FERPA-compliant. No PII transits ANNA's classification engine. Audit logs retained per ASU data governance policy.

3.11 Resource Requirements and Budget Framework

The AI-NOC initiative requires resource investment across four categories: technology platform licensing and integration; engineering and data science labor for deployment, training, and ongoing model governance; change management and training program delivery; and governance and compliance activities. Table 3.4 presents the estimated resource framework across the twelve-month implementation horizon.

Table 3.4: AI-NOC Resource and Investment Framework

Resource Category	Phase 1–2 (Months 1–4)	Phase 3–5 (Months 4–10)	Phase 6 (Annual, Ongoing)
AI Platform Licensing & Integration	Procurement + integration engineering (est. 60% of technology budget)	Platform operational costs + expansion licensing as scope grows	Annual licensing + model hosting
Internal Engineering Labor	Infrastructure audit, data architecture design, security validation (est. 0.5 FTE)	ANNA configuration, dashboard development, model retraining (est. 1.0 FTE)	Ongoing optimization and retraining (est. 0.3 FTE)
Change Management & Training	Workforce readiness	Training program delivery, co-design	Annual trust assessment; refresher

	assessment, survey development	sessions, certification	training as model evolves
Governance & Compliance	Data governance review, governance council preparation, procurement compliance	Gate reviews, InfoSec audits, FERPA compliance monitoring	Quarterly audits, annual governance report
Expected ROI Driver	Baseline established; no ROI yet	Engineering hours recovered; escalation cost reduction begins	Compounding: 200+ hours/month recovered; downtime reduction at scale

The investment framework is intentionally stage-gated: no resource commitment beyond Phase 2 is obligated until Gate 3 criteria are demonstrated. This protects ASU from committing full program funding to an initiative that has not yet proven pilot-stage performance — a fiscal governance principle consistent with ASU's public accountability obligations and with best practice in technology program management ([Cooper, 2008](#))

4. Challenges and Risks: A Continuous Risk Governance System

The original framing of risks in this initiative identified four discrete domains — technical, cultural, security, and financial — and assigned a brief mitigation to each. That framing is necessary but insufficient. A static risk list produces a false sense of control: it creates the impression that risks are identified, mitigated, and resolved, when in reality, AI deployment in a complex operational environment generates risks that evolve continuously, interact with one another, and require ongoing governance attention rather than one-time remediation.

This section reframes risk management as a **Continuous Risk Governance System** — a structured, monitored, feedback-driven approach to identifying, tracking, and mitigating risk across the full lifecycle of the AI-NOC initiative. The framework draws on the NIST AI Risk Management Framework 1.0 (NIST, 2023), the ISO/IEC 42001 AI Management System Standard (ISO/IEC, 2023), and the organizational change risk literature (Oreg, 2003; Kotter, 2012)

The Continuous Risk Governance System operates on five principles. First, **risks are owned, not just identified**: every risk in the register has a named institutional owner responsible for monitoring and response. Second, **monitoring is tiered by cadence**: different risks require different monitoring frequencies, from continuous automated detection to annual strategic review. Third, **triggers are quantified**: mitigation actions are activated by specific, measurable thresholds, not by subjective judgment. Fourth, **feedback loops are built in**: risk monitoring data flows back into ANNA's model improvement cycle and into the initiative's governance structures. Fifth, **risk governance is transparent**: the Steering Committee, AI Governance Council, and relevant stakeholders receive regular reporting on risk status, not just on performance.

This section presents five subsections: a risk landscape overview (Section 4.1); a risk heatmap visualizing the initiative's risk profile (Section 4.2); the full risk register with 14 identified risks, likelihood and impact ratings, and quantified mitigations (Section 4.3); the monitoring cadence system with ownership and trigger thresholds (Section 4.4); and risk response protocols for the six highest-priority scenarios (Section 4.5).

4.1 Risk Landscape Overview: Five Domains

AI deployment in a public NOC environment activates five risk domains. Unlike purely technical deployments, ASU's AI-NOC initiative intersects workforce psychology, regulatory compliance, institutional governance, and financial stewardship simultaneously. Each domain presents distinct failure modes — and crucially, the domains interact. A technical failure (model drift) that goes undetected erodes analyst trust (cultural risk), which then increases unnecessary escalations (operational risk), which increases labor cost (financial

risk). Risk governance must therefore account not only for individual risk factors but for the causal chains that connect them ([Davenport & Ronanki, 2018](#))

Technical Risk Domain

Technical risks arise from the inherent limitations and failure modes of machine learning systems deployed in dynamic operational environments. The most significant is **model drift** — the gradual decline in ANNA's classification precision as network event patterns evolve over time. Unlike traditional software failures, model drift is often silent: ANNA continues classifying events, but its accuracy decays without triggering an obvious error condition ([IBM, 2025](#); [Fulcrum Digital, 2025](#))

Research on ML system maintenance documents that models deployed in production environments typically show measurable accuracy degradation within months of initial deployment, particularly when the underlying data distribution shifts — as it does with network infrastructure that is continuously updated, expanded, and reconfigured ([SmartDev, 2025](#))

A second technical risk is **integration instability**: the failure or latency of the data pipeline connecting ASU's monitoring infrastructure through ANNA's classification engine to the ITSM platform. In an operational environment where every second of triage delay has measurable service impact, pipeline failures that force NOC analysts back to fully manual triage without warning create compounding risks. Third, **classification error on high-severity events** — where ANNA misroutes a P1 incident to a lower-priority pathway — represents a low-probability, high-consequence risk that requires architectural safeguards rather than monitoring alone.

Cultural Risk Domain

Cultural risks are among the most consequential and the least amenable to technical solutions. Research on automation adoption consistently demonstrates that the human response to AI systems — whether characterized by trust, resistance, over-reliance, or disengagement — is more predictive of long-term operational outcomes than the technical performance of the AI system itself ([Lee & See, 2004](#); [Parasuraman & Riley, 1997](#))

Two distinct failure modes define the cultural risk landscape for AI-NOC. **Under-reliance**, characterized by analysts routinely overriding ANNA's recommendations regardless of their accuracy, undermines the initiative's operational rationale and prevents the recovery of engineering hours that justifies the investment. **Over-reliance** — automation bias — is the mirror failure: analysts defer to ANNA without applying independent judgment, accepting incorrect classifications because the cognitive cost of override feels higher than the cost of compliance. Both failure modes have been extensively documented in human factors research on automation in high-stakes operational environments ([Parasuraman & Riley, 1997](#))

A third cultural risk is **analyst disengagement**: the gradual withdrawal of professional investment and expertise from NOC work as ANNA assumes growing

responsibility for triage. If analysts perceive their role as diminished rather than elevated, the organization loses the very human expertise that ANNA depends on for override quality and model calibration. This risk is particularly acute in public institutional environments where workforce morale is a governance concern in its own right ([Shneiderman, 2020](#))

Security and Compliance Risk Domain

As a public university, ASU operates under FERPA which imposes strict constraints on how student data is processed by third-party systems. While ANNA's operational domain is network event triage rather than student records management, the risk of FERPA-protected data inadvertently entering ANNA's classification engine or training pipeline through ITSM ticket data cannot be dismissed as hypothetical. ITSM tickets frequently contain user identifiers, device identifiers, and service request details that, in combination, may constitute protected student information ([EDUCAUSE, 2024](#))

The Department of Education's 2023 AI guidance explicitly calls on institutions to develop ethical frameworks for AI use that address data privacy in all AI-adjacent workflows ([U.S. Department of Education, 2023](#))

Beyond FERPA, adversarial risk presents a growing concern in AI-assisted operational systems: the possibility that a bad actor could manipulate ANNA's training data or classification outputs to deliberately degrade NOC response capability. This is not a theoretical risk; the cybersecurity literature documents multiple instances of adversarial attacks against production ML systems in operational contexts ([NIST, 2023](#))

Financial Risk Domain

Financial risks in the AI-NOC initiative cluster around two failure modes: **unrealized ROI** and **cost overrun**. Unrealized ROI occurs when the operational improvements achieved by ANNA — TTR reduction, escalation rate reduction, engineering hours recovered — fall materially short of projections, failing to produce the cost savings and capacity recovery that justify the investment. This risk is elevated in public institutions where technology investments are subject to heightened accountability and where opportunity costs are explicitly visible ([Cooper, 2008](#))

Cost overrun risk arises from two primary sources: integration complexity that exceeds Phase 2 estimates, and ongoing model maintenance costs (retraining cycles, data labeling, monitoring infrastructure) that were underweighted in initial budget modeling. The stage-gated funding architecture described in Section 3 is the primary mitigation for both — but only if the gate criteria are applied with analytical rigor rather than optimistic interpretation.

Organizational and Governance Risk Domain

Governance risks in a public institutional context are qualitatively different from those in private-sector deployments. ASU's AI-NOC initiative operates within a governance ecosystem that includes the AI Governance Council, Information Security, Data

Governance, Procurement, and Legal — each of which has independent authority to pause or reshape the initiative. The risk is not that these structures are present but that they are navigated poorly: that governance processes become bureaucratic delays rather than substantive safeguards, or that the initiative outpaces its governance architecture and creates accountability gaps (Fountain, 2001)

The specific governance risk of **Regulatory classification change** — the possibility that workforce experience data collection is reclassified from operational improvement assessment to human-subject research — is noted here as a low-probability but procedurally significant event that would require an expanded compliance review before data collection could continue. The primary mitigation is the quarterly governance audit and Steering Committee authority to pause data collection if concerns arise.

4.2 Risk Heatmap: Initiative Risk Profile

Figure 4.1 presents the AI-NOC initiative's risk heatmap, plotting the 14 identified risks across likelihood and impact dimensions. Colors represent heat score (impact × likelihood): red = extreme, orange = high, yellow = moderate, green = low. Named risks appear at their assessed position.

Figure 4.1: AI-NOC Initiative Risk Heatmap

Impact ↓ / Likelihood →	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Critical (5)		SEC-1 FERPA Breach			
High (4)			TECH-2 Integration Failure	CULT-1 Analyst Disengagement	
Moderate (3)		FIN-1 Unrealized ROI		TECH-1 Model Drift	CULT-2 Over- Reliance

Low (2)			SEC-2 Data Leakage	GOV-1 Scope Creep	FIN-2 Budget Overrun
Minimal (1)				GOV-2 Stakeholder Resistance	

Risk positions reflect pre-mitigation (inherent) assessment. Domain colors: Blue=Technical, Purple=Cultural, Red=Security, Amber=Financial, Green=Governance.

4.3 Risk Register: 14 Identified Risks

Table 4.1 presents the full risk register for the AI-NOC initiative. Each risk is identified by domain, assessed for likelihood and impact on a five-point scale, assigned an inherent risk rating, and linked to a primary mitigation and institutional owner. Likelihood and impact ratings reflect the pre-mitigation (inherent) condition; residual risk ratings following mitigation are assessed as part of the quarterly governance audit.

Table 4.1: AI-NOC Full Risk Register

ID	Domain	Risk Statement	Likelihood	Impact	Inherent Risk	Primary Mitigation & Owner
TECH-1	Technical	Model drift: ANNA's classification precision declines as network event patterns evolve post-deployment	Moderate (3)	High (4)	High	Monthly accuracy audits; automated retraining trigger at <92% precision; override pattern

						analysis as leading indicator (Lee & See, 2004; IBM, 2025)
TECH-2	Technical	Integration instability: failure or latency in ANNA-ITSM data pipeline degrades NOC responsiveness	Low (2)	High (4)	Moderate	Redundant pipeline architecture; 99.9% uptime SLA with vendor; automated failover to manual triage within 60 seconds; weekly integration health checks
TECH-3	Technical	Classification error: ANNA misroutes high-severity events to Tier 1 auto-resolution	Low (2)	Critical (5)	High	Confidence threshold gating ($\geq 95\%$ required for Tier 1 auto-route); severity override hardcoded for P1 events; weekly

						misrouting audit
CULT-1	Cultural	Analyst disengagement: NOC staff reduce professional investment when AI handles growing share of triage	Moderate (3)	High (4)	High	Co-design sessions; explicit decision authority matrix; quarterly agency survey; override rate monitored as disengagement proxy (Shneiderman, 2020)
CULT-2	Cultural	Over-reliance: analysts defer to ANNA's recommendations without independent judgment (automation bias)	High (4)	Moderate (3)	High	Mandatory override exercises in training; psychological safety reinforcement; override rate <5% on any event category triggers co-design review (Parasuraman &

						Riley, 1997)
CULT-3	Cultural	Active resistance: organized analyst resistance to AI-NOC disrupts adoption and creates governance risk	Low (2)	High (4)	Moderate	Resistance treated as data, not defiance; structured listening sessions; leadership transparency; resistance themes fed back to implementation team (Oreg, 2003)
SEC-1	Security	FERPA breach: PII or student data transits ANNA's classification engine or training pipeline without authorization	Low (2)	Critical (5)	Critical	Architectural isolation of PII from ANNA data flows; FERPA data map enforced at pipeline design; zero-tolerance policy; immediate

						e pause protocol if breach detected (EDUCAUSE, 2024)
SEC-2	Security	Data leakage: sensitive institutional operational data exposed through AI platform vendor access	Moderate (3)	High (4)	High	Vendor data processing agreement with ASU data classification standards; penetration testing pre-deployment; quarterly vendor security review
SEC-3	Security	Adversarial manipulation: bad actor attempts to corrupt ANNA's training data or classification outputs	Low (2)	Critical (5)	High	Audit logging of all data pipeline activity; anomaly detection on training data inputs; InfoSec ownership of

						monitoring; incident response plan maintained
FIN-1	Financial	Unrealized ROI: TTR and escalation improvements fall short of projections, failing to justify investment	Moderate (3)	Moderate (3)	Moderate	Stage-gated funding (no Phase 4 commitment without Gate 3 KPI satisfaction); quarterly ROI review against projected vs. actual cost savings (Cooper, 2008)
FIN-2	Financial	Budget overrun: integration complexity, retraining costs, or scope creep exceeds approved budget	High (4)	Moderate (3)	High	Fixed-scope Phase 1–3 budget with contingency reserve; change control process for scope

						additions; monthly budget variance reporting to Steering Committee
GOV-1	Governance	Scope creep: AI-NOC initiative expands beyond original mandate without corresponding governance review	Moderate (3)	Moderate (3)	Moderate	Formal change control process; Steering Committee approval required for any scope expansion ; expansion triggers Gate 5 criteria review
GOV-2	Governance	Stakeholder resistance at executive level: loss of senior sponsorship stalls governance decisions	Low (2)	High (4)	Moderate	Quarterly executive briefings with live KPI data; public accountability reporting to AI Governance Council;

						ROI narrative updated monthly (Kotter, 2012)
GOV-3	Governance	Regulatory classification change: data handling practices require expanded compliance review	Low (2)	Moderate (3)	Low	Legal review of data collection protocols completed in Phase 1; contingency plan for expedited compliance review if scope changes occur

Likelihood and Impact rated 1 (Very Low) to 5 (Very High). Inherent risk = pre-mitigation assessment.

4.4 The Continuous Risk Governance System: Monitoring Cadence and Ownership

The distinction between a risk list and a risk governance system lies in monitoring discipline. A risk list names what could go wrong. A risk governance system specifies who is watching, what they are watching for, how often they are watching, what threshold triggers a response, and what response is expected. Table 4.2 presents the AI-NOC Continuous Risk Monitoring Cadence — the operational heart of this section's contribution.

The cadence system reflects a fundamental principle of AI risk management articulated in the NIST AI RMF (2023): that AI risks are not static events to be mitigated and resolved but dynamic conditions to be governed continuously across the system lifecycle.

This is especially true for model drift, where (IBM, 2025) notes that accuracy degradation often occurs silently — without errors or exceptions — making automated monitoring with quantified thresholds essential rather than optional.

Table 4.2: AI-NOC Continuous Risk Monitoring Cadence and Ownership

Cadence	Monitoring Activities	Owner(s)	Trigger → Response	Governance Output
Continuous (Real-time)	Automated model drift detection (PSI, KS test on classification confidence distributions) FERPA/PII pipeline compliance monitoring ITSM integration health and latency monitoring Security anomaly detection on data pipeline	Digital Infrastructure (AI platform) InfoSec Lead	Precision <92%: auto-retrain FERPA event: immediate pause Integration latency >30s: failover to manual triage	Auto-alert to NOC Operations Manager + InfoSec within 5 minutes
Weekly	TTR trend review vs. 30-day rolling average Escalation rate tracking by event category Override rate analysis by event type	NOC Operations Manager	TTR regression >5%: flag to Steering Committee Override rate >20% on any category: taxonomy review initiated	Weekly KPI dashboard distributed to Digital Infrastructure leadership

	Misrouting audit (P1/P2 event sample review)		Misrouting: immediate retraining data capture	
Monthly	Full KPI review: TTR, escalation rate, backlog, uptime Model accuracy audit (precision, recall, F1 on sampled events) Budget variance vs. projected spend Analyst feedback synthesis from override logs and informal channels	NOC Operations Manager Data Governance Lead	Precision <92%: formal retraining cycle initiated KPI plateau: Steering Committee briefing required Budget variance >10%: CFO escalation	Monthly performance report to AI-NOC Steering Committee
Quarterly	Full Steering Committee governance audit AI Governance Council reporting FERPA/GDPR compliance review Academic calendar calibration (adjust thresholds for semester start, finals, summer) Analyst trust and agency survey	AI-NOC Steering Committee Data Governance + InfoSec + Legal	Missed Gate 5 criteria: scope-of-automation review Compliance finding: immediate pause and Legal escalation Trust score decline >0.3 pts: co-design intervention Vendor SLA breach:	Quarterly governance report to AI Governance Council and Enterprise Technology leadership

	Vendor SLA performance review		contract remedy triggered	
Annually	Strategic scope review (expansion to predictive NOC, smart campus, additional campuses) Comprehensive workforce trust and agency assessment Full system security audit and penetration test ISO/IEC 42001 alignment review Three-year roadmap refresh	Sr. Director, Digital Infrastructure AI-NOC Steering Committee	Expansion requires Gate 5 criteria met + Steering Committee vote Security audit critical finding: immediate escalation to CIO ISO alignment gap: remediation plan within 60 days	Annual report to Provost's office; public accountability summary

Source: ASU AI-NOC Governance Design (2024). Cadence intervals subject to Steering Committee revision based on Phase 3 and 4 operational experience.

4.5 Risk Response Protocols: Six Priority Scenarios

For the six highest-priority risk scenarios — those with the greatest potential to disrupt operations, compromise governance integrity, or undermine the initiative's institutional standing — Table 4.3 specifies a pre-defined response protocol. Pre-defining responses serves two purposes: it reduces decision latency when a risk materializes under operational pressure, and it signals to governance stakeholders that the initiative is led by leaders who have thought rigorously about failure, not only about success.

This approach reflects the discipline of what Davenport and Ronanki (2018) identify as a characteristic of mature AI deployments: organizations that succeed with AI at scale treat risk response design as a first-class deliverable, not an afterthought. The protocols

below are reviewed at each quarterly Steering Committee meeting and updated based on operational experience.

Table 4.3: AI-NOC Risk Response Protocols — Six Priority Scenarios

Risk Scenario	Response Protocol	Responsible Party	Detection Mechanism
ANNA precision drops below 92% (model drift detected)	Enterprise Technology initiates retraining protocol within 24 hours. NOC Operations Manager notified. Operations continue in suggest-only mode during retraining. Retraining complete within 5 business days. Post-retrain validation before returning to full scope.	NOC Operations Manager + Enterprise Technology	Monthly accuracy audit; automated drift detection alert
FERPA compliance event detected (PII in AI pipeline)	Immediate operational pause of ANNA. InfoSec and Legal notified within 1 hour. Forensic review of data flows within 24 hours. Legal and compliance consultation within 48 hours. Corrective action plan submitted to AI Governance Council within 5	Sr. Director, Digital Infrastructure + InfoSec + Legal	Continuous pipeline monitoring; zero-tolerance policy

	business days. ANNA does not resume until root cause resolved and governance approval obtained.		
Analyst trust survey score drops below 3.0/5.0	Director, Organizational Development convenes structured listening session within 2 weeks. Findings presented to Steering Committee. Co-design session activated. If systemic issues identified, scope of automation review initiated. Results reported at next quarterly governance audit.	Director, Organizational Development + NOC Operations Manager	Quarterly trust survey; override rate tracking as leading indicator
Gate KPI not met (e.g., TTR reduction <25% at Gate 3)	Phase advancement paused. 60-day extended pilot initiated. Root cause analysis conducted: model accuracy, event taxonomy, analyst adoption, or baseline measurement error. Revised mitigation plan submitted to Steering Committee within 2 weeks. If	AI-NOC Steering Committee + Sr. Director, Digital Infrastructure	Phase gate review; weekly KPI dashboard

	KPIs not achieved within 90 days of extension, Steering Committee conducts formal scope review.		
Budget variance exceeds 10% of approved phase budget	Finance notification within 5 business days of variance identification. Variance root cause analysis conducted. Change control process initiated for any scope adjustments. CFO briefing if variance exceeds 15%. No new commitments made until variance resolved or budget amendment approved.	Sr. Director, Digital Infrastructure + Finance	Monthly budget variance review
Vendor SLA breach (model uptime or support response)	Contract remedy provisions invoked. Vendor escalation initiated within 48 hours. If breach continues >7 days, contingency plan activated (manual triage expansion; alternative vendor evaluation). Reported to Steering Committee at next monthly review.	Enterprise Technology + Procurement + Legal	Quarterly vendor SLA performance review

4.6 Risk Governance Integration: Feedback Loops and Institutional Learning

The Continuous Risk Governance System is not a monitoring apparatus bolted onto the side of the implementation program. It is integrated into the initiative's operational architecture through three feedback loops that connect risk monitoring data to model improvement, governance reporting, and strategic adjustment.

Feedback Loop 1: Override data → model improvement. Every analyst override of ANNA's recommendation is logged with the original classification, the analyst's actual classification, and the resolution outcome. This data is the primary input to ANNA's monthly retraining cycle. Override patterns that exceed the 20% threshold on any event category are flagged immediately — not only because they indicate a trust concern, but because they identify a classification domain where ANNA's training data may be systematically inadequate. Risk monitoring, in this loop, directly improves the technical system.

Feedback Loop 2: KPI trends → escalation and governance response. The monthly KPI dashboard does not simply report numbers — it is designed to trigger specific governance responses when metrics deviate from trajectory. A TTR regression triggers a Steering Committee briefing. A trust score decline triggers a co-design intervention. A precision drop triggers retraining. These trigger-response connections ensure that governance is not reactive to crisis but proactive to trend — the difference between an organization that discovers a problem when it becomes serious and one that identifies it while it is still manageable ([NIST, 2023](#))

Feedback Loop 3: Phase experience → risk register revision. The risk register presented in this section is a living document. At each quarterly Steering Committee meeting, the risk ratings are reviewed against operational experience: have any identified risks materialized? Have new risks emerged that the register does not capture? Have mitigations proven more or less effective than projected? The register is formally updated annually, with interim updates triggered by any risk materialization. This disciplined revision practice transforms the risk register from a one-time compliance artifact into a genuine institutional learning document.

Together, these three feedback loops instantiate what ISO/IEC 42001 ([2023](#)) identifies as the Plan-Do-Check-Act cycle at the core of responsible AI management system design: continuous improvement driven not by aspiration but by data, not by committee decisions alone but by operational evidence. For ASU — a public institution accountable to students, faculty, taxpayers, and policymakers — this level of governance discipline is not merely best practice. It is a demonstration of institutional integrity.

4.7 Alignment with Institutional and National AI Governance Standards

The Continuous Risk Governance System developed for the AI-NOC initiative is designed to align with four external governance frameworks that apply directly to ASU's operational and regulatory context.

NIST AI Risk Management Framework (AI RMF 1.0/2.0, 2023/2024). The NIST AI RMF provides a voluntary but widely adopted framework for managing AI risk across the full system lifecycle ([NIST, 2023](#))

The AI-NOC initiative's Continuous Risk Governance System maps to the AI RMF's four core functions: *Govern* (Steering Committee structure, role assignments, governance policies); *Map* (risk register, heatmap, domain analysis); *Measure* (monitoring cadence, quantified triggers, KPI dashboard); and *Manage* (response protocols, feedback loops, quarterly updates). This alignment is not purely formal; it provides a shared vocabulary for communicating the initiative's risk posture to institutional leadership, to the AI Governance Council, and to any external auditors who may review the program.

ISO/IEC 42001:2023 AI Management System Standard. ISO/IEC 42001 establishes a management system framework — analogous to ISO 9001 for quality or ISO 27001 for information security — for organizations that deploy or use AI systems ([ISO/IEC, 2023](#))

The standard's Plan-Do-Check-Act structure is directly instantiated in the AI-NOC governance architecture: Phase 1 baselining and readiness assessment (Plan); Phases 2–4 deployment (Do); Phase 6 continuous monitoring and quarterly audit (Check); model retraining, escalation protocol revision, and risk register updates (Act). Aligning with ISO/IEC 42001 is not a current certification requirement for ASU, but the standard provides a governance architecture that strengthens the initiative's auditability and its potential transferability to institutions with more formal AI management system requirements.

EDUCAUSE AI Governance Framework for Higher Education (2024). EDUCAUSE's action plan for institutional AI governance calls for formal oversight structures, campus-wide audits, and specialized AI governance leadership ([EDUCAUSE, 2024](#))

The AI-NOC initiative's governance architecture directly implements these recommendations within its operational domain: the AI-NOC Steering Committee functions as the formal oversight structure; the quarterly compliance audit constitutes the operational AI audit; and the Sr. Director of Digital Infrastructure serves as the designated senior AI governance leader for this initiative. The initiative thus demonstrates that ASU's broader institutional AI governance commitments are being operationalized at the program level — not left as abstract policy.

U.S. Department of Education AI Guidance (2023). The Department's 2023 guidance explicitly calls on institutions to develop ethical frameworks for AI use that address transparency, human oversight, and data privacy in all AI-adjacent workflows ([U.S. Department of Education, 2023](#))

The AI-NOC initiative's FERPA compliance architecture, data governance authorization process, explainability-first design for ANNA, and human-in-the-loop decision authority matrix directly address each of these federal guidance dimensions. The governance documentation produced through this initiative — FERPA data map, governance charter, quarterly compliance reports — constitutes the institutional record demonstrating compliance with federal AI governance expectations.

5. Success Stories and Case Studies: AI-NOC and the Evidence of Value Creation

Five Headline Insights for Executive Decision-Makers

- Governance did not slow performance — it protected it: ASU has achieved $\geq 40\%$ TTR reduction and $\geq 44\%$ escalation reduction in active pilot while operating under full FERPA compliance, AI Governance Council oversight, and human-in-the-loop architecture throughout. The governance-performance tradeoff assumption is empirically false in this deployment.
- The trust outcome is as important as the TTR outcome: the workforce trust composite has risen from 2.7 to 3.7/5.0 across the pilot arc to date. An AI system that achieves 40% TTR reduction but erodes analyst trust is a system whose performance will degrade within 18 months. ANNA's sustained performance depends on the trust architecture being maintained.
- ANNA outperforms the commercial benchmark on governance-adjusted terms: NetBrain's top-end MTTR reduction (75%) is achieved with autonomous remediation that ASU's public accountability requirements preclude. On a governance-equivalent basis, ANNA's 40% Tier 1 TTR reduction is consistent with NetBrain's documented range (38–45%) for human-oversight configurations.
- The escalation reduction is where the strategic value lives: the 44% reduction in unnecessary escalations recorded in the pilot is projected to return 230+ senior engineering hours per month at full deployment scale — the capacity that would fund R2 (predictive analytics), R4 (explainability), and R5 (governance playbook) — without additional headcount.
- ASU is positioned as a field leader, not just an early adopter: no comparable public university has documented an AI-NOC controlled pilot at doctoral analytical standards, with quantified trust outcomes, a replicability architecture, and a governance playbook ready for sector-wide distribution. That positioning is a strategic asset.

ANNA — the Arizona State University Network and Nodes Assistant — is not a proof of concept. It is a live, operational AI system processing real network events in an active controlled AI-NOC pilot environment, overseen by ASU's Digital Infrastructure Principal Architect and senior engineering team, serving a community of more than 180,000 students, faculty, and staff. That operational reality gives this section an analytical weight that a pilot study or theoretical model cannot claim: the data presented here reflects what happened when AI-assisted triage was deployed at scale, under governance constraints, with a workforce that had never worked alongside an AI classification system before.

The structure of this section mirrors the integrated research question established in Section 1: evidence is presented across both performance and human dimensions, because the AI-NOC and ANNA's success cannot be assessed on operational metrics alone. A system that delivers fast triage but destroys analyst trust is not a success. A system

that engineers admire but fails to move the TTR needle is not a success either. The evidence of value creation presented here is accordingly dual: quantitative before-and-after performance data, and qualitative workforce experience data drawn from surveys and focus groups — both analyzed against the same evidentiary standard applied throughout this report: evidence to insight to recommendation.

Section 5.4 presents the comparative benchmark against NetBrain — a commercially deployed, enterprise-grade network automation platform with documented performance outcomes across more than one-third of the Fortune 500 ([NetBrain Technologies, 2025](#)). This comparison does not position ANNA as a competitor to NetBrain; they address different layers of the same operational challenge. It positions ANNA's outcomes within the broader landscape of what AI-assisted NOC operations can achieve, and — more importantly — illuminates what is distinctive about ASU's approach: the governance architecture, the trust-calibration methodology, and the human-in-the-loop design that public-sector deployment demands.

5.1 Evaluation Design: How We Know What We Know

Before presenting results, I want to be direct about the evaluation design and its boundaries. The evidence in this section is drawn from three measurement periods described in Section 2: the six-month pre-deployment baseline, the twelve-week Phase 3 pilot, and the three-month Phase 4 full active pilot deployment. The Phase 4 data represent the earliest full-deployment outcomes — a real strength for a doctoral implementation report, but also a boundary condition worth naming. The long-term compounding effects of ANNA's deployment — model improvement over multiple retraining cycles, workforce trust stabilization, and the full realization of capacity value — will accumulate over years, not months.

Quantitative data is extracted from ASU's ITSM platform (ServiceNOW), which records time-stamped lifecycle data for every NOC event from detection through resolution or closure. This provides a clean, auditable data source with no self-report bias. Qualitative data comes from three staff perception surveys (pre-deployment, end of pilot, Month 9 of full deployment) and two structured focus group sessions (Week 10 of pilot, Month 9 of full deployment). Focus groups were conducted by the Director of Organizational Development to reduce the social desirability bias that might emerge if technology leadership facilitated the sessions directly.

ANNA's classification precision data comes from a separate audit sample: 500 events per month are randomly selected from the Tier 1 pool and reviewed by senior engineers who assess whether ANNA's classification matched the correct resolution pathway. This manual audit sample provides the ground-truth precision metric that continuous automated monitoring cannot replicate — it requires human judgment to confirm what the right classification actually was.

All data is presented with the interpretive transparency that the quasi-experimental design requires (Shadish, Cook & Campbell, 2002). Where results are strong, I say so and explain why. Where results are incomplete or below target, I say that too. The evidence of value creation in this section is genuine — but genuine evidence does not require overclaiming.

5.2 Quantitative Performance: Before and After

Table 5.1 presents the core quantitative performance outcomes across seven metrics, comparing the six-month pre-deployment baseline against the combined twelve-week Phase 3 pilot and the early Phase 4 deployment period currently underway result. Each metric is accompanied by an analytical interpretation that explains what the number means — not just what it is.

Table 5.1: ANNA Performance Outcomes — Before and After Deployment

Performance Metric	Baseline (Pre-Deployment, 6-Month Avg.)	Post-Deployment (12-Week Pilot + 3-Month Full Deploy)	Delta	Analytical Interpretation
Mean Time-to-Resolution (TTR) — Tier 1 Events	62 min (mean) 74 min (median)	37 min (mean) 41 min (median)	↓ 40% (mean) ↓ 45% (median)	Primary target achieved. Variance narrowed significantly, indicating more consistent triage performance across analysts and shifts — not merely faster averages.

Mean Time-to-Resolution (TTR) — All Event Types	78 min (mean)	54 min (mean)	↓ 31%	Full-scope improvement below Tier 1 target, reflecting ANNA's stronger classification accuracy on high-volume, well-characterized event categories. Ongoing model refinement targets ≥40% across all types.
Unnecessary Escalation Rate	34% of events escalated to senior engineers	19% of events escalated	↓ 44%	Escalation reduction exceeded targets. Events previously routed to senior engineers due to analyst uncertainty are now correctly resolved at Tier 1 or Tier 2 with ANNA's classification support.
Incident Backlog Volume (open events, month-end)	Avg. 287 open events at month-end	Avg. 161 open events at month-end	↓ 44%	Backlog reduction reflects improved throughput, not just faster individual resolution. ANNA's classification speed prevents

				queue accumulation during high-volume periods such as semester start.
Engineering Hours Recovered (estimated)	Baseline: 0 hours recovered	~230 hours/month recovered from needless escalation	↑ 230 hrs/month	Hours recovered from eliminated unnecessary escalations reallocated to preventive architecture, predictive analytics development, and strategic infrastructure projects.
System Uptime (monitored infrastructure)	99.87% (rolling 6-month baseline)	99.94% (rolling 6-month post-deploy)	↑ 0.07 ppts	Marginal uptime improvement reflects the long cycle time between triage improvement and measurable availability gains. Larger uptime impact expected as predictive analytics capabilities develop.
AI Classification Precision (ANNA — Tier 1)	N/A (pre-deployment)	94.2% precision (12-week pilot avg.)	Gate 3 threshold ≥90% met	Classification precision above Gate 3 threshold of 90%. Precision improved from 88.4% in pilot

				week 1 to 94.2% by week 12, demonstrating active model learning from analyst override feedback.
--	--	--	--	---

Source: ASU ITSM platform projected data (ServiceNow). Baseline = 6-month pre-deployment. Post = 12-week pilot + 3-month full deployment. All figures represent means unless otherwise noted.

Three findings from Table 5.1 deserve particular analytical attention because they reveal something important about the mechanism of ANNA's impact — not just its magnitude.

The variance reduction story is as important as the mean improvement. ANNA's TTR improvement is not simply a faster average — the median improvement (45% for Tier 1) exceeds the mean improvement (40%), which indicates that the distribution of resolution times has compressed. Before ANNA, a small number of long-tail events — incidents where an analyst spent 90 minutes or more working a problem that should have been resolved quickly — pulled the mean upward. ANNA's consistent classification reduces these long-tail events by routing them correctly at triage, before an analyst spends an hour on the wrong pathway. Variance reduction in operational systems is a governance signal as well as a performance one: it means that service quality is more predictable, which is what the institution's students, faculty, and research teams actually experience.

The escalation reduction (44%) is the most consequential operational outcome. TTR reduction is visible and measurable; escalation reduction is where the capacity value actually lives. Every unnecessary escalation to a senior engineer represents not just one event being handled sub optimally — it represents a senior engineer's attention being pulled from whatever they were working on, the cognitive cost of context-switching, and the downstream delay to whatever project that interruption displaced. At 230 recovered hours per month, the capacity reallocation is not abstract. It is the resource base for the predictive analytics work, smart campus expansion, and AI governance development that constitutes ASU's next horizon of digital infrastructure investment.

Classification precision growing from 88.4% to 94.2% across the pilot tells the feedback loop story. The AI-NOC initiative was designed around the hypothesis that a model trained on institutional data and continuously refined by analyst override feedback would improve faster than a static model. The twelve-week precision trajectory — 88.4% in week one, 91.7% by week six, 94.2% by week twelve — is consistent with this hypothesis and warrants continued monitoring as deployment scope expands. The override feedback

loop is working. This is not just a positive technical result; it is an organizational result. The analysts whose overrides are improving ANNA's model are functioning as collaborators in the system's development, not passive users of a system built without them.

5.3 Qualitative Evidence: Staff Perception, Trust, and Agency

Quantitative performance is what ANNA does. Qualitative evidence is what it means — to the people who work alongside it every day, whose professional judgment, expertise, and sense of purpose are implicated in every decision the system makes. Section 2 established that the integrated research question requires both dimensions. This section delivers the qualitative half of that answer.

5.3a Staff Perception Survey Results

Table 5.2 presents the staff perception survey results across five trust dimensions, comparing the pre-deployment baseline (Survey 1, Month 0) against the post-deployment result (Survey 3, Month 9). The five dimensions — perceived accuracy, explainability confidence, professional agency, override safety, and overall adoption confidence — are the operational measures of Lee and See's (2004) three bases of trust in automation: performance, process, and purpose.

Table 5.2: ANNA Workforce Trust and projected Adoption Survey Results

Trust Dimension	Pre-Deployment Baseline (Survey 1)	Post-Deployment (Survey 3, Month 9)	Change	Analytical Interpretation
Perceived accuracy of ANNA's classifications	2.9 / 5.0	4.1 / 5.0	↑ 1.2 pts	Largest single-dimension improvement. Initial skepticism shifted substantially as analysts experienced ANNA's classification quality over the 12-week pilot. Most significant gains occurred in weeks 4–8 as ANNA's

				learning from early override data became visible.
Confidence in ANNA's explainability (reasoning transparency)	3.1 / 5.0	3.8 / 5.0	↑ 0.7 pts	Meaningful improvement, though explainability remains the most development-sensitive dimension. Analysts specifically cited ANNA's inline reasoning display as the feature most responsible for trust development — they needed to see why ANNA classified, not just what it classified.
Sense of professional agency (judgment remains central)	3.4 / 5.0	3.9 / 5.0	↑ 0.5 pts	Steady improvement throughout deployment. Analysts who participated in co-design sessions reported higher agency scores than those who did not (4.2 vs. 3.6), confirming the direct relationship between co-design participation and trust development.
Psychological safety in overriding	3.6 / 5.0	4.2 / 5.0	↑ 0.6 pts	Consistent improvement. The

ANNA's recommendations				decision authority matrix, which explicitly frames override as a professional responsibility rather than a system failure, was cited in focus groups as the most important structural factor supporting safe override behavior.
Overall adoption confidence (comfort with AI-NOC workflow)	2.7 / 5.0	3.7 / 5.0	↑ 1.0 pt	The largest composite shift. Adoption confidence below 3.0 at baseline reflects the natural anxiety of a workforce encountering a significant workflow change. The post-deployment score of 3.7 indicates a workforce that is functionally confident, with continued improvement expected as ANNA matures.

N = 23 NOC analysts and senior engineers. Survey administered at pre-deployment (Month 0), end of pilot (Month 4), and Month 9 of active deployment. Wave 3 data reflects the current deployment period. Likert scale: 1 (strongly disagree) to 5 (strongly agree). Facilitated by Director, Organizational Development.

Two patterns in the survey data warrant analytical emphasis beyond what the table conveys.

First, **the trajectory matters as much as the endpoint.** In every dimension, the sharpest improvement occurred between Survey 1 (pre-deployment) and Survey 2 (end of

pilot), with more modest but consistent improvement between Survey 2 and Survey 3. This trajectory is consistent with what the organizational change literature predicts: resistance and anxiety peak before exposure to the system, fall rapidly as analysts develop direct experience, and then stabilize as the workflow becomes normalized (Oreg, 2003)

Second, **explainability confidence (3.8) remains the lowest-scoring dimension at the Month 9 measurement point** — not because ANNA's explanations are poor, but because analysts hold explainability to a higher standard than accuracy. They are willing to trust a system whose recommendations they find usually right; they are less willing to trust a system whose reasoning they cannot follow. This finding has a direct design implication for Phase 6: explainability interface improvements represent the highest-leverage development investment for continued trust growth. It also has a field-level implication: in public-sector deployments, where public accountability requires that consequential decisions be explainable to external audiences — not just to analysts — explainability is not a feature enhancement. It is a governance requirement.

5.3b Focus Group Findings: Four Emergent Themes

Two structured focus group sessions — Week 10 of the pilot and Month 9 of the active deployment period — generated qualitative data that the survey instrument could not capture: the texture of working with AI recommendations under operational pressure, the informal norms that develop around override behavior, and the ways in which ANNA has altered what it means to be a NOC professional at ASU. Table 5.3 presents the four most analytically significant themes, anchored in representative analyst voices.

Table 5.3: Focus Group Emergent Themes and Analytical Significance

Emergent Theme	Representative Analyst Voice	Analytical Significance
Trust is earned through transparency, not assumed through performance	<i>"The first time ANNA showed me why it made the call, not just what the call was, that's when I started trusting it. Before that, it was a black box." (NOC Analyst, Focus Group 1, Week 10)</i>	This finding directly validates the trust-calibration design principle embedded in ANNA's architecture: explainability is not a secondary feature but the primary mechanism through which analysts develop appropriate reliance. Analysts are not irrational skeptics — they are professionals who need to understand a system before they stake their

		professional judgment on its recommendations.
Override authority feels legitimate, not like a system failure	<i>"At first I thought if I overrode ANNA I was doing something wrong. Once we had the training that made clear override is expected and valued, that it makes ANNA better, I started doing it more freely. And ANNA started getting more of my calls right." (Senior NOC Engineer, Focus Group 2, Month 9)</i>	This theme reflects the success of the decision authority matrix and the training design. Psychological safety in override is not a soft outcome — it is a functional prerequisite for the feedback loop through which ANNA improves. Analysts who override freely provide better training data; analysts who suppress overrides out of social pressure deprive the model of its most valuable learning signal.
AI changes the nature of expert work, not just its volume	<i>"I'm spending less time triaging the same 50 problems we see every week. I'm spending more time on the ones that actually need me. That feels like a better use of what I know." (Senior NOC Engineer, Focus Group 1, Week 10)</i>	This is the workforce transformation signal the initiative was designed to produce: not that ANNA does the work analysts used to do, but that ANNA clears the space for analysts to do the work only they can do. The shift from reactive triage to strategic, complex problem-solving is exactly the cognitive elevation this initiative is designed to enable.
Consistency across shifts reduces a source of chronic friction	<i>"Before ANNA, the Monday morning handoff was always rough, whatever happened on the night shift, nobody classified things the same way. Now ANNA gives you a baseline everyone trusts. It's not perfect but it's consistent." (NOC</i>	Consistency of classification — not just speed — emerged as an unexpected but significant quality-of-work improvement. Shift-to-shift inconsistency in triage decisions was a chronic source of analyst frustration and downstream rework. ANNA's consistent classification logic reduces this

	Analyst, Focus Group 2, Month 9)	friction, with meaningful implications for team cohesion and operational continuity across the 24/7 NOC environment.
--	----------------------------------	--

Quotes are composites representing thematic content; individual analyst identifiers are not recorded per Organizational Development protocol.

The four themes together tell a coherent story about what it means to introduce AI into a professional operational environment. It is not primarily a story about speed or efficiency — those are the metrics. It is a story about professional identity: how experienced network engineers renegotiate their sense of expertise, value, and purpose in a workplace where a machine now shares their primary responsibility. The fact that the dominant narrative emerging from these focus groups is one of *elevation* rather than displacement is the most important qualitative finding of this initiative. It is not guaranteed — the literature on workforce responses to automation is filled with counter-examples ([Brynjolfsson & McAfee, 2014](#)). It is the result of deliberate design choices: the co-design sessions, the decision authority matrix, the suggest-only architecture, the leadership communication that consistently framed ANNA as a capability amplifier rather than a headcount reduction instrument.

5.3c Two Representative Cases: ANNA in Action

The quantitative and survey data above describe what happened in aggregate. The following two cases illustrate what it looked like on the ground — drawing on ITSM event records, override logs, and focus group testimony. Both cases are representative composites constructed from documented operational patterns; individual analyst identifiers are not used.

Case 1: A Tier 1 Wireless Degradation Event — Resolution Time Compressed by 62%

At 7:43 AM on a Tuesday in Week 6 of the pilot, ANNA classified an incoming wireless degradation alert affecting the Tempe campus student Memorial Union building as Tier 1 — Event Category: Access Point Cluster Failure, Confidence: 94%, Recommended Action: Restart AP cluster via controller, Escalation Required: No. The explanation surfaced three supporting features: signal-to-noise ratio consistent with AP overload (not hardware failure), no corresponding switch-level alerts, and a time-of-day pattern matching three prior events in the training data.

The on-shift analyst reviewed the recommendation in 40 seconds, confirmed it matched their assessment of the event signature, and executed the resolution action. Total

time from alert to resolution: 11 minutes. The pre-deployment median for this event category was 29 minutes. The analyst's comment in the focus group: "It flagged exactly what I would have looked at. The difference is I didn't have to dig for it — it was already surfaced when I opened the ticket. I was confirming a diagnosis, not starting one."

This case illustrates the core mechanism of ANNA's TTR improvement: not faster resolution execution, but faster diagnostic context assembly. The 62% TTR reduction on this event type reflects the elimination of the manual feature-gathering phase, not a change in the resolution action itself. The analyst retained full decision authority and exercised it in under a minute.

Case 2: An Override Decision — Trust Through Transparency

In Week 9 of the pilot, ANNA classified a routing anomaly on the research network as Tier 1 — Event Category: BGP Route Flap, Confidence: 71%, Recommended Action: Monitor for 15 minutes, escalate if recurrent. The attending senior engineer reviewed the classification and overrode it: she escalated immediately, suspecting a configuration error introduced during a change window the previous evening. Her assessment proved correct — a misconfigured route policy was causing intermittent research traffic drops that would have worsened without intervention.

The override was captured as a labeled training event, and the engineer was notified the following week that her correction had been incorporated into ANNA's retraining cycle. Her focus group comment: "The 71% confidence score is what made me look twice. If it had said 94% I might have trusted it more than I should have. The score told me ANNA wasn't sure, which told me I needed to be."

This case illustrates two design principles functioning together. The suggest-only architecture preserved the senior engineer's override authority at a moment when it mattered operationally. The confidence score — part of the explainability interface — gave her the calibrated information she needed to exercise that authority appropriately. The override was not a system failure; it was the system working as designed. And the subsequent model improvement demonstrates the feedback loop that makes ANNA more accurate over time precisely because overrides are treated as professional contributions.

5.4 Comparative Benchmark: ANNA and NetBrain

NetBrain is a commercially deployed network automation and AI-assisted observability platform used by more than one-third of the Fortune 500 and deployed in federal government environments ([NetBrain Technologies, 2025](#))

It has been in continuous development since 2004 and has amassed a body of documented enterprise performance outcomes that provide a credible external reference point for evaluating ANNA's results. The comparison presented in Table 5.4 examines six dimensions: system architecture and classification approach; resolution acceleration; human oversight model; institutional governance integration; adoption maturity and workforce trust; and transferability model.

The comparison is analytical, not competitive. ANNA and NetBrain address different institutional contexts and different layers of the network operations challenge. The purpose of the comparison is not to determine which system is superior — a question that misframes what both systems are — but to illuminate what ASU's implementation achieves in relation to established practice, and where the distinctive contribution of ANNA's approach lies.

Table 5.4: Comparative Analysis — ANNA (ASU AI-NOC) vs. NetBrain

Comparison Dimension	ANNA (ASU AI-NOC)	NetBrain (Commercial Platform)	Analytical Interpretation
System Architecture & Classification Approach	Purpose-built for ASU's specific event taxonomy; trained exclusively on ASU's historical ITSM incident data; classification model updated monthly via analyst override feedback loop	Intent-based automation: generalizable across multi-vendor hybrid environments; uses Dynamic Maps and Network Intent automation rather than ML classification; diagnostics triggered by deviation from codified network intent	ANNA's strength is institutional specificity — it knows ASU's network and improves with every ASU-specific override. NetBrain's strength is multi-environment generalizability. ANNA's precision on Tier 1 events (94.2%) reflects this contextual advantage; NetBrain's breadth enables deployment across thousands of organizations

			without custom training.
Resolution Acceleration (MTTR/TTR Reduction)	40% TTR reduction (Tier 1 events); 31% across all event types (Phase 4, 3-month full deployment)	38%–75% MTTR reduction documented across enterprise deployments; 50%+ reduction reported in ServiceNow-integrated configurations; halving MTTR every 12–18 months cited as product trajectory (NetBrain, 2025)	ANNA's 40% Tier 1 result places it at the lower range of NetBrain's documented enterprise outcomes. However, ASU's result is achieved in a governance-constrained public sector environment, with a suggest-only deployment architecture that deliberately preserves human decision authority — a constraint that NetBrain's autonomous remediation mode does not impose. Adjusted for deployment scope, the comparison is favorable.
Human Oversight Model	Strict human-in-the-loop architecture: Tier 1 auto-route (analyst notified, 5-minute override window); Tier 2 analyst	Configurable: supports both advisory mode (human confirms all actions) and autonomous remediation mode (auto-close, auto-remediation without human initiation). Configurable approval gates for compliance. Some deployments allow auto-	This is the most analytically significant dimension of difference. ASU's governance framework — as a public institution with FERPA obligations and

	confirmation required; Tier 3 senior engineer mandatory. No autonomous remediation at any tier during pilot and early full deployment.	close without human review (NetBrain, 2025).	public accountability — makes autonomous remediation architecturally incompatible with the initiative's governance requirements. ANNA's human-in-the-loop design is a governance necessity, not a technical limitation. NetBrain's configurable model offers flexibility that private-sector organizations can exploit; ASU's model demonstrates what responsible public-sector AI deployment looks like when governance is treated as architecture.
Institutional Governance Integration	Embedded within ASU's AI Governance Council, FERPA compliance architecture, and procurement framework	Commercial platform with configurable compliance features; ITSM integration with ServiceNow enables audit trail and change management governance. No inherent public-sector governance architecture; institutional governance must be layered on top of the platform by the	NetBrain provides the technical infrastructure for governance (audit logs, approval gates, ITSM integration) but does not provide the institutional governance architecture itself.

	from Phase 1. Quarterly Steering Committee oversight. Governance is a first-class design requirement, not a compliance layer.	deploying organization (NetBrain, 2025).	ASU's AI-NOC governance model — the Steering Committee, the FERPA data map — is the institutional contribution that NetBrain cannot supply. This is precisely where ASU's implementation offers a replicable model for other public institutions that must deploy AI within formal accountability structures.
Adoption Maturity & Workforce Trust	Analyst trust survey composite score: 2.7 (pre-deployment) → 3.7 (Month 9). Override rate stabilized at 12% (Tier 1). Co-design participation directly correlated with higher trust scores (4.2 vs. 3.6).	User adoption documented across more than one-third of Fortune 500; no published workforce trust survey data. BT Enterprise reported strong adoption across 2,000+ managed networks after integration into NOC Incident Management Dashboard (NetBrain, 2022).	NetBrain's adoption evidence is volume-based: the number of organizations using the platform. ANNA's adoption evidence is depth-based: measured trust, agency, and behavioral indicators within a specific workforce. This methodological difference reflects the AI-NOC initiative's commitment to the integrated research question — operational performance and

			human trust are co-equal outcomes, not hierarchy.
Transferability Model	ASU's governance architecture, trust-calibration methodology, and phased deployment model are designed as a replicable framework for public-sector institutions. The contribution is organizational and governance design, not a product.	Commercial product transferability: available for purchase and deployment across any enterprise or government environment. Used in more than one-third of Fortune 500 and in federal government environments with GSA Schedule availability (NetBrain, 2025).	NetBrain transfers as a product; ANNA's framework transfers as a governance and organizational model. They are not competing transfer mechanisms — they address different layers of the same challenge. An institution adopting NetBrain still needs the governance architecture, trust-calibration methodology, and workforce change management model that the AI-NOC initiative has developed. These are complementary, not mutually exclusive, contributions to the field.

NetBrain performance data sourced from: NetBrain Technologies (2022, 2025); Network Automation Forum (2025); NetBrain Exchange Community (2026). ANNA data sourced from ASU ITSM platform and internal evaluation instruments.

Three insights from Table 5.4 are worth drawing out analytically before moving to the value creation synthesis.

ANNA's performance is competitive with NetBrain's enterprise outcomes when adjusted for deployment scope. NetBrain's upper-bound outcomes (75% MTTR reduction) reflect configurations with autonomous remediation enabled across mature enterprise environments with years of model refinement ([Network Automation Forum, 2025](#))

ANNA's 40% Tier 1 TTR reduction — expected in the first fifteen months of deployment, in a governance-constrained public-sector environment, with a suggest-only architecture that preserves full human decision authority — is a strong result by any comparative standard. The 31% all-event-type result reflects the expected performance gradient between well-characterized Tier 1 events and the broader event population, which includes novel and complex incidents where AI classification is inherently harder. This gap is not a failure; it is the expected shape of AI-assisted triage maturation.

The human oversight model difference is the most strategically significant finding. NetBrain's configurable autonomous remediation architecture — which allows auto-close and auto-remediation without human initiation — is technically more aggressive than ANNA's suggest-only model ([NetBrain Technologies, 2025](#))

This difference is not a capability gap on ANNA's part. It is a governance design choice imposed by ASU's public accountability environment. FERPA compliance and public institutional accountability make autonomous remediation architecturally incompatible with ASU's governance framework during the current phase of deployment. What this means for the field is significant: public institutions that want to deploy AI in operational systems cannot simply adopt enterprise automation platforms at their most aggressive configuration settings. They need a governance architecture that determines which automation decisions are appropriate for which institutional context — and ANNA's human-in-the-loop model demonstrates what that architecture looks like in practice.

The governance integration dimension reveals what NetBrain cannot supply and ANNA must provide. NetBrain delivers sophisticated technical infrastructure for governance: audit logs, configurable approval gates, ITSM integration, change management workflows ([NetBrain, 2025](#))

But technical governance infrastructure is not institutional governance. The AI Governance Council authorization, the FERPA data architecture, the Steering Committee oversight structure — these are organizational and policy artifacts that no commercial platform can provide. They are the institutional contribution that makes ANNA's deployment legitimate and replicable in a public-sector context. The comparison with NetBrain makes this gap visible — and in doing so, identifies the specific governance design work that other public institutions will need to undertake if they are to deploy AI responsibly in operational systems.

5.5 Evidence of Value Creation: Six Dimensions

The central question of this section is not whether ANNA works — the quantitative and qualitative data presented above establishes that it does, within the boundaries of the

controlled pilot and early Phase 4 deployment period. The central question is: *what kind of value has been created?* Value creation in the AI-NOC initiative is not reducible to TTR improvement or escalation rate reduction, any more than a university's value is reducible to its graduation rate. The initiative was designed to produce value across multiple dimensions simultaneously — and its success must be evaluated on that basis.

Table 5.5 presents the six-dimension value creation framework, tying each dimension to specific evidence and to its institutional significance. This is the framework through which this initiative's contribution to ASU's mission — and to the broader field — is most clearly visible.

Table 5.5: ANNA Evidence of Value Creation — Six Dimensions

Value Dimension	What Changes	Evidence	Institutional Significance
Operational Value	Faster, more consistent triage across all NOC shifts	TTR ↓40% (Tier 1); Escalation rate ↓44%; Backlog ↓44%	Academic continuity protected; student-facing services restored faster; senior engineers freed from avoidable interruptions
Capacity Value	Senior engineering time redirected to strategic work	~230 engineering hours/month recovered from unnecessary escalations	Recovered capacity deployed to predictive analytics development, smart campus infrastructure, and AI-NOC model improvement
Financial Value	Reduction in escalation-driven labor costs and downtime exposure	Estimated 230 hours/month × loaded cost of senior engineer time; downtime reduction	ROI accrues through labor cost avoidance and reduced downtime cost; compounding value

		of 0.07 uptime percentage points	as ANNA's scope and precision grow
Governance Value	Demonstrable public-sector AI governance at the operational level	FERPA compliance architecture validated; AI Governance Council reporting in place; zero compliance events	ASU can point to AI-NOC as evidence that its institutional AI governance commitments are operationalized at the program level — not abstract policy
Workforce Value	Analyst professional development and cognitive elevation	Trust survey composite: 2.7 → 3.7; Override safety: 3.6 → 4.2; Agency sense: 3.4 → 3.9	Analysts transitioning from reactive triage operators to strategic problem-solvers; skill development in human-AI collaboration with increasing market value
Field Contribution Value	A replicable governed sociotechnical model for public-sector AI deployment	Six-dimension analytical framework; governance architecture; trust-calibration methodology; phased deployment with decision gates	First documented public university AI-NOC implementation with embedded governance, trust measurement, and workforce transformation — directly actionable by comparable institutions

The six dimensions in Table 5.5 are not independent. They form a value chain. Operational value — faster, more consistent triage — produces capacity value by freeing senior engineers from avoidable interruptions. Capacity value produces financial value by reducing labor costs and downtime exposure. Governance value protects operational and financial value by ensuring the initiative remains compliant, auditable, and institutionally

legitimate. Workforce value sustains operational value over time by ensuring that the human expertise ANNA depends on for override quality and model learning continues to develop rather than atrophy. And field contribution value — the replicable governance and trust-calibration model — is the institutional dividend that justifies the investment in analytical rigor throughout.

What I want to be precise about is the nature of the field contribution. ANNA is not the first AI-assisted NOC system. NetBrain has been deployed at scale for two decades ([NetBrain Technologies, 2025](#))

What ANNA adds to the field is not a faster classification model or a more sophisticated automation architecture. It adds a **documented, evidence-based model for deploying AI in a public institution** — one that shows how governance, trust-calibration, workforce development, and operational performance can be designed as interdependent outcomes rather than competing priorities. That is the contribution. And it is a contribution the field needs: not more proof that AI can improve MTTR, but proof that AI can do so in a way that a public institution — with its accountability obligations, its workforce responsibilities, and its mission to serve a community — can be proud of.

5.6 Limitations and What We Still Do Not Know

Intellectual honesty requires naming three significant limitations of the evidence presented in this section. First, **the deployment timeline is short. We are reporting from within a controlled pilot, not a completed production deployment.** Fifteen months of operational data — twelve weeks of pilot, three months of full deployment — is not enough to observe ANNA's long-term performance trajectory. Model drift, workforce normalization, and the compounding capacity effects of recovered engineering hours all play out over years. The evidence presented here is real and meaningful; it is also early.

Second, **the workforce sample is small.** Twenty-three analysts and senior engineers is a statistically limited sample for survey analysis. The directional findings are consistent and analytically coherent, but they cannot support strong inferential claims about what the workforce experience data would look like in a larger institutional context. Replication at scale — through the public university AI-NOC consortium proposed in Section 6 — would substantially strengthen the evidentiary foundation.

Third and most importantly, **the causal attribution challenge remains.** The quasi-experimental design establishes a before-and-after comparison, but it cannot rule out all alternative explanations for the observed improvements. Network infrastructure changes, staffing additions, ITSM workflow modifications made independently of ANNA, and the Hawthorne effect of being studied — all are potential contributors to the performance improvements observed ([Shadish, Cook & Campbell, 2002](#)). The evaluation design has addressed these alternatives where possible through period-adjusted comparisons and behavioral triangulation, but absolute causal certainty is not available in operational

research of this kind. What is available is rigorous documentation of what changed, in what direction, and at what magnitude — and that is the appropriate evidentiary standard for a Strategic Implementation Report.

6. Adjustments and Forward Strategy

Every strategic initiative produces surprises — outcomes that differ from projections, risks that materialize earlier or later than expected, and possibilities that only become visible once the work is underway. The ANNA deployment is no exception. What the evidence from Sections 4 and 5 reveals is not a story of failure and course correction; it is a story of a well-designed initiative producing results that are strong in some dimensions, incomplete in others, and generative of new strategic possibilities that were not fully visible at the outset. This section translates that evidence into seven concrete, analytically grounded recommendations.

Ideas without evidence anchors are not recommendations. They are ambitions. Ambitions are appropriate in executive vision documents; they are insufficient in a doctoral implementation report. Every recommendation in this section is therefore anchored to three things: the specific evidence that makes the recommendation necessary or possible, the risk or gap that the recommendation addresses, and the implementation horizon that reflects the governance and resource conditions under which it can responsibly proceed.

This discipline is not merely methodological. It reflects a leadership principle I have come to understand through this initiative: in public institutions, where every resource commitment is a public accountability decision, the credibility of a forward strategy depends entirely on the quality of the evidence that grounds it. An AI governance council, a steering committee, a provost's office — none of these bodies should be asked to authorize the next phase of an initiative based on enthusiasm. They should be asked based on data, analysis, and a clear-eyed account of what the evidence does and does not support.

Table 6.1 presents the full recommendation register — seven evidence-anchored recommendations, each tied to a specific evidence base, a specific risk or gap from the Section 4 register, a priority level, and an implementation horizon. Sections 6.1 through 6.7 develop each recommendation in full analytical prose. Section 6.8 presents the forward implementation roadmap.

Table 6.1: AI-NOC Adjustment and Recommendation Register

#	Recommendation	Evidence Anchor	Risk / Gap Addressed	Priority	Implementation Horizon
R1	Expand ANNA's classification scope to Tier 2 and complex Tier 3 events with enhanced explainability layer	ANNA achieved 94.2% precision on Tier 1 events and 40% TTR reduction on active pilot, validating the model's classification architecture. Tier 2 and complex events remain at 31% TTR reduction — the largest remaining performance gap.	TECH-1 (model drift); CULT-2 (over-reliance risk increases with scope); widening gap between Tier 1 and all-event-type performance	High	Phase 6 (Months 12–18)
R2	Deploy ANNA's predictive analytics capability: shift from reactive triage to pre-incident detection for recurring event patterns	230 engineering hours/month recovered from escalation elimination. Recovered capacity is currently being redeployed to strategic work but is not yet directed	GOV-1 (scope must expand through formal gate); FIN-1 (ROI plateau risk if operational performance gains are not compounded by predictive capability)	High	Phase 6+ (Months 15–24)

		toward systematic pattern analysis. NetBrain's documented trajectory shows MTTR halving every 12–18 months when predictive capabilities are layered onto reactive triage (NetBrain, 2025).			
R3	Recalibrate ANNA's classification thresholds for academic calendar cycles — semester start, finals, summer intersession — to address event volume volatility	Backlog volume fluctuated by up to 38% between peak (semester start) and low (summer intersession) periods during the Phase 4 deployment. Static thresholds optimized for average event volume underperform at both extremes.	TECH-1 (drift risk elevated during volume spikes); FIN-2 (budget overrun risk from unplanned retraining during peak periods)	High	Immediate (Months 10–12)
R4	Strengthen ANNA's	Explainability confidence	CULT-1 (analyst	High	Immediate (Months 10–14)

	explainability interface — the single lowest-scoring trust dimension — through analyst co-design of reasoning displays	scored 3.8/5.0 at Month 9 — the lowest of all five trust dimensions and the only one that analysts consistently cited as a remaining barrier to full adoption confidence in focus groups.	disengagement risk); CULT-2 (over-reliance risk increases when reasoning is opaque); long-term model improvement quality depends on informed override decisions		
R5	Develop and publish ASU's AI governance playbook as a transferable model for public-sector AI deployment	The AI-NOC initiative has produced — through operational experience — a governance architecture (FERPA data map, Steering Committee structure, decision gate criteria, risk register) that no comparable public university AI-NOC deployment has yet documented at this level of analytical rigor.	GOV-2 (stakeholder resistance risk is reduced when the model's external contribution is visible and recognized); field gap in public-sector AI governance documentation	Medium	Year 2 (Months 18–24)

R6	Establish a regional public university AI-NOC consortium to share governance frameworks, model training data, and operational benchmarks	ANNA's classification precision is constrained by the volume and diversity of ASU's historical incident data. A consortium of four to six comparable public universities would multiply the training data available while distributing the governance development cost that each institution would otherwise incur independently.	TECH-1 (model precision plateau risk from single-institution data); FIN-1 (ROI ceiling on single-institution deployment); field gap in collaborative AI governance for higher education	Medium	Year 2–3 (Months 18–36)
R7	Expand AI-NOC integration to smart campus infrastructure — building management systems, physical security, and IoT device networks	ANNA's triage architecture is event-classification agnostic: the same ML classification model that routes network events can be retrained to classify building management	GOV-1 (scope expansion requires Steering Committee vote and Gate 5 criteria); TECH-1 (model drift risk increases with event type diversity); requires data governance review if new	Medium	Year 3+ (Months 30+)

		alerts, access control events, and IoT anomalies. The governance architecture is already in place.	data types include PII		
--	--	--	------------------------	--	--

Priority levels: High = should begin within current phase. Medium = requires Gate 5 criteria + Steering Committee approval. Evidence anchors reference Section 5 data.

6.1 R1: Expand ANNA's Scope to Tier 2 and Complex Events

The most direct evidence-driven recommendation in this report is also the most operationally consequential. ANNA achieved 40% TTR reduction on Tier 1 events — the high-volume, well-characterized alerts where its training data was deepest and its classification confidence highest. The all-event-type result was 31%. That 9-percentage-point gap is not a rounding error. It represents the structured ceiling of a suggest-only Tier 1 deployment, and closing it requires deliberately expanding ANNA's operational scope to the Tier 2 and complex events where the classification challenge — and the performance opportunity — is greatest.

The evidence supports this expansion. ANNA's classification precision grew from 88.4% in pilot week one to 94.2% by week twelve — a trajectory that demonstrates active model learning rather than static performance. The override feedback loop is working. The governance architecture is proven. The analyst workforce is certified and operating with a composite trust score of 3.7/5.0. These are the conditions under which scope expansion is responsible, not merely aspirational.

The expansion carries two risks that must be mitigated in design, not in response. First, Tier 2 events involve more complex diagnostic chains, which means ANNA's explainability layer must work harder — analysts need to understand more nuanced reasoning before they can override intelligently. This makes Recommendation R4 (explainability enhancement) a prerequisite for R1 full deployment, not a parallel workstream. Second, expanding ANNA's scope increases the surface area for model drift: more event types means more dimensions along which network evolution can outpace training data. The monthly precision audit and automated retraining trigger established in Section 4 remain in force and must be recalibrated for the expanded event population before full Tier 2 rollout.

The implementation sequence is therefore: R4 (explainability co-design) launches in Month 10 → Tier 2 pilot on selected event categories in Month 12 → full Tier 2 rollout at Gate 5 Q2 review in Month 15, contingent on $\geq 90\%$ Tier 2 precision and explainability score $\geq 4.0/5.0$. Complex Tier 3 event support follows in Phase 6B, where ANNA provides diagnostic context and historical precedent without classification authority.

6.2 R2: Deploy Predictive Analytics — From Reactive Triage to Pre-Incident Detection

ANNA was built as a triage system: it classifies events after they are detected. This is the right architecture for Phase 3 and 4, where the priority was proving that AI-assisted classification could improve resolution speed and reduce escalation. But the evidence from Phase 4 — specifically the 230 engineering hours recovered per month from eliminated unnecessary escalations — creates a strategic resource that the initiative has not yet fully deployed: senior engineering capacity directed toward systematic pattern analysis of ASU's incident history.

The data is available. ASU's ITSM platform holds years of time-stamped incident records, resolution outcomes, and network state data from the same monitoring infrastructure that feeds ANNA's classification engine. The analytical capability is available: the same Enterprise Technology team that built ANNA's classification model can apply ML pattern-recognition to the historical incident corpus to identify recurring failure signatures — the infrastructure conditions that reliably precede high-volume event periods. What has been missing is the engineering time to do that analysis. The capacity recovery from escalation elimination is now providing it.

The research literature on AI-assisted NOC operations identifies predictive capability as the natural maturation trajectory beyond reactive triage ([NetBrain Technologies, 2025](#); [Booz Allen Hamilton, 2025](#))

NetBrain's documented outcomes show MTTR halving every 12–18 months when predictive analytics are layered onto reactive automation ([NetBrain Technologies, 2025](#))

The ASU implementation is positioned to achieve a comparable trajectory — not by purchasing a commercial predictive analytics add-on, but by deploying the recovered engineering capacity that ANNA's escalation reduction has made available. This is the compounding value of the initiative: operational improvement funds the next layer of capability, which funds the next layer after that.

The predictive analytics pilot will target three recurring event categories first — the incident types that appear most frequently in ANNA's Tier 1 classification logs and that follow the most predictable pre-incident signatures. Success is defined as pre-incident detection of 15% or more of these recurring event types within the pilot period, meaning

ANNA flags the signature before the event generates an alert. Gate 5 Q3 review at Month 21 is the go/no-go decision point for expansion.

6.3 R3: Academic Calendar Calibration — An Immediate Adjustment

This recommendation is the most urgent in the register, and the most operationally straightforward. The evidence from Phase 4 shows that ANNA's static classification thresholds — optimized during the pilot on event volumes representative of mid-semester conditions — underperform at both extremes of the academic calendar. At semester start, when event volume spikes by up to 38% above the mid-semester baseline, ANNA's confidence thresholds generate more Tier 2 escalations than necessary because the model has not seen enough high-volume data to classify confidently under peak conditions. At summer intersession, when event volume drops by a comparable margin, the same thresholds generate occasional false positives — events classified as requiring analyst attention that would resolve automatically under low-load conditions.

The solution is not a new model. It is a calibration adjustment: reconfiguring ANNA's confidence thresholds for four distinct calendar periods (semester start, mid-semester steady state, finals, summer intersession) based on the event volume and composition data collected during Phase 4. This calibration is a Phase 6 governance responsibility — it requires Steering Committee notification but not a full gate review — and it should be completed before the first post-Phase-4 semester start.

I want to be direct about why this is classified as an immediate adjustment rather than a future recommendation. The academic calendar is not a surprise. ASU's rhythm of enrollment, instruction, and assessment has been known since before Phase 1. The fact that ANNA's calibration does not account for it is the kind of implementation gap that retrospective analysis reveals and that forward planning must address. This is what the evidence-to-insight-to-recommendation framework is for: not to celebrate what worked, but to identify what needs to be fixed while there is still time to fix it cleanly.

6.4 R4: Strengthen ANNA's Explainability Interface

The trust survey data from Section 5 is unambiguous on one point: explainability confidence (3.8/5.0) is the lowest-scoring trust dimension at Month 9, and it is the dimension that analysts most consistently cite in focus groups as the remaining barrier to full adoption. This is not a finding I can characterize as satisfactory and move past. A system that analysts trust because it is usually right, but whose reasoning they cannot consistently follow, is a system that is one high-profile misclassification away from a trust collapse. The explainability interface is where ANNA's long-term operational resilience is built or lost.

The specific gap that focus groups identified is granular: analysts understand ANNA's output (what it classified the event as) but do not consistently understand ANNA's reasoning (which features of the event drove that classification, and with what confidence weighting). ANNA currently displays a confidence score and a classification label. Analysts want to see — in plain language, not in model parameters — why ANNA made the call it made. "High CPU on Router-Core-12 combined with three similar events in the last six hours triggered a Tier 2 routing" is an explainability output an analyst can evaluate and either confirm or override with informed judgment. A confidence score of 87% and a classification label is not.

The design work for this improvement belongs to the analysts who will use it, not to the engineering team that will build it. I am recommending a structured co-design series — four sessions over three months, facilitated by the Director of Organizational Development with Enterprise Technology participation — in which NOC analysts define the specific reasoning display that would make override decisions feel informed rather than arbitrary. This is consistent with Shneiderman's (2020) human-centered AI design principle and with the co-design methodology that produced the decision authority matrix in Phase 5. The output of the co-design series is an explainability interface specification that Enterprise Technology implements in ANNA's production deployment by Month 14.

The target is an explainability confidence score of 4.0/5.0 or higher by Month 15. If that target is not met, it is a signal not that the improvement failed but that the co-design process needs another iteration — because the gap between what the engineering team thinks is clear and what the analyst workforce finds legible is exactly the kind of gap that co-design exists to close.

6.5 R5: Publish the AI Governance Playbook

One of the clearest findings from the comparative analysis in Section 5.4 is that NetBrain — a sophisticated, mature, commercially available network automation platform — cannot provide what ASU has developed through the AI-NOC initiative: an institutional governance architecture for AI deployment in a public-sector environment. The FERPA data map, the AI Governance Council authorization framework, the decision gate criteria, the risk register with quantified monitoring triggers — none of these are features of a commercial platform. They are organizational artifacts that ASU has built, refined through operational experience, and validated against real governance requirements. They are also artifacts that no comparable public university currently has access to in documented, replicable form.

The recommendation is to formalize this governance architecture into a public-facing AI Governance Playbook — a document written not as an ASU internal policy but as a practitioner's guide for senior technology leaders at other public universities who want to deploy AI in operational systems and need a governance framework they can adapt rather than invent from scratch. The audience is the Chief Information Officer or Senior Director of Digital Infrastructure at a public institution who has read about AI-assisted NOC operations

and is asking: how do I do this responsibly, within our public accountability obligations, without starting from zero?

The playbook is not a research paper. It is a leadership tool: structured around the six phases of the ANNA implementation, organized by the five governance domains from Section 4, and written in the voice of a practitioner who has lived through the decisions it describes. It should include a template FERPA data architecture review, a decision gate framework adaptable to different institutional contexts, and the workforce trust-calibration methodology — because these are the elements that the field does not currently have and that the AI-NOC initiative has now produced.

Publication through EDUCAUSE — the primary professional association for higher education IT leadership — and through the Thunderbird School of Global Management's practitioner publication channels would ensure the playbook reaches the audience that needs it. The field contribution value identified in Section 5.5 is only realized if the contribution is shared.

6.6 R6: Establish the Public University AI-NOC Consortium

The single most significant technical constraint on ANNA's long-term performance is the volume and diversity of its training data. ANNA's classification model is trained on ASU's historical ITSM incident data — a corpus that is large by single-institution standards but that reflects only one institution's network topology, one institution's monitoring tool configuration, and one institution's incident taxonomy. This is appropriate for Phases 3 and 4, where institutional specificity is a classification advantage. It becomes a constraint in Phase 6 and beyond, when ANNA is attempting to classify increasingly complex and novel event types where ASU's historical incident data offers fewer precedents.

A consortium of four to six comparable public research universities — institutions with similar network scale, similar monitoring tool ecosystems, and similar public governance requirements — would multiply the available training data while distributing the governance development cost that each institution currently incurs independently. If ASU, the University of Arizona, Arizona State's peer institutions in the Pac-12, and other large public research universities in similar digital infrastructure contexts share anonymized incident data (under a data-sharing agreement that preserves FERPA compliance and institutional data sovereignty), the resulting training corpus would be materially richer than any single institution can build alone.

The consortium also serves a governance function that goes beyond data sharing. When four to six public universities are operating comparable AI-NOC systems under a shared governance framework, the field has a collaborative evidence base for evaluating what works, what does not, and what the governance requirements of responsible public-sector AI deployment actually look like in practice. This is the kind of field-building contribution that individual institutional implementations cannot produce, and that the

EDUCAUSE community — which identified AI governance as a top-ten strategic priority for higher education in 2024 ([EDUCAUSE, 2024](#)) — is positioned to facilitate.

I am proposing that ASU take the convening role in forming this consortium, for two reasons. First, ASU has the most advanced implementation and the most developed governance architecture among comparable institutions — it has something substantive to offer, not merely a vision to pitch. Second, ASU's size, research profile, and Charter commitment to broad impact position it as a natural leader in collaborative higher education initiatives of this kind. The first consortium meeting — a structured working session with senior technology leaders from prospective member institutions — should take place in Year 2, following the publication of the governance playbook in R5.

6.7 R7: Expand to Smart Campus Infrastructure

The seventh recommendation is the most forward-looking and the most conditional: expanding ANNA's event classification architecture to smart campus infrastructure — building management systems, physical access control, environmental monitoring, and IoT device networks. I include it in this section not because it is ready to execute but because the evidence from ANNA's deployment makes it credible in a way it was not before Phase 4, and because strategic planning for Year 3 needs to begin before Year 2 is over.

The technical case for smart campus expansion is straightforward: ANNA's ML classification architecture is event-type agnostic. The same model that classifies network triage events can be retrained on building management alerts, access control anomalies, and IoT sensor data — provided the training corpus is adequate and the classification taxonomy is well-defined. The governance architecture is already in place. The institutional trust in AI-assisted operational systems has been built through the network triage deployment. The incremental governance cost of expanding to smart campus infrastructure is lower than the cost of building a new governance architecture for a new system from scratch.

The risks are real and must drive the sequencing. Smart campus data introduces new PII considerations — access control logs, building occupancy patterns, and environmental sensor data can contain or imply information about identifiable individuals in ways that network event data typically does not. This means the data governance review must be revisited before smart campus data enters ANNA's classification pipeline. The FERPA data map must be extended. The data governance review must confirm that the proposed data architecture keeps smart campus telemetry appropriately isolated from student record systems.

The recommendation is therefore conditional: smart campus expansion proceeds if and only if Gate 5 Year 3 criteria are met (network AI-NOC operating at $\geq 40\%$ all-event-type TTR reduction, Steering Committee vote approving expanded scope, data governance authorization covering new data types, and legal review of data architecture). The value of

naming this recommendation now is not to commit to it but to ensure that the governance preparation work — data governance scoping, data architecture design, legal review — begins early enough that it does not delay execution when the performance and resource conditions are ready.

6.8 Implementation Roadmap: Four Horizons

Table 6.2 presents the forward implementation roadmap, organizing the seven recommendations across four time horizons: Immediate (Months 10–12), Phase 6A (Months 12–18), Phase 6B (Months 15–24), and Year 3+ (Months 30 and beyond). The roadmap is designed to be governance-realistic: no horizon advances without the gate criteria specified in Section 3, and no resource commitment is made beyond the immediate horizon without Steering Committee authorization. This is how a public institution responsible to its community should plan: ambitiously, but within the constraints that accountability imposes.

Table 6.2: AI-NOC Forward Implementation Roadmap

Horizon	Active Recommendations	Primary Owners	Governance Gate	Success Indicators	Strategic Intent
Immediate (M10–12)	R1 scope planning R3 calendar calibration R4 explainability co-design launch	NOC Ops Mgr Enterprise Tech Dir. Org. Dev.	Gate 5 Q1 review	TTR all-event-type $\geq 35\%$ Explainability score ≥ 4.0	Consolidate pilot gains. Close the Tier 1–all-events performance gap. Fix the explainability gap before it limits long-term adoption. Protect what has been built.
Phase 6A (M12–18)	R1 Tier 2 full rollout R5 governance playbook draft	Sr. Director, DI	Gate 5 Q2 review	Tier 2 precision $\geq 90\%$	Scale ANNA's scope responsibly. Begin

		Steering Committee		Playbook draft complete	externalizing the governance contribution by publishing the playbook. Establish ASU as a field leader in public-sector AI-NOC governance.
Phase 6B (M15–24)	R2 predictive analytics pilot R5 playbook published R6 consortium formation	Sr. Director, DI Enterprise Tech Provost engagement	Gate 5 Q3–Q4 review	Pre-incident detection >15% of recurring events ≥3 consortium members signed	Shift ANNA from reactive to predictive. Launch the consortium infrastructure. Multiply institutional and field-level impact by distributing governance development cost.
Year 3+ (M30+)	R7 smart campus expansion R6 consortium operational R2 predictive NOC at scale	AI-NOC Steering Cmte VP IT Enterprise Technology	Annual strategic scope review	Smart campus pilot launched Consortium ≥5 institutions Predictive triage >25% of events	Institutionalize AI-NOC as a permanent strategic capability. Operate the consortium. Expand the architecture to smart campus operations. Lead the field.

M = Month from Phase 4 full deployment launch. All horizons require Gate 5 criteria met before advancement. Year 3+ requires Steering Committee strategic scope vote.

The roadmap reflects a deliberate sequencing logic. The immediate horizon closes gaps in what has already been built — calibration, explainability, scope readiness — before extending the system's reach. Phase 6A scales what is proven before moving toward what is predicted. Phase 6B is where the initiative's external contribution takes institutional form: the playbook published, the consortium launched, the predictive capability piloted. Year 3+ is the horizon at which ANNA becomes something qualitatively different from what it is today: not a network triage assistant but the classification engine of an intelligent, predictive, multi-domain campus infrastructure capability.

I want to be clear about what the roadmap does not claim. It does not promise that all seven recommendations will be executed on schedule. Implementation timelines in public institutions are subject to budget cycles, procurement constraints, governance processes, and leadership transitions that no planning document can fully anticipate. What the roadmap does is establish the analytical logic of the sequence — why R4 before R1, why R5 before R6, why R3 immediately rather than deferred — so that when implementation conditions change, the decisions about what to accelerate, defer, or modify are made from a principled foundation rather than from improvisation.

Recommendation Prioritization: Impact, Feasibility, and Sequencing

The seven recommendations are not equally urgent, equally feasible, or equally independent. Table 6.3 presents an explicit prioritization framework — scoring each recommendation on impact and feasibility, assigning a time-to-value horizon, and naming the sequencing logic that connects them. The framework is designed to support the Steering Committee's resource allocation decisions: not every recommendation should begin simultaneously, and the dependencies between them are real.

Table 6.3: Recommendation Prioritization Matrix — Impact, Feasibility, and Sequencing

Rec	Impact (1–5)	Feasibility (1–5)	Time-to-Value	Priority Tier	Sequencing Logic
R3	4	5	Immediate (Month 10)	Do Now	Highest feasibility — calibration adjustment, not new development. Highest urgency — every academic cycle without it produces degraded performance. Zero dependencies.
R4	5	4	Short-term (Months 10–15)	Do Now	Directly addresses lowest-scoring trust dimension (3.8/5.0). Blocks R1 — Tier 2 expansion is inadvisable without explainability improvement. Co-design resources already engaged.

R1	5	4	Short-term (Month 12–15)	Plan Now	Highest operational impact — extends ANNA's TTR benefit to all event types. Depends on R4 (explainability must improve first). Laboratory validation at 87% Tier 2 precision supports confidence.
R5	4	4	Medium-term (Months 12–18)	Plan Now	Low marginal cost — playbook is synthesized from documentation already produced. High field impact. Builds ASU's external positioning. Depends on Phase 4 completion for full evidentiary basis.
R2	5	3	Medium-term (Month 18+)	Schedule	Transformational long-term impact (reactive → predictive). Technically demanding — requires recovered engineering capacity from R1 success. Dependencies: R1 must be validated first.
R6	4	3	Long-term (Month 18–24)	Schedule	Multiplies training data diversity and distributes governance cost. Requires R5 (playbook) as the consortium's shared artifact. Convening role depends on ASU's demonstrated leadership.
R7	3	2	Year 3+	Conditional	Technically feasible but governance-intensive. PII scope expansion requires dedicated data architecture review. Conditional on Gate 5 Year 3 criteria and Steering Committee strategic vote.

Impact and Feasibility scored 1 (low) to 5 (high). Priority Tier: Do Now = initiate within current phase; Plan Now = design and resource in current phase, execute next; Schedule = future horizon pending gate criteria; Conditional = dependent on external criteria.

The most important sequencing constraint in Table 6.3 is the R4 → R1 dependency: Tier 2 scope expansion (R1) should not proceed until the explainability interface improvement (R4) is sufficiently advanced that analysts can make informed override decisions on the more complex diagnostic chains that Tier 2 events involve. Deploying R1 before R4 risks an over-reliance failure mode precisely where the diagnostic stakes are highest.

6.9 The Institutional Transformation Underway

The seven recommendations in this section share a common logic that goes deeper than the evidence anchors that justify each individually. Together, they describe the trajectory of an institutional transformation — not just a technology upgrade — that the AI-NOC initiative has set in motion.

Before ANNA, ASU's Digital Infrastructure organization was operationally competent and strategically constrained. It managed a complex network environment with skilled people operating largely manual processes, working hard to keep pace with an event volume that was growing faster than headcount could scale. That organization is now something different: it has demonstrated that AI can be deployed within a public institution's governance architecture without sacrificing accountability, and it has produced a workforce that is developing new capabilities — human-AI collaboration, systematic pattern analysis, strategic infrastructure design — that the pre-ANNA organization could not develop because its senior engineers were too busy triaging tickets.

That shift — from reactive operations to strategic infrastructure leadership — is what I mean when I say that the AI-NOC initiative is a transformation and not a deployment. The 40% TTR reduction is real and it matters. But what it makes possible — the recovered capacity, the predictive analytics capability, the consortium, the playbook, the smart campus vision — is the initiative's true institutional value. And that value compounds. Every month that ANNA operates, the model improves, the trust deepens, the evidence base grows, and the organization becomes more capable of the next thing. That is what a strategic transformation is supposed to do. The evidence in this report suggests it is happening.

7. Conclusion and Next Steps

At the beginning of this report, I posed an integrated research question: ***How can AI-enabled triage simultaneously improve operational performance — measured through TTR, escalation rate, and uptime — and reshape trust and agency in human-AI teams within a public-sector digital infrastructure environment?*** The evidence across Sections 3 through 6 constitutes my answer. But an answer to a doctoral research question is not the same thing as a conclusion. A conclusion is an accounting: what was at stake, what was demonstrated, what it changes, and what it demands of the people and institutions who take it seriously.

This section delivers that accounting. It is organized around the three questions that are necessary for a conclusion that does not merely summarize but actually contributes — to the institution, to the field, and to the broader project of responsible AI deployment in public-sector organizations. The three questions are: What changes institutionally? What scales next? What is the model contribution to the field?

I address each question directly, without the hedging that comes from uncertainty and without the overclaiming that comes from wanting the work to matter more than the evidence supports. The AI-NOC initiative is not finished — it is fifteen months into a multi-year transformation. But what has been built and demonstrated in those fifteen months is real, analytically defensible, and consequential enough to warrant a decisive conclusion.

7.0 The Three Outcomes This Initiative Was Designed to Produce

Before answering the three forward-looking questions, I want to name what the initiative was designed to prove — because these three outcomes are the frame through which every result in this report should be read. The AI-NOC initiative was not designed to maximize a single metric. It was designed to demonstrate that three outcomes the field has too often treated as competing are in fact interdependent: **operational efficiency**, **governance integrity**, and **human agency**. The case for this interdependence is not philosophical. It is empirical, and the evidence is now in.

Operational Efficiency

Efficiency is the most visible outcome and the easiest to quantify. ANNA has demonstrated a 40% reduction in mean TTR on Tier 1 events, a 44% reduction in escalation rate, and a 44% reduction in incident backlog in the active pilot period, with approximately 230 engineering hours recovered per month within the current pilot scope. System uptime has improved from 99.87% toward 99.94% across the measurement period to date. These numbers represent real minutes of restored service, real reductions in academic disruption, and real capacity — formerly consumed by reactive triage — now available for the strategic infrastructure work that ASU's mission demands.

But efficiency is not the initiative's terminus. It is its fuel. Every hour recovered from avoidable escalation is an hour a senior engineer can direct toward predictive analytics, infrastructure architecture, or AI governance development. The efficiency gains compound — they do not simply accumulate. This is why the 40% TTR reduction matters more than its face value suggests: it is the resource base for everything the forward strategy in Section 6 proposes.

Governance Integrity

Governance integrity is the outcome that distinguishes this initiative from a private-sector AI deployment. As a public institution, ASU is accountable not only for what it achieves but for how it achieves it — to students, to faculty, to taxpayers, to accreditors, and to the regulatory frameworks that govern the handling of student data. The AI-NOC initiative operated within formal AI governance structures from Phase 1: a data governance authorization was secured before workforce experience data was collected; a FERPA data architecture was validated before any data flowed through ANNA's pipeline; the AI Governance Council authorized the initiative before deployment began; and the Steering Committee received quarterly performance and compliance reporting throughout Phases 3 and 4.

The result to date is a zero-compliance-event record across the Phase 3 pilot and the Phase 4 deployment period in progress — not because the risks were small, but because the governance architecture made them manageable. This is the evidence that governance integrity and operational performance are not in tension. The governance structures that slowed the initiative's early phases also made its results more trustworthy, more defensible, and more replicable. An AI deployment that achieves 40% TTR reduction but generates a FERPA breach is not a success — it is a liability. ASU's deployment achieved the performance and protected the institution. That is what governance integrity looks like in practice.

Human Agency

Human agency is the outcome that required the most deliberate design and that is hardest to measure — and it is the one I am most committed to defending as a genuine outcome rather than a rhetorical flourish. The AI-NOC initiative was explicitly designed so that analysts would end the deployment with more professional agency than they started with, not less. This meant the suggest-only architecture — ANNA recommends, humans decide, always. It meant the decision authority matrix, which named override as a professional responsibility rather than a system failure. It meant co-design sessions that gave analysts genuine input into the classification taxonomy and the explainability interface. And it meant treating analyst resistance as information rather than a change management problem to be solved.

The evidence that these design choices worked is in the survey data. The trust composite has risen from 2.7 to 3.7 across the pilot period to date. Psychological safety in overriding ANNA has reached 4.2/5.0 — the highest-scoring trust dimension. And the

qualitative finding from focus groups is the one I find most significant: analysts report feeling not replaced by ANNA but elevated by it. They are spending less time on the incidents they have diagnosed a hundred times before and more time on the ones that actually require what only they can bring. That shift — from reactive triage operator to strategic problem-solver — is the human agency outcome this initiative was designed to produce. The data says it happened.

These three outcomes are the initiative's integrated argument. Efficiency without governance integrity is institutional recklessness. Governance integrity without efficiency fails to justify its investment. Efficiency and governance without human agency produces a workforce that quietly routes around the system — because no AI deployment survives a workforce that has collectively decided not to trust it. The AI-NOC initiative demonstrates that all three can be achieved simultaneously, in a public institution, at operational scale. That demonstration is the foundation on which everything in this conclusion rests.

7.1 What Changes Institutionally

The most important institutional change the AI-NOC initiative is producing through the active pilot is not the 40% TTR reduction, as significant as that is. It is the emerging structural proof — documented, governed, and measured in a controlled environment — that artificial intelligence can be deployed within a public university's accountability architecture without compromising the integrity of that architecture. Before the AI-NOC, that proposition was theoretical at ASU. It is now empirical.

Table 7.1 organizes the institutional changes across four dimensions — structural, operational, cultural, and governance — and traces each dimension from what has changed in the pilot period so far, through what scales next in Phase 6, to the long-term institutional horizon. The table is deliberately prospective: a conclusion that only looks backward at what has been accomplished misses the point of an implementation report, which is to orient the institution toward what the evidence makes possible.

Table 7.1: Institutional Change Across Four Dimensions — Now, Next, and Long-Term

Dimension	What Changed (Now)	What Scales Next	Long-Term Institutional Horizon
Structural	Escalation hierarchy flattened: ANNA routes ~80% of Tier 1	Predictive analytics capability embedded in Phase 6: senior	Long-term: emergence of hybrid roles combining

	events without senior engineer involvement. Two NOC analyst roles redefined — from reactive triage operators to AI-oversight specialists responsible for override quality, model calibration, and performance monitoring.	engineers designing pattern-detection systems rather than diagnosing individual incidents. Engineering roles evolving toward data science and infrastructure architecture.	network engineering expertise with AI governance responsibility — a workforce profile that does not yet formally exist in higher education IT and that ASU is now developing ahead of the market.
Operational	NOC throughput improved structurally: 40% faster Tier 1 resolution, 44% escalation reduction, 44% backlog reduction. These are not one-time gains — they are the new operational baseline from which Phase 6 improvements compound.	Predictive analytics shifts the NOC from reactive to anticipatory. The question changes from 'how quickly can we restore service?' to 'how do we prevent the failure before it generates an alert?'	Smart campus integration (R7) extends ANNA's classification architecture beyond network events — the same governance model applied to building management, access control, and IoT telemetry across ASU's physical and digital infrastructure.
Cultural	Analyst relationship to AI shifted from skepticism (trust composite 2.7/5.0 pre-deployment) to functional confidence (3.7/5.0 at Month 9). Override authority normalized as a professional responsibility, not a system override.	Co-design methodology institutionalized: analysts expect to shape the tools they work with. This expectation — that technology deployment involves workforce co-ownership — will carry forward to every	ASU Digital Infrastructure positioned as a learning organization in the AI governance domain: one that generates transferable governance knowledge, not just operational outcomes. The consortium and

		subsequent AI initiative.	playbook formalize that identity externally.
Governance	FERPA architecture validated, AI Governance Council reporting in place. Zero compliance events across Phase 3 and 4. Public accountability requirements have been operationalized at the program level.	Governance playbook (R5) converts operational experience into transferable institutional knowledge. ASU's governance architecture becomes a field resource — not proprietary, but contributory.	Consortium (R6) distributes governance development cost across public institutions, making responsible AI deployment economically feasible for universities that cannot build the architecture from scratch independently.

Source: Sections 4, 5, and 6 of this report. Long-term horizon reflects Recommendations R5–R7 from Section 6.

Three institutional changes from Table 7.1 deserve analytical emphasis beyond the table.

The redefinition of what a senior network engineer does. Before ANNA, the primary work of ASU's most experienced NOC engineers was event diagnosis under time pressure — skilled, necessary, and chronically oversubscribed. Through the active pilot, that work is still there, but it is beginning to occupy a fundamentally different proportion of their professional day. The 230 hours recovered monthly from eliminated unnecessary escalations represent not just labor cost savings but cognitive bandwidth — the condition under which engineers can think at the systems level rather than the incident level. The organization has not added engineers. It has elevated them. That is an institutional change that compounds: every month ANNA operates, the engineers who are freed from reactive triage become more capable of the predictive and architectural work that will define the next phase of ASU's digital infrastructure strategy.

The normalization of AI governance as operational practice, not compliance exercise. One of the risks I identified at the outset of this initiative was that governance — the FERPA compliance architecture, the AI Governance Council authorization — would be

treated by the implementation team as an obstacle to be cleared rather than a structure to be embedded. The evidence at Month 9 is that this risk was mitigated. The governance structures are not peripheral to ANNA's operation; they are part of it. The Steering Committee meets quarterly and receives live KPI data. The monthly precision audit feeds directly into the retraining protocol. The FERPA data map is a living document reviewed at each governance checkpoint. This is what it looks like when governance is treated as architecture — and it is an institutional capability that will outlast ANNA's specific deployment, applicable to every subsequent AI initiative ASU undertakes.

The workforce's changed relationship to AI-mediated work. A trust composite that began at 2.7/5.0 and has reached 3.7/5.0 at the Month 9 measurement point is a number. What it represents is something harder to quantify: a workforce that entered this initiative with legitimate anxiety about what AI-assisted operations would mean for their professional identities and that emerged from the pilot with a substantially different answer than they feared. They are not less expert because ANNA exists. They are differently expert — capable of directing their expertise toward the problems where human judgment is irreplaceable, while delegating the classification work that was always beneath the level of what their expertise made possible. That shift in professional self-understanding is the cultural change that will sustain the initiative when the technology evolves, when new engineers join the team, and when the next AI system is proposed.

7.2 What Scales Next

The seven recommendations in Section 6 define what scales next with analytical specificity. This subsection addresses the strategic logic that connects them — the reason why the sequence matters and what the cumulative trajectory of that sequence represents.

Three scaling trajectories are underway or in design simultaneously, and they are designed to reinforce one another.

Capability scaling. ANNA's operational scope will expand from Tier 1 events (40% TTR reduction demonstrated in pilot) through Tier 2 and complex events (R1), and eventually to smart campus infrastructure (R7). Each expansion is conditioned on demonstrated performance at the prior scope level — this is what stage-gating looks like in practice, not in theory. The capability trajectory also includes the shift from reactive triage to predictive analytics (R2): the most consequential technical evolution the initiative will undergo, and the one that will require the most from the engineering team that the escalation recovery is now freeing. The question that used to define the NOC — how fast can we resolve this? — gives way to the question that defines a strategically mature infrastructure organization: how do we prevent this from happening at all?

Governance scaling. The governance architecture built for ANNA — the Steering Committee structure, the decision gate framework, the risk monitoring cadence — is not proprietary to network triage. It is a governance model for public-sector AI deployment.

Publishing it as a practitioner's playbook (R5) converts internal operational experience into an external institutional contribution. Establishing the consortium (R6) distributes both the benefit and the development cost of that governance architecture across multiple public universities simultaneously. The governance scaling trajectory is the one that gives the AI-NOC initiative its broadest institutional significance — because the problem of governing AI responsibly in public institutions is not an ASU problem. It is a sector-wide problem, and ASU's fifteen months of operational experience now position it to contribute to the sector-wide solution.

Impact scaling. The most direct measure of the initiative's growing impact is the compounding of its value dimensions. Operational value — faster triage, fewer escalations — produces capacity value, which produces the engineering time for predictive analytics, which produces earlier incident detection, which reduces downtime, which protects academic continuity more reliably, which advances ASU's mission. Financial value compounds as recovered engineering hours are redirected toward work that generates institutional capability rather than merely restoring equilibrium. Field contribution value scales as the playbook is published, the consortium is formed, and the governance model is adopted and adapted by institutions that would otherwise spend years reinventing what ASU has already built. The initiative does not need to be replicated to scale its impact. It needs to be documented and shared — and that is precisely what Recommendations R5 and R6 are designed to accomplish.

7.3 What Is the Model Contribution to the Field

The model contribution of the AI-NOC initiative is examined in full in Section 8.3. The brief answer is this: the contribution is not a classification algorithm, a monitoring architecture, or a specific governance policy. It is a governed sociotechnical framework for deploying AI in public-sector operational systems — one that integrates performance architecture, trust-calibration methodology, and governance design as a single system, and demonstrates through operational evidence that all three can be achieved simultaneously. Section 8.3 names the four specific contributions and explains what each adds to the field that did not previously exist in published form.

7.4 Leadership Reflection: What This Initiative Required

I want to be honest about what this initiative required of me as a leader, because the leadership dimension is inseparable from the analytical one in a Doctorate in Professional Practice. The institutional analysis and the evidence tables are my scholarly voice. This subsection is my practitioner voice — and it matters as much.

Leading the AI-NOC initiative required navigating a tension I did not fully anticipate at the outset: the tension between moving with the speed that operational improvement demands and building the trust that durable AI adoption requires. These two imperatives

pull in opposite directions. Speed says: deploy ANNA broadly, demonstrate results quickly, capture the efficiency gains before the institutional window closes. Trust says: go slowly enough that analysts understand what is happening, have genuine input into how it happens, and develop the calibrated confidence in ANNA that prevents both over-reliance and rejection. The performance pressure is real — every month the initiative is not fully deployed is a month of avoidable downtime and unnecessary escalations. But so is the trust imperative — a workforce that does not trust the system will find ways to route around it, and no amount of technical capability survives a workforce that has decided, quietly and collectively, that the system does not deserve their confidence.

I resolved this tension through a principle I would now name explicitly: **trust is engineered through transparency, not assumed through performance.** This means that ANNA's explainability layer was a governance requirement before it was a feature request. It means that the decision authority matrix was published before ANNA went live, not after adoption problems surfaced. It means that analyst overrides were celebrated in team communications as evidence of professional judgment, not quietly tracked as indicators of adoption failure. These were deliberate design choices — and they were choices, which means they could have gone differently. A leader who prioritized speed over trust would have made different choices. The evidence suggests that the choices I made produced better long-term outcomes, both for the initiative's operational performance and for the workforce's professional experience of the transformation.

Three leadership insights crystallized through this work.

Governance is a leadership tool, not a constraint. Every external governance requirement — the AI Governance Council authorization, the FERPA compliance review — could have been experienced as bureaucratic friction. I chose to experience them, and to frame them to my team, as institutional credibility builders. The governance rigor that made the initiative slower also made it more defensible, more trustworthy to the workforce, and more replicable to other institutions. A technically superior AI system deployed without governance integrity would have produced worse outcomes than a moderately capable system deployed with full governance compliance. Governance is not the price of working in a public institution. It is the architecture of institutional legitimacy.

AI transformation is a cultural intervention first. The classification model is necessary but not sufficient. What determines whether a human-AI operational team actually produces better outcomes than a human team alone is not the model's accuracy — it is the quality of the relationship between the analysts and the system they are asked to trust. Building that relationship required change management investments that a purely technical implementation would not have made: co-design sessions, structured focus groups, explicit decision authority frameworks, leadership communications that named the workforce's anxieties rather than dismissing them. These investments paid returns that showed up in the trust survey data and in the focus group narratives — in the analyst who said he started trusting ANNA when it showed him not just what it classified but why.

The outcome is not just improved operations — it is a more capable organization.

This is the insight that I think matters most for the field, and that I want to state as precisely as I can. ASU's Digital Infrastructure organization is not better at the same thing it was doing before ANNA. It is doing something different — something that requires different capabilities, different professional identities, and different relationships between its people and its tools. That organizational transformation is not a side effect of improved TTR. It is the point. The 40% TTR reduction is the evidence that the transformation is real. The transformation itself is the value.

7.5 Final Positioning Statement

The AI-NOC is not an automation initiative. It is not a cost-reduction exercise. It is not a technology pilot that will prove a point and then be decommissioned.

The AI-NOC is a governed sociotechnical transformation — the deliberate redesign of how a public institution achieves reliability, deploys human expertise, and fulfills its accountability obligations in an era of AI-enabled operations. That transformation is now institutionalized at ASU. It is also, through the governance playbook and the consortium, in the process of becoming available to the broader community of public universities that face the same structural challenge ASU faced three years ago: how to scale operational reliability in alignment with a growing, digitally dependent community, without scaling headcount proportionally, without sacrificing governance integrity, and without treating the workforce as a constraint on efficiency rather than a strategic asset.

The outcome I am most proud of is not the TTR reduction the pilot has produced, though that matters. It is not the escalation rate improvement, though that represents real recovered capacity. It is the answer that the AI-NOC initiative is beginning to provide to a question the field has been asking without a practitioner-level response: can AI be deployed in a public institution in a way that makes the institution simultaneously more capable and more trustworthy? The answer this report documents, with evidence and across fifteen months of operational experience, is yes.

That answer is not a guarantee for every institution that attempts what ASU has attempted. The conditions that have made AI-NOC's pilot possible — committed executive sponsorship, a governance architecture that was treated as a design requirement rather than a compliance burden, a workforce that was given genuine co-ownership of the system it was asked to adopt, and a leadership team that understood that trust and performance are interdependent rather than competing priorities — are reproducible. But they require deliberate choices, not just technical capability.

The next question — the one this conclusion cannot answer, but that the institutions who read it will have to answer for themselves — is whether they are willing to make those choices. The evidence from ASU suggests it is worth it.

8. The Next Horizon: From AI-NOC to Augmented Innovation Organization

The successful deployment of an AI-NOC is not an endpoint. It is a structural inflection point — a moment at which the questions an organization can ask about itself change permanently. Before ANNA, the Digital Infrastructure organization at Arizona State University asked: how quickly can we resolve this? After ANNA, it is beginning to ask a different question: how do we design systems that prevent failure before it occurs? That shift in question is a shift in organizational identity, and it represents the deepest contribution this initiative makes to the field.

This section does something different from the seven that precede it. The earlier sections document what was done, what was found, what it means, and what should happen next. This section makes the future-forward argument that a Doctorate in Professional Practice requires: not just that the AI-NOC initiative worked, but why it represents original thinking in the field of public-sector AI deployment, what the model contributes that did not exist before, and why the inflection point it marks — from reactive operations to augmented innovation — is one that other institutions can reach, with the right architecture, and why so few have.

8.1 What Makes This Unique: The Integration Is the Contribution

The field of AI-assisted IT operations has produced a substantial literature on each of the three elements this initiative combines: AI classification performance ([Notaro, Cardoso & Gerndt, 2021](#)), governance frameworks for responsible AI deployment ([NIST, 2023](#); [ISO/IEC 42001, 2023](#)), and human trust in automation ([Lee & See, 2004](#); [Shneiderman, 2020](#)). What it has not produced — at least not in the specific context of public-sector operational systems — is a practitioner-level demonstration that all three must be designed as a single integrated system, that each one's success depends on the other two, and that the integration itself is what makes the deployment sustainable, legitimate, and replicable.

This is the contribution I am making explicit. The AI-NOC initiative does not contribute a better classification algorithm. Commercial platforms like NetBrain have more sophisticated automation architectures and two decades of enterprise deployment experience ([NetBrain Technologies, 2025](#))

The AI-NOC initiative contributes a **governed human-AI operational model** — a design framework in which AI performance, governance architecture, and human trust are treated not as three separate workstreams that run in parallel but as three interdependent structural elements that must be built together, evaluated together, and sustained together. Remove any one of them and the model fails — not metaphorically, but operationally and institutionally.

What Is Innovative in This Model — Four Explicit Claims

- **Governance as architecture (not compliance):** AI governance is embedded in ANNA's event flow, decision gate criteria, and monitoring cadence — not added as a post-deployment review layer. This is architecturally novel in public-sector NOC deployments, where governance is typically treated as a constraint on, rather than a component of, the technical system.
- **Trust as a measurable KPI with gate-level consequence:** ANNA is the first documented public-university AI-NOC deployment to make workforce trust a gate criterion with real stopping power. A trust composite below 3.2/5.0 at Gate 3 would have halted full deployment — not metaphorically, but operationally.
- **A human-AI co-decision model designed for public accountability:** the decision authority matrix, the suggest-only pilot architecture, and the override-as-data philosophy constitute a human-AI teaming model specifically designed for public institutional contexts — not adapted from enterprise automation defaults.
- **Public-sector replicability by design:** the governance playbook (R5) and the consortium (R6) are not add-ons to an operational initiative. They are structural elements of the model's contribution to the field, designed from Phase 1 to convert ASU's institutional experience into transferable knowledge.

Table 8.1 makes this integration explicit by showing what each element provides, what fails when either of the other two is absent, and why the integration is the contribution rather than any individual element.

Table 8.1: The Three Integrations — Why AI + Governance + Trust Must Be Designed as One

Integration Element	What It Provides	What Fails Without the Other Two	Why Integration Is the Contribution
AI Performance (Operational Engine)	Machine learning classification accelerates triage. ANNA processes high-volume, well-characterized events at machine speed, routing Tier 1 events within seconds and surfacing diagnostic context for Tier 2	Without governance: a technically capable system operating without public accountability produces results that cannot be defended, audited, or scaled beyond a single deployment.	AI performance is necessary but not sufficient. It is the engine. Governance and trust are the architecture and the fuel. Remove either and the engine stalls.

	and 3 events before a human analyst opens the ticket.	Without trust: a technically capable system that analysts distrust produces override patterns that degrade classification quality, eliminate the feedback loop, and ultimately fail operationally.	
Governance Architecture (Institutional Legitimacy)	Public accountability structures — FERPA compliance, AI Governance Council oversight, Steering Committee review, decision gate criteria — embed the deployment within ASU's legal, ethical, and regulatory obligations from Phase 1.	Without AI performance: governance without results is bureaucratic overhead that cannot sustain executive sponsorship or justify public investment. Without trust: governance that protects institutional compliance but ignores workforce experience produces a compliant system that nobody uses.	Governance architecture is what makes the model public-sector specific. Private enterprises can move faster precisely because they face fewer accountability obligations. Public institutions that govern well are not slower — they are more legitimate, more defensible, and ultimately more scalable.
Human Trust (Operational Sustainability)	Analyst calibrated trust — developed through explainability design, co-design participation, decision authority clarity, and override	Without AI performance: a trust-building program deployed around a system that does not work is theater. Analyst goodwill is finite; it	Human trust is what makes the model sustainable. AI systems that erode analyst agency eventually lose the human expertise that keeps them

	safety — sustains model quality over time. Every informed override improves ANNA's training data. Analyst expertise is the model's most valuable input.	cannot substitute for demonstrated classification quality. Without governance: trust without accountability structures produces informal workarounds, shadow AI behavior, and compliance gaps that surface as institutional risk later.	calibrated. The workforce is not a recipient of AI capability — it is a co-producer of it. That insight is the deepest design principle of the AI-NOC initiative.
--	--	---	--

The governed human-AI operational model is the integration of all three columns. No column alone constitutes the contribution.

The practical significance of Table 8.1 is this: most public institutions attempting AI deployment in operational systems are making the mistake of optimizing one element at the expense of the others. They are deploying AI systems with strong performance characteristics but inadequate governance documentation — and discovering the governance gap when a compliance event forces an institutional pause. They are building governance architectures that satisfy public accountability requirements but ignore workforce trust — and discovering the trust gap when adoption metrics reveal that analysts have found quiet ways to route around a system they were never convinced they should trust. Or they are investing in workforce change management programs that build analyst readiness for a system that never delivers the performance improvements that justified the investment.

The AI-NOC initiative is the first public university deployment to design all three simultaneously, to measure all three simultaneously, and to demonstrate — with controlled pilot evidence — that all three can be achieved simultaneously. That is original. That is what the field needed, and that is what this report provides.

8.2 The Inflection Point: From Reactive Operations to Augmented Innovation

The phrase "structural inflection point" deserves analytical precision, because it is easy to say and important to mean. A structural inflection point is not a milestone on a linear improvement trajectory. It is a moment at which the nature of the work changes — not just how fast it is done, but what it is. The ANNA deployment represents such a moment for ASU's Digital Infrastructure organization, and understanding why requires understanding what the organization was before, what it is now, and what it is becoming.

Before ANNA, the NOC was a reactive system: skilled people applying professional judgment to a stream of events that arrived faster than they could be comprehensively analyzed. The constraint was human attention — how many events a team of analysts could triage per hour, and how consistently they could apply diagnostic expertise under time pressure across varying shifts, experience levels, and workload conditions. The organizational question was always a speed question: how do we process this faster?

After ANNA, that constraint is being structurally relieved through the active controlled pilot. ANNA processes Tier 1 events at machine speed, with 94.2% classification precision measured in the pilot period, freeing approximately 230 hours of senior engineering attention per month within the current pilot scope — a capacity recovery that will scale as deployment expands. But — and this is the structural inflection — what is done with that released attention is not determined by ANNA. It is determined by the organization. The inflection point is the moment at which the organization must decide what it is becoming, because the old answer — we are a reactive triage operation, and our value is measured in resolution speed — is no longer sufficient to account for the capacity the organization now has.

The answer ASU's Digital Infrastructure organization is giving, through the forward strategy in Section 6, is: we are becoming an augmented innovation organization — one in which AI handles the high-volume, well-characterized operational work, freeing human expertise for the systems-level, predictive, and governance work that only humans can lead. Table 8.2 maps this evolution across four organizational dimensions, tracing the trajectory from the AI-NOC operational phase through the predictive and augmented phase to the long-term institutional horizon.

Table 8.2: From AI-NOC to Augmented Innovation Organization — Four Dimensions of Evolution

Organizational Dimension	Phase 3–4 (AI-NOC Operational)	Phase 6+ (Predictive & Augmented)	Long-Term Horizon (Augmented Innovation Organization)
The Question the Organization Asks	"How quickly can we restore service once an event is detected?"	"How do we detect and resolve events before they generate user-facing impact?"	"How do we design infrastructure systems that learn, adapt, and prevent failure — so that the question of speed never arises?"
Where Senior Engineering Expertise Lives	In reactive diagnosis: senior engineers are the irreplaceable resource for complex triage. Their expertise is consumed by incident response.	In pattern analysis and predictive model design: senior engineers direct recovered capacity toward systems-level analysis, anomaly detection model development, and pre-incident workflow design.	In infrastructure architecture and AI system design: senior engineers build self-healing systems, govern AI capability expansion, and lead the consortium's governance development.
What Human-AI Collaboration Looks Like	ANNA classifies; analyst confirms or overrides. Feedback loop improves model. Analyst is the decision authority at every tier. Trust is being built.	ANNA classifies and flags pre-incident signatures. Analysts design and validate predictive models. The collaboration is increasingly generative rather than reactive — analysts are not just reviewing ANNA's outputs but shaping what ANNA looks for.	Human and AI roles are deeply integrated. Engineers govern AI capability expansion, set intent parameters for autonomous monitoring, and direct the consortium's shared model development. The question is no longer whether to trust AI — it is how to

			govern AI systems that are trusted enough to operate at greater autonomy.
The Workforce Profile Being Developed	AI-oversight specialists: analysts who combine network engineering expertise with AI governance responsibility, override quality assurance, and model calibration skills. A role that did not formally exist in higher education IT before this initiative.	Infrastructure data scientists: engineers whose primary work is pattern recognition, predictive model validation, and systems-level anomaly analysis. The boundary between network engineering and applied data science is dissolving.	AI governance leaders: senior technology professionals who design governance frameworks for AI operational systems across institutional and consortium boundaries. ASU is developing this workforce profile ahead of the market.

The evolution is directional, not sequential — all four dimensions shift simultaneously as ANNA matures. The long-term horizon represents a qualitatively different organizational model, not a quantitative extension of the current one.

The most significant shift in Table 8.2 is in the column labeled "The Question the Organization Asks." This is the deepest indicator of organizational identity. A NOC that asks "how quickly can we restore service?" is organized around restoration. A NOC that asks "how do we prevent the failure before it generates an alert?" is organized around anticipation. And an infrastructure organization that asks "how do we design systems that learn, adapt, and prevent failure?" is organized around innovation. The AI-NOC initiative has moved ASU's Digital Infrastructure organization from the first question to the second. The forward strategy is designed to move it to the third.

This trajectory is not linear, and it is not guaranteed. The organizational evolution described in Table 8.2 depends on sustaining the conditions that have produced the Phase 3 and early Phase 4 results: governance integrity that keeps the Steering Committee engaged and the compliance architecture maintained; human trust that keeps analysts generating quality override data and participating in co-design; and operational performance that keeps demonstrating to executive leadership that the investment is producing the results it promised. These three conditions are not a list of prerequisites — they are an ongoing system. They must be maintained simultaneously, continuously, and with the same discipline that built them.

8.3 Original Contribution to Practice and Knowledge

A doctoral Strategic Implementation Report is evaluated not only on the quality of its analysis but on the originality of its contribution — what it adds to practice and knowledge that was not available before. This section states that contribution explicitly and without equivocation. The AI-NOC initiative produces five original contributions, each grounded in the evidence of this report and each designed to be transferable beyond ASU.

1. An AI-NOC Governance Architecture for Public Institutions. The FERPA data map, AI Governance Council authorization framework, Steering Committee charter, five-gate decision architecture, risk register with quantified monitoring triggers, and FERPA-compliant data pipeline design constitute a complete, replicable governance architecture for AI deployment in public-sector network operations. No comparable institution has published this architecture in documented, transferable form. Public universities attempting comparable deployments currently face a choice between building this architecture from scratch — an 18-to-24-month governance development process — or proceeding without it and accepting the compliance and accountability risks that follow. This initiative eliminates that constraint.

2. A Trust-Calibration Model for Human-AI Operational Teams. The five-element trust-calibration methodology — suggest-only pilot architecture, decision authority matrix, override-as-data norm, co-design as structural participation, and behavioral triangulation of trust outcomes — constitutes a reproducible model for engineering calibrated human-AI trust in public-sector operational environments. It is grounded in the Phase 3 pilot and early Phase 4 operational evidence, validated through Cronbach's alpha ($\alpha=0.87-0.89$) and inter-rater reliability testing ($\kappa=0.81$), and designed to be adapted to any public institution's workforce context.

3. A Human-in-the-Loop Decision Authority Framework. The decision authority matrix — which explicitly codifies the boundary between ANNA's classification authority and human override authority across all event tiers — is a governance artifact that does not exist in published form for public-sector AI-NOC deployments. It operationalizes the human-AI teaming literature's design recommendations (Shneiderman, 2020; Parasuraman & Riley, 1997) in a specific institutional context, with defined thresholds, escalation protocols, and feedback mechanisms. It is the mechanism through which ASU maintains public accountability in an AI-assisted operational system while still capturing the efficiency benefits of AI classification.

4. A Public-Sector AI-NOC Implementation Roadmap. The six-phase deployment model — with explicit go/no-go gate criteria, named phase owners, quantified performance thresholds, and a trust criterion embedded as a gate requirement — is a replicable implementation architecture for public institutions. It differs from commercial deployment

frameworks in that it is designed for FERPA compliance, multi-stakeholder governance review, and public accountability from Phase 1, rather than adapting a private-sector deployment model to a public-sector context after the fact. The implementation roadmap, the recommendation prioritization matrix (Table 6.3), and the replicability conditions (Table 8.5) together constitute a field-ready practitioner's guide.

5. A Practitioner-Scholar Model for AI Deployment Research. The methodological contribution of this report is the demonstration that a doctoral-level, evidence-based evaluation of a live AI deployment is both achievable and valuable within the DPP tradition. The integrated research question, the quasi-experimental evaluation design, the three-wave longitudinal survey, the thematic focus group analysis, the Threats to Validity framework, and the explicit researcher positionality statement together constitute a research methodology that the field of public-sector AI deployment currently lacks. Vendor case studies dominate the literature; independent, institution-led evaluations at doctoral analytical standards are rare. This report is a model for that kind of work.

These five contributions are not independent. The governance architecture enables the trust-calibration model by establishing the institutional legitimacy that makes workforce co-ownership possible. The decision authority framework operationalizes the trust-calibration model in the event flow. The implementation roadmap integrates all three into a deployable sequence. And the practitioner-scholar research model is the mechanism through which all four are documented at the standard that makes them transferable rather than merely institutional. The integration of these Table contributions is the original contribution.

8.4 The Replicability Architecture: Five Conditions

A future-forward contribution is only genuinely forward-looking if it can be replicated — if the model it demonstrates is adoptable by other institutions that did not build it. The governed human-AI operational model is designed to be replicable. But replicability is not automatic, and the conditions that made the ANNA deployment successful are not universally present. Table 8.3 identifies five replicability conditions — the specific institutional design choices that determined the AI-NOC initiative's success — and names what happens when each is absent. This table is written for the practitioners at other public institutions who will read this report and ask: what do I actually need to do to make this work?

Table 8.3: Replicability Conditions — What the Governed Human-AI Model Requires

Replicability Condition	How ASU Instantiated It	What Happens Without It
Executive sponsorship committed to governance, not just performance	ASU's Senior Director of Digital Infrastructure and Enterprise Technology leadership authorized the initiative with explicit governance obligations — FERPA compliance, AI Governance Council authorization — built into the program design from Phase 1, not added after deployment.	Institutions that deploy AI primarily to achieve efficiency gains, treating governance as a compliance checkbox rather than a design requirement, will produce deployments that are faster to stand up and faster to fail — through compliance breach, workforce rejection, or loss of executive credibility when early performance claims cannot be sustained.
Governance architecture designed before technology deployment	The FERPA data map and AI Governance Council authorization were both completed before ANNA processed its first live event. The governance architecture preceded the system, not the reverse.	Governance that is built around an existing AI system is governance that fits the system rather than governance that constrains the system. In a public institution, the constraint is the point — it is the mechanism through which public trust is warranted. Retrofit governance consistently produces gaps that only become visible when something goes wrong.
Workforce co-ownership from the beginning	NOC analysts participated in Phase 1 readiness assessment, co-designed the escalation taxonomy during Phase 3, contributed override data that directly improved ANNA's training, and shaped the explainability interface requirements in	AI deployments that present a finished system to the workforce it affects — however technically sophisticated — produce adoption patterns driven by compliance rather than trust. Compliance-driven adoption produces override suppression, which eliminates the feedback loop, which degrades the model. The workforce is not a deployment target; it is a co-designer.

	Phase 6. Co-ownership was structural, not consultative.	Institutions that miss this will spend years trying to recover adoption they never built.
Stage-gated commitment with genuine stopping power	Gate 3 — the pilot-to-full-deployment gate — had real consequences: if the $\geq 25\%$ TTR threshold, $\geq 90\%$ classification precision, and $\geq 3.2/5.0$ trust score were not met, full deployment did not proceed. The gate criteria were not aspirational targets; they were operational commitments.	Stage-gating without genuine stopping power is theatrical planning. Institutions that articulate gate criteria but advance deployments regardless of whether criteria are met signal to their governance structures — and to their workforces — that the evaluation framework is performative. This erodes the credibility of every subsequent governance claim the initiative makes.
Measurement that treats trust and performance as co-equal outcomes	The ANNA evaluation collected quantitative performance data (ITSM platform) and qualitative trust data (surveys, focus groups) simultaneously, treating both as primary outcomes rather than treating trust as a secondary indicator of adoption success.	Deployments that measure only operational performance will optimize for operational performance — and will discover, often too late, that the workforce has developed coping strategies that preserve their sense of agency while undermining the system's effectiveness. Trust is not soft. It is the mechanism through which human expertise remains productively engaged with AI systems over time. It must be measured, not assumed.

These conditions are design choices, not prerequisites. They must be built into the initiative's architecture before deployment begins, not added after adoption problems emerge.

The five conditions in Table 8.3 are not a checklist. They are an integrated architecture — the five elements of the governed human-AI operational model that must all be present for the model to function. An institution that has four of the five will find that the missing one eventually compromises the others. Governance without workforce co-ownership produces compliance without trust. Stage-gating without genuine stopping

power produces theatrical evaluation. Performance measurement without trust measurement produces optimization of the wrong outcomes.

The most common institutional failure mode I would predict for public universities attempting to replicate this model is the third condition: workforce co-ownership from the beginning. The temptation — especially in institutions where technology deployment is led primarily by technical teams — is to build the system and then present it to the workforce as a fait accompli, with change management programming designed to smooth adoption rather than to shape design. That sequence produces a workforce that was never given genuine co-ownership and that therefore never developed genuine trust. The AI-NOC initiative demonstrates, with survey evidence and focus group data, that the alternative is possible: a workforce that enters an AI deployment anxious about its implications and exits it feeling elevated by the system's presence. That outcome requires starting co-design in Phase 1, not Phase 5.

8.5 The Question the Field Must Now Answer

This report ends where a doctoral contribution should end: not with a summary of what was found but with a question that the findings make possible. The AI-NOC initiative has demonstrated — in controlled pilot — that a governed human-AI operational model can be built in a public university and can produce measurable results across three interdependent outcome dimensions, and can establish the institutional architecture for ongoing capability expansion. It has produced a governance playbook and a consortium framework designed to make these results available to the broader public university community.

The question the field must now answer is not whether AI-assisted operations are valuable in public-sector digital infrastructure environments. The evidence says yes. The question is whether the institutions responsible for public digital infrastructure — the public universities, the government IT agencies, the publicly accountable healthcare systems — are willing to make the deliberate governance investments that responsible AI deployment requires, before performance pressure tempts them to move faster than their governance architecture can support.

The AI-NOC initiative is my answer to that question for ASU. It is also, through the playbook and the consortium, my attempt to make it easier for the next institution to give the same answer. The field has the model. The field has the evidence. What the field needs now is the leadership will to replicate it — to treat AI governance not as a bureaucratic obstacle to operational improvement but as the institutional architecture through which operational improvement becomes sustainable, defensible, and worthy of the communities that public institutions exist to serve.

The successful deployment of an AI-NOC is not an endpoint. It is a structural inflection point. The question is not whether AI will transform public-sector digital infrastructure. It is whether the institutions responsible for that infrastructure will transform themselves with the governance discipline, the workforce trust, and the operational rigor that their public missions demand. ASU has. Others can.

References

- ACI Infotech. (2025). AIOps for IT operations: Turning chaos into insight in 2025. Retrieved from <https://www.aciinfotech.com/blogs/aiops-for-it-operations>
- Arizona State University. (2014). ASU charter. Office of the University Provost. <https://provost.asu.edu/governance/charter>
- Arizona State University. (2023). Digital transformation strategy. Enterprise Technology. Internal institutional document.
- Arizona State University Institutional Data. (2024). Enrollment and campus statistics. Office of Institutional Analysis.
- Booz Allen Hamilton. (2025). Accelerating incident response with AIOps. Retrieved from <https://www.boozallen.com/insights/ai-research/accelerating-incident-response-with-aiops.html>
- Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W. W. Norton & Company.
- Cai, C. J., Winter, S., Steiner, D., Wilcox, L., & Terry, M. (2019). "Hello AI": Uncovering the onboarding needs of medical practitioners for human-AI collaborative decision-making. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–24. <https://doi.org/10.1145/3359206>
- Coghlan, D., & Brannick, T. (2014). *Doing action research in your own organization* (4th ed.). SAGE Publications.
- Cooper, R. G. (2008). Perspective: The stage-gate idea-to-launch process — Update, what's new, and NexGen systems. *Journal of Product Innovation Management*, 25(3), 213–232. <https://doi.org/10.1111/j.1540-5885.2008.00296.x>
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.
- Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review*, 96(1), 108–116.
- Desouza, K. C., Dawson, G. S., & Chenok, D. (2020). Designing, developing, and deploying artificial intelligence systems: Lessons from and for the public sector. *Business Horizons*, 63(2), 205–213. <https://doi.org/10.1016/j.bushor.2019.11.004>
- EDUCAUSE. (2024). AI landscape study and action plan for AI policy development. EDUCAUSE Publications.
- Fountain, J. E. (2001). *Building the virtual state: Information technology and institutional change*. Brookings Institution Press.
- Fulcrum Digital. (2025). AI model drift in production: What enterprises must monitor. Retrieved from <https://fulcrumdigital.com/blogs/ai-model-drift-in-production-what-enterprises-must-monitor/>

- Gartner. (2024). Emerging technology: AIOps market guide. Gartner Research.
- Highsmith, J. (2010). Agile project management: Creating innovative products (2nd ed.). Addison-Wesley.
- Hoff, K. A., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human Factors*, 57(3), 407–434. <https://doi.org/10.1177/0018720814547570>
- IBM. (2025). What is model drift? IBM Think Topics. Retrieved from <https://www.ibm.com/think/topics/model-drift>
- ISO/IEC 42001:2023. (2023). Artificial intelligence — Management system. International Organization for Standardization. <https://www.iso.org/standard/81230.html>
- Kotter, J. P. (2012). Leading change. Harvard Business Review Press.
- Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors*, 46(1), 50–80. https://doi.org/10.1518/hfes.46.1.50_30392
- Luftman, J. (2004). Managing the information technology resource: Leadership in the information age. Pearson Prentice Hall.
- National Institute of Standards and Technology (NIST). (2023). Artificial intelligence risk management framework (AI RMF 1.0). U.S. Department of Commerce. <https://doi.org/10.6028/nist.ai.100-1>
- NetBrain Exchange Community. (2026). Reducing MTTR and network downtime by up to 50% year over year. Retrieved from <https://exchange.netbrain.com/news-2/reducing-mttr-and-network-downtime>
- NetBrain Technologies. (2022). Case study: BT Enterprise managed services and NetBrain. Retrieved from <https://staging.netbraintech.com/wp-content/uploads/2022/04/NetBrain-Case-Study-BT-Enterprise.pdf>
- NetBrain Technologies. (2024). Artificial intelligence features. Retrieved from <https://www.netbrain.com/features/ai/>
- NetBrain Technologies. (2025). Agentic AI for network automation. Retrieved from <https://www.netbrain.com/agentic-ai/>
- NetBrain Technologies. (2025). Auto remediation. Retrieved from <https://www.netbrain.com/features/auto-remediation/>
- NetBrain Technologies. (2025). Network operations center solution. Retrieved from <https://www.netbrain.com/solution/network-operation-centers/>
- Network Automation Forum. (2025). Beyond building networks: The day two automation challenge. Retrieved from <https://networkautomation.forum/blog/beyond-building-networks-the-day-two-automation-challenge>

- Notaro, P., Cardoso, J., & Gerndt, M. (2021). A survey of AIOps methods for failure management. *ACM Transactions on Intelligent Systems and Technology*, 12(6), 1–45. <https://doi.org/10.1145/3483424>
- Oreg, S. (2003). Resistance to change: Developing an individual differences measure. *Journal of Applied Psychology*, 88(4), 680–693. <https://doi.org/10.1037/0021-9010.88.4.680>
- Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. *Human Factors*, 39(2), 230–253. <https://doi.org/10.1518/001872097778543886>
- Research Square. (2025). Reducing mean time to repair (MTTR) with AIOps: An advanced approach to IT operations management. <https://doi.org/10.21203/rs.3.rs-7383044/v1>
- ScienceLogic. (2024). Cracking the code: AIOps unleashed for lightning-fast MTTR. Retrieved from <https://sciencelogic.com/blog/cracking-the-code-aiops-unleashed-for-lightning-fast-mttr>
- Scott, A. (2025). Case study: How enterprises use AIOps to cut MTTR by 40%. AI Accelerator Institute. Retrieved from <https://medium.com/@alexendrascott01/case-study-how-enterprises-use-aiops-to-cut-mttr-by-40-576600a4215a>
- Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). Experimental and quasi-experimental designs for generalized causal inference. Houghton Mifflin.
- Shneiderman, B. (2020). Human-centered artificial intelligence: Reliable, safe & trustworthy. *International Journal of Human-Computer Interaction*, 36(6), 495–504. <https://doi.org/10.1080/10447318.2020.1741118>
- SmartDev. (2025). AI model drift and retraining: A guide for ML system maintenance. Retrieved from <https://smartdev.com/ai-model-drift-retraining-a-guide-for-ml-system-maintenance/>
- U.S. Department of Education, Office of Educational Technology. (2023). Artificial intelligence and the future of teaching and learning: Insights and recommendations. <https://www.ed.gov/ai>
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478. <https://doi.org/10.2307/30036540>

Appendix

ANNA (Arizona State University Network and Nodes Assistant) Agentic AI architecture explanation

Note. Adapted from ANNA Executive Summary by Todd Simmons, ASU Principal Network Architect, 2026

Enterprise networks have become increasingly complex, distributed, and vendor diverse. As a result, diagnosing connectivity issues is no longer a single-system problem—it requires correlating data across wireless infrastructure, wired Layer 2/Layer 3 networks, security systems, and centralized logging platforms.

ANNA (Arizona State University Network and Nodes Assistant) is designed to address this challenge by acting as a unified intelligence layer across the network. It leverages a hybrid AI architecture—combining Large Language Models (LLMs) for reasoning and explanation with Small Language Models (SLMs) for fast, deterministic analysis—to transform raw telemetry into clear, actionable insights.

By integrating directly with internal systems such as the ASU Logging Lake, as well as vendor APIs and packet-level diagnostics, ANNA provides real-time visibility and automated analysis across the entire network stack.

Problem Statement

Modern network operations face several critical challenges:

- **Fragmentation across vendors and domains**
Wireless, switching, routing, and firewall systems operate independently, each with its own tooling and data models.
- **Disconnected telemetry sources**
APIs, SYSLOGS, SNMP traps, and packet captures exist in silos, requiring manual aggregation.
- **Manual correlation and interpretation**
Engineers must reconstruct timelines across multiple systems to determine root cause.
- **High dependency on expertise**
Effective troubleshooting relies heavily on experienced personnel, creating inconsistency and scaling challenges.

- **Delayed response to critical conditions**

Key events captured in logging systems are often not acted upon in real time.

These limitations result in increased Time to Resolution (TTR), operational inefficiencies, and inconsistent user experiences.

Solution

ANNA introduces a unified, AI-driven approach to network troubleshooting by focusing on **node-level intelligence**—analyzing the behavior of clients, devices, and infrastructure components across all domains.

The platform performs four core functions:

1. **Ingest** data from multiple sources
2. **Normalize** it into a canonical model
3. **Correlate** events across layers and systems
4. **Act** by providing insights, alerts, and recommended remediation

This approach eliminates the need for manual cross-system analysis and enables consistent, repeatable troubleshooting workflows.

ASU Logging Lake Integration

A defining capability of ANNA is its integration with the ASU Logging Lake, an internally developed platform aggregating syslog data and SNMP traps from across the network.

This integration allows ANNA to:

- Monitor high-volume, real-time event streams
- Detect conditions not exposed through vendor APIs
- Correlate logging data with client-level telemetry
- Trigger automated responses based on predefined patterns

The Logging Lake effectively serves as ANNA's **real-time observability backbone**, enabling proactive detection and response rather than reactive troubleshooting.

AI Architecture (LLM + SLM Hybrid Model)

ANNA's intelligence layer combines two complementary AI approaches:

- **Small Language Models (SLMs)**
 - Provide fast, deterministic classification of events and patterns
 - Enable real-time processing and low-latency decision-making

- **Large Language Models (LLMs)**
 - Provide contextual reasoning across multiple data sources
 - Generate human-readable explanations and summaries
 - Translate complex technical data into actionable insights

This hybrid model ensures both **performance and interpretability**, allowing ANNA to operate efficiently while still delivering meaningful explanations.

Key Capabilities

- Vendor-agnostic architecture across all major network domains
- Unified visibility across wireless, wired, and security systems
- Real-time monitoring using both APIs and Logging Lake telemetry
- Automated correlation of events across multiple layers
- Integrated packet-level diagnostics (PCAP retrieval and analysis)
- AI-driven root cause identification and explanation
- Actionable notifications and remediation guidance

Business Impact

ANNA delivers measurable improvements across network operations:

- **Reduced Time to Resolution (TTR)**
 - Faster diagnosis through automated correlation and analysis
- **Improved operational efficiency**
 - Eliminates manual data gathering and interpretation
- **Consistency across support teams**
 - Standardized workflows reduce variability in outcomes
- **Reduced reliance on specialized expertise**
 - Enables first-level support teams to resolve complex issues
- **Proactive issue detection**
 - Real-time monitoring of Logging Lake data enables early identification of problems

Conclusion

ANNA represents a fundamental shift from reactive troubleshooting to intelligent, automated network operations. By unifying telemetry across vendors and domains, integrating real-time logging data, and applying AI-driven analysis, ANNA enables organizations to diagnose issues faster, operate more efficiently, and scale their network operations with confidence.