Mattermost

Collaboration as Mission Infrastructure

Contents

Why Feature-Level Evaluation No Longer Holds Under Sovereign, Coalition, and Incident Pressure

Across defence and public-sector environments, collaboration platforms increasingly function as operational infrastructure rather than workplace productivity tools.

Yet procurement and accreditation processes keep evaluating these systems primarily through feature comparisons and control checklists designed for enterprise IT. Under stable conditions, that approach can appear sufficient. Under operational stress, however, it reveals a gap between how collaboration environments are evaluated and how they must perform when authority, coordination, and accountability are tested.

Collaboration environments therefore need to be assessed using the same infrastructure-level dimensions applied to other mission-critical systems — governance authority, forensic auditability, degraded-environment operability, and cross-border coordination. For accreditation authorities and senior decision-makers, this shifts evaluation toward how collaboration infrastructure must perform during operational incidents rather than how platforms appear on procurement scorecards.

Collaboration Has Become Infrastructure

Multi-jurisdiction and coalition operations are where governance and coordination assumptions encounter conditions they were not designed for — and where the time taken to establish authority, synchronise escalation, and produce a coherent operational picture determines whether a collective response is possible at all.

Operational experience from Ukraine illustrates what sustained adversarial pressure reveals. Maintaining command and communication arrangements under persistent cyber and electronic warfare required multiple pathways, adaptive switching, and local autonomy that conventional architectures had not assumed. Resilience depended not on the capabilities of individual systems in normal conditions, but on redundancy and the capacity to adapt when primary systems were unavailable. These conditions are now treated as planning baselines, not contingencies.

ENISA's work on EU incident response and cyber crisis management identifies the coordination challenge directly: cross-border incidents require shared situational awareness and coordinated decision-making by national and EU bodies, supported by exercises and procedures that test the capacity to act collectively under time pressure. ENISA's stress-testing framework extends this across national, regional, and EU-wide levels, explicitly assessing control and authority gaps across sectors and jurisdictions.

Analysis of NATO's digital backbone identifies a persistent gap between stated interoperability ambitions and the governance mechanisms, standardisation, and shared procedures required to deliver them under operational conditions. Interoperability is not a property of individual systems — it is a property of agreed authority structures and tested procedures. In multinational settings, fragmented approaches and siloed development produce coordination friction precisely when coherent collective action is most required.

European policy analysis on strategic autonomy highlights that many critical digital technologies underpinning defence and security are dominated by non-EU actors, creating vulnerabilities in coalition operations where EU actors depend on external systems for situational awareness, command, and logistics.

The pattern that emerges is consistent. In multi-jurisdiction operations — whether EU crisis response or NATO digital backbone initiatives — the decisive factors are clarity of authority, shared governance mechanisms, and assured control over infrastructure and data. The maturity or usability of individual collaboration platform features is not among them.

The Control-Resilience Disconnect in Evaluation Frameworks

Current evaluation approaches may not reliably predict infrastructure performance because they assess presence rather than persistence, components rather than systems, and assumptions rather than constraints. The UK National Audit Office's January 2025 government cyber resilience assessment revealed a pattern, now visible across allied nations, that systems meeting control requirements often do not demonstrate operational resilience when tested under realistic threat scenarios. Independent assessment of 58 critical IT systems found "significant gaps in cyber resilience" despite "multiple fundamental system controls" being present. The gap between having the required security features and maintaining operations when infrastructure is degraded has proven to be substantial and consistent.

The GovAssure process assessment of 72 government IT systems between April 2023 and July 2024 provides mechanism insight. Departments self-assessed control maturity, then independent evaluation revealed substantial overestimation, particularly for systems with lower actual resilience. The natural result of evaluating control implementation rather than operational outcomes was critical deficiencies in asset management, protective monitoring, and response planning that remained hidden because feature-level evaluation treated capability deployment as outcome achievement.

The US Government Accountability Office (GAO) has also documented this evaluation gap for 15+ years. Since 2010, GAO has made 1,600+ recommendations addressing cybersecurity shortcomings across federal systems. As of May 2024, 567 recommendations remained unimplemented with a recurring theme: compliance with security requirements does not correlate with operational resilience under stress conditions.

Regulatory evolution also reflects growing recognition of this disconnect. The EU shift from NIS1 to NIS2 mandates service continuity under stress, coordinated cross-border incident response through EU-CyCLONe, and explicit supply chain resilience requirements — moving from assessing whether an organization has controls to assessing whether it can deliver outcomes when everything else fails. The European Union Agency for Cybersecurity's May 2025 stress testing framework operationalises this philosophy by targeting assessment of organisational resilience and the ability to withstand and recover from significant cybersecurity incidents — testing whether systems maintain operation when adversaries actively degrade infrastructure, not just whether controls exist on paper.

Evaluation Boundaries Miss Operational Dependencies

The UK NAO finding that government departments "do not understand their digital estate and its interdependencies" reflects evaluation frameworks unable to assess what remains invisible to them. When collaboration platforms depend on identity providers, network infrastructure, external services, or vendor-managed components, tool-level evaluation does not readily assess cascade failure risks because it tests components while ignoring systems. RUSI's UK defence digital infrastructure analysis documents a significant visibility gap, noting that "MOD lacks an understanding of what its digital enterprise looks like" with Digital Backbone deficiencies stemming partly from "fragmented" architecture "held back by legacy systems" remaining "largely opaque to government officials and operators."

Vendor Dependencies are Operational Constraints

Evaluation frameworks typically assume vendor-controlled environments where governance, support, and incident response flow through commercial relationships. Geopolitical tensions that restrict vendor access, classified operations prohibiting external dependencies, and coalition partners unable to share vendor relationships now represent operational realities rather than edge cases. The challenge extends beyond vendor lock-in to governance sovereignty. When collaboration platforms require external authentication, cloud infrastructure, or vendor-managed encryption keys, evaluation must assess scenarios where those dependencies may be severed through adversary action, legal restriction, or operational security requirements. Feature-level evaluation treats these as architectural choices, but infrastructure-level assessment recognises them as operational constraints potentially preventing mission execution. The NAO's finding that legacy systems often represent unexamined single points of failure reinforces the same concern — formal vendor relationships and security arrangements have repeatedly proven insufficient when external dependencies become unavailable under operational stress.

Governance Authority Under Contested Conditions

NIS2 Article 23 of the EU's Network and Information Security Directive (2022) requires incident response within 24 hours of detection, detailed notification within 72 hours, and cross-border impact assessment. Compliance demands governance structures determining what constitutes reportable incidents, who holds declaration authority, and how incident data flows across organisational boundaries during active contestation — not merely logging capability.

ENISA's stress-testing framework explicitly separates "incident management" assessment from preventive control verification, evaluating whether organisations can activate crisis response plans and communicate with all external stakeholders. GAO's February 2024 National Cybersecurity Strategy assessment identified that strategy outlined governance principles, but implementation plans lacked "outcome-oriented performance measures" for key initiatives. Organisations may not be able to distinguish between possessing governance structures and actually governing during incidents without outcome-based measurement.

Forensic Auditability Across Jurisdictional Boundaries

Saudi Arabia's National Cybersecurity Authority Essential Cybersecurity Controls (ECC-1:2018) distinguish explicitly between activity logging for operational purposes and forensic logging for investigation and compliance, mandating comprehensive logging with tamper-evident storage and multi-year retention. Infrastructure-level assessment asks whether legally admissible evidence can be provided during multi-jurisdictional incident investigations rather than whether logging capability exists.

NIS2's coordinated incident response through EU-CyCLONe presumes participating states can provide forensically sound evidence across jurisdictional boundaries. When collaboration platforms span multiple legal regimes, log custody, data residency, and evidence admissibility become operational constraints. The US Cybersecurity and Infrastructure Security Agency's December 2025 update to its Cybersecurity Performance Goals (CPG 2.0) aligns with this forensic dimension, addressing logging and monitoring capabilities that support incident investigation beyond detection.

Performance During Infrastructure Degradation

NATO operations assume contested environments with adversaries actively degrading infrastructure. AJP-6 addresses this through explicit resilience requirements, federation across classification boundaries, and operation within mission network environments shaped by "guidance and direction by commanders and mutual agreements during mission planning processes." Static feature assessment does not evaluate dynamic adaptability required when primary communication channels fail, authentication systems degrade, or operations must continue across partners with different security postures under active attack.

The UK NAO also identified this evaluation blind spot when their assessment revealed that 228 legacy systems lacked detailed cyber resilience assessments because "many of GSG's recommended system controls would not be applicable to legacy systems." Legacy systems often represent single points of failure, yet their resilience under stress remains unexamined because feature-level frameworks do not assess degraded-mode operation. ENISA's 2025 stress-testing methodology addresses this gap through progressive degradation scenarios, assessing "time-to-detect" and "time-to-recover" as quantitative resilience metrics rather than inferring resilience from control presence.

Cross-Border Coordination Beyond Technical Interoperability

Coalition operations require governance, legal, and procedural interoperability that all go beyond mere technical protocol compatibility. NATO's federated CIS approach acknowledges that "sometimes ad-hoc measures must be negotiated with and accepted by troop contributing nations" with federation delivering "benefits of unity of effort and speed of command compared with each running isolated networks." NIS2 implementation revealed coordination complexity through fragmented transposition as nineteen member states received reasoned opinions for incomplete transposition by May 2025, with over forty distinct interpretations of incident reporting thresholds and supply chain assessment criteria emerging across member states. Regulatory fragmentation directly impacts operational coordination when incidents span jurisdictions. GAO's June 2024 congressional testimony on cybersecurity regulatory harmonisation documented conflicting requirements across federal agencies ranging from 49% to 79% conflict rates, with state officials reporting conflicts led to "a great increase or very great increase in time and staff hours needed to address" them. During incidents, these conflicts can translate directly into operational failure rather than administrative delay.

Evaluation that Matches Impact

The shift from feature-level to infrastructure-level evaluation represents assessment methodology evolution rather than wholesale practice rejection. Controls remain necessary but should not serve as the sole evaluation criteria when platforms function as mission infrastructure. Infrastructure-level assessment evaluates system behaviour under stress rather than control presence at rest. ENISA's stress-testing framework operationalises this through progressive degradation scenarios testing preparedness, response, and recovery across escalating threat conditions, revealing failure modes control catalogues may not predict.

Governance and operability matter as much as features when platforms serve as mission infrastructure. The UK NAO recommended accounting officers ensure senior decision-making boards include "at least one digital leader with cyber expertise and one non-executive director with cyber expertise" — an acknowledgment that technical capability requires governance structures to translate into operational resilience. The distinction here is that feature-level evaluation assesses what systems can do while infrastructure-level evaluation assesses what organisations can actually accomplish under pressure.

Evaluation criteria should align with operational doctrine and regulatory requirements rather than vendor taxonomies. NATO's AJP-6 provides defence-specific requirements for resilience, federation, and contested-environment operation. NIS2 establishes service-continuity and cross-border coordination mandates. NIST CSF 2.0 emphasises governance alongside technical controls. These institutional frameworks define infrastructure expectations more authoritatively than feature comparison matrices.

If collaboration platforms are now infrastructure — which they clearly are — then Security and Accreditation Authorities should evaluate them as infrastructure. This includes stress-testing continuity, validating governance under incident conditions, verifying cross-border coordination functions before operational necessity, and distinguishing between systems that just meet control requirements versus systems that deliver assured outcomes when everything else fails.

Operational Criteria for Infrastructure Assessment

NATO doctrine, EU regulatory evolution, US oversight findings, and allied national audits consistently conclude that feature-level evaluation does not reliably predict infrastructure behaviour under operational pressure. Control catalogues, usability assessments, and capability matrices remain useful for certain procurement decisions but do not substitute for infrastructure-level evaluation when platforms underpin command and control, enable coalition coordination, or provide continuity during contested operations. Existing evaluation frameworks provide familiar metrics, established procurement processes, and vendor-comparable assessments, but infrastructure-level evaluation requires different competencies, new assessment methodologies, and operational validation that traditional procurement cycles often cannot accommodate.

The evaluation dimensions outlined in this brief — governance authority, forensic auditability, degraded-environment operability, and cross-border coordination — provide the conceptual basis for reassessing how collaboration environments are accredited and governed. Translating these dimensions into structured decision criteria is the next step for Security and Accreditation Authorities moving from evaluation reset to infrastructure-level assessment.

Sources Referenced

NATO

- Allied Joint Publication-6 (AJP-6) — Allied Joint Doctrine for Communication and Information Systems, Edition B Version 1, 2024

European Union & ENISA

- Directive (EU) 2022/2555 — Network and Information Security Directive (NIS2), 2022
- European Union Agency for Cybersecurity (ENISA) — Handbook for Cyber Stress Tests, 2025
- European Cyber Security Organisation — NIS2 Directive Transposition Tracker, 2025

United Kingdom

- National Audit Office — Government Cyber Resilience (HC 546), 2025
- Ministry of Defence — Digital Strategy for Defence, 2021
- Royal United Services Institute (RUSI) — Making Sense of Britain's Digital Targeting Web, 2025

United States

- National Institute of Standards and Technology (NIST) — Cybersecurity Framework 2.0, 2024
- US Government Accountability Office (GAO) — High-Risk Series: Cybersecurity, 2024
- US Government Accountability Office (GAO) — National Cybersecurity Strategy Implementation, February 2024
- US Government Accountability Office (GAO) — Cybersecurity: Efforts to Harmonize Regulations, June 2024
- Cybersecurity and Infrastructure Security Agency (CISA) — Cybersecurity Performance Goals 2.0, December 2025

Middle East

- National Cybersecurity Authority, Kingdom of Saudi Arabia — Essential Cybersecurity Controls (ECC-1:2018), 2018

Full citations available on request.