

BRIDGING THE GAP: HOW BUSINESS RELATIONSHIP MANAGEMENT (BRM) CAN STRENGTHEN IT GOVERNANCE TO SUPPORT FASTER ACQUISITION TEMPO ACROSS THE DEPARTMENT OF DEFENSE

DR. TOBALINA BECK, JD, BRMP, CISM, CISSP

Information Technology as an Enabler of Defense Acquisition Effectiveness

Defense acquisition runs on information technology. Contracts are managed, performance assessed, and capability decisions coordinated through digital systems that span organizations, geographies, and program offices. When those systems — or the governance processes behind them — fail to translate mission needs into delivered capability, acquisition timelines slow and the Department's ability to exploit technological advances erodes.¹

Commercial technology cycles have compressed. Cloud services, data analytics, and AI now shape how acquisition organizations manage complexity at scale, and the pace of that change is not slowing. Defense organizations that cannot evaluate and integrate these capabilities fall behind — not because innovation is unavailable, but because internal processes cannot absorb it.²

When demand governance is weak, the friction shows up everywhere: delayed decisions, rework that could have been avoided, and eroding confidence in modernization efforts. The gap between technological opportunity and organizational execution is real, and it carries direct costs for acquisition timelines.³

The problem is fundamentally one of governance. Without disciplined mechanisms to shape demand and adjudicate priorities, even well-resourced IT organizations struggle to convert ideas into outcomes. Intake systems that lack transparency become bottlenecks. Business Relationship Management — practiced by certified professionals with a defined skill set — provides a structural answer. The DCMA experience shows how.

The Demand-Decision Gap in Defense IT

Every defense IT organization has an intake process. The problem is what happens after a request enters it. Too often, requests stall without resolution or fail to translate into delivered capability. Over time, that pattern erodes trust and reinforces the perception that participation yields little return.⁴

The core challenge is the gap between what and how. When requests arrive without clear ownership or defined pathways to adjudication, governance bodies spend their time seeking clarification rather than making decisions. The result is friction: delayed decisions, repeated rework, and stakeholders who eventually stop submitting.⁵

Defense environments make this worse. Policy compliance, security review, appropriated funding timelines, and workforce ceilings each add friction that a well-scoped request can absorb — but a half-formed one cannot. Intake mechanisms that lack discipline become symbolic. Restoring confidence requires a structure that translates mission need into decision-ready input and carries it through governance to outcome.⁶

Business Relationship Management provides that structure. BRM is a recognized profession with certified practitioners, a codified body of knowledge, and established competency standards — one that cannot be improvised by assigning someone a title. When organizations

deploy certified BRM professionals rather than ad hoc coordinators, the difference in governance outcomes is measurable. DCMA is the proof.⁷

Business Relationship Management as a Recognized Profession

What a certified BRM brings to an organization, and how that differs from informal liaison work, is central to evaluating the DCMA case and the broader applicability of this model across the Department of Defense.

A. The BRM Institute and the Professional Framework

The BRM Institute, established in 2012, is the premier global membership, professional development, and certification organization for the Business Relationship Management discipline. The Institute defines BRM as a role, a discipline, and an organizational capability — a construct that distinguishes it from narrower conceptions of IT coordination or stakeholder management.⁸

The role definition matters because it sets expectations for how BRM professionals are hired, placed, and held accountable. As an individual role, BRM refers to the competencies a practitioner must develop to advance organizational capability. As an organizational capability, it describes the enterprise-level capacity to systematically shape and channel demand toward the highest-value opportunities. Deploying BRM effectively requires more than assigning someone a title — it requires structured investment in professional development and deliberate placement within governance structures.⁹

B. The Certification Pathway: BRMP and CBRM

The BRM Institute administers a tiered certification pathway with clear, testable standards for BRM practice. The foundational credential, the Business Relationship Management

Professional (BRMP®), is accredited through APMG International and recognized globally as the authoritative entry-level certification in the discipline. BRMP holders demonstrate verified proficiency in the characteristics of the BRM role, strategic partnering, portfolio management for value maximization, business transition management, and the alignment of services with mission needs.¹⁰

The advanced practitioner credential, the Certified Business Relationship Manager (CBRM®), builds on the BRMP and requires it as a prerequisite. The CBRM focuses on strategic-level practice: convergence of organizational and provider strategies, value optimization across the enterprise, and executive engagement. CBRM holders are positioned to function as genuine strategic partners, capable of influencing organizational direction and governance design — not simply executing within it. The credential is valid for three years and requires ongoing professional development to maintain.¹¹

A third tier, the Master of Business Relationship Management (MBRM®), represents mastery of the discipline, requiring demonstrated thought leadership, innovation, and sustained organizational impact. Together, the three credentials constitute a rigorous professional development pathway comparable to those in project management (PMP) or IT governance (COBIT). For defense organizations, that matters practically: BRM competencies can be recruited for, trained toward, and verified.¹²

C. Core BRM Competencies and Their Relevance to Defense IT

The BRM Body of Knowledge defines six core competencies required in the BRM role. Strategic partnering builds credibility and genuine partnerships with mission stakeholders. Business IQ requires deep understanding of the partner organization's strategy, operations, and objectives. Portfolio management encompasses the disciplined pursuit of value realization across

products, services, and capabilities. Provider domain knowledge ensures the BRM can credibly represent IT capability and constraints. Powerful communication enables translation between technical and operational vocabularies. Relationship building underpins all other competencies by establishing the trust necessary for effective demand shaping and governance influence.¹³

The BRM Body of Knowledge also describes the practitioner's role through three operational metaphors: connector, navigator, and orchestrator. As connector, the BRM builds and sustains relationships between mission partners and the IT provider organization. As navigator, the BRM facilitates business-technology strategy alignment and supports capability roadmapping. As orchestrator, the BRM coordinates the resources and stakeholders required to translate demand into value, ensuring that approved capabilities move from adjudication to delivery without fragmentation or loss of accountability.¹⁴

The demand-decision gap is, at its core, a problem of missing connectors, navigators, and orchestrators. Requests fail to reach governance forums in decision-ready form because no one owns the translation process. Approved initiatives stall because no one is orchestrating the handoffs. A certified BRM addresses each of these failure modes through a structured, verifiable skill set — not through access or personality.

D. BRM in Practice: Beyond Liaison

A persistent misconception — one that organizations risk replicating when they deploy BRM without professional grounding — is that BRM is a sophisticated liaison function. The BRM Institute is explicit that this framing is insufficient. A liaison transmits information between parties. A certified BRM shapes demand, enforces requirements discipline, influences governance design, manages value realization, and drives organizational culture toward strategic partnership. The difference is not cosmetic.¹⁵

The distinction appears most clearly in governance forums. A liaison presents what stakeholders want. A certified BRM presents what the organization needs — filtered through strategic alignment, feasibility analysis, and enterprise context — and then follows that request through adjudication, delivery, and value assessment. That governance engagement function, grounded in professional competency, is what makes BRM well-suited to the structural governance challenges of defense IT environments.

Conceptual Foundations: BRM, Governance, and Value Flow

Business Relationship Management aligns organizational demand with delivery capacity through structured engagement and shared accountability. Effective BRMs operate as integrators, connecting mission priorities, technical realities, and governance constraints into a coherent demand narrative. The professional competency framework makes this integration systematic and repeatable rather than dependent on individual access or personality.¹⁶

Governance effectiveness depends on the quality of information provided, not the volume of requests presented. Decision forums function best when submissions arrive scoped, validated, and contextualized, when leaders can weigh value, risk, and trade-offs rather than spend time deciphering intent or feasibility. Certified BRMs enforce this discipline upstream, before requests reach adjudication, drawing on the portfolio management and requirements translation skills embedded in the BRMP and CBRM competency frameworks.¹⁷

A key distinction in this process is the difference between demand and requirements. Demand reflects a perceived need or desired outcome; requirements translate that need into actionable, testable criteria. Without that translation, governance decisions are inherently unstable

— leading to rework, delay, or misalignment during execution. Requirements translation is a defined BRM competency, developed through certification and practice.¹⁸

Value accumulates as requests move from ideation to prioritization, delivery, and assessment. Transparency across that flow, visibility into status, rationale, and outcomes, reinforces trust even when requests are deferred or declined. When stakeholders understand not only what decisions were made but why, confidence in the system grows. The BRM Body of Knowledge addresses this through its value harvesting discipline, which ensures that governance outcomes are tracked, assessed, and fed back into planning.¹⁹

Defense organizations need exactly this kind of sustained accountability across the demand lifecycle. By linking people, process, and governance through certified professional practice, BRMs enable leadership to move from reactive intake management toward intentional, outcome-driven decision-making. The BRM framework's core principles — demand governance, value realization, and stakeholder accountability — align with established external governance standards including ISACA's COBIT framework and OMB Circular A-130, confirming that the discipline addresses recognized gaps in IT governance practice that extend well beyond any single certification body.^{20 21}

Organizational Context: DCMA's IT Demand Environment

DCMA operates across a geographically dispersed workforce with significant reliance on digital tools to execute its acquisition oversight mission. Demand for IT capabilities originated across that workforce — from mission owners, functional communities, and enabling organizations — each framing legitimate needs through different operational lenses. While demand was persistent, the structures intended to adjudicate it were increasingly ineffective.²²

Over time, formal IT intake boards at DCMA largely ceased to function as intended. Many boards were convened inconsistently; others stopped meeting altogether. Intake mechanisms existed in name but not in practice. Requests were submitted without a reliable forum for review, prioritization, or disposition, leaving stakeholders uncertain whether governance bodies had visibility into their needs at all.²³

In the absence of functioning intake boards, demand did not disappear - it fragmented. Mission partners pursued informal pathways to raise issues, relied on personal networks, or disengaged from intake entirely after repeated non-response. From the IT perspective, this created a growing accumulation of unadjudicated demand without a clear mechanism for decision-making. The problem was not volume, but the absence of a consistent adjudication engine capable of converting demand into actionable decisions.

The breakdown had cascading effects. Without active governance forums, requirements discipline eroded. Requests lacked clear ownership, scope, and articulation of mission value. Even when work advanced, it often did so without enterprise context, increasing the likelihood of duplication, misalignment, or late-stage rework. Governance became episodic and reactive, engaged only when issues escalated rather than as a routine part of lifecycle management.

Policy compliance, cybersecurity mandates, records management requirements, accessibility standards, and workforce limitations remained unavoidable realities throughout. Without early adjudication and prioritization, these constraints surfaced late, reinforcing perceptions of delay and inefficiency while masking the underlying governance gap.²⁴

The result was a widening trust deficit. Mission partners questioned the value of participating in intake processes with no visible outcomes, while IT organizations struggled to manage expectations without authoritative governance decisions. Restoring confidence required a

structural capability to reconstitute intake discipline, reconnect demand to governance, and ensure that requests were actively evaluated rather than passively received. The introduction of certified BRMs at DCMA was a direct response to that deficit.

DCMA's experience reflects a pattern that repeats across the Department of Defense. IT governance bodies have frequently struggled to sustain regular cadence, clear ownership, and consistent adjudication authority over time. As mission tempo and delivery complexity increased, many intake forums became episodic or informal, while others atrophied entirely. GAO assessments and DoD-level modernization reviews have repeatedly identified these dynamics, noting that the absence of disciplined demand governance undermines both agility and accountability.²⁵

Implementing Business Relationship Management at DCMA

Business Relationship Managers at DCMA were established as part of the IT Strategy and Planning function, with the intent to strengthen alignment between mission demand, enterprise priorities, and IT delivery. The Director of IT Strategy and Planning made a deliberate decision to staff the BRM function with certified practitioners, professionals who had pursued or were pursuing BRMP and CBRM credentials through the BRM Institute, rather than assigning coordination duties to existing staff or creating informal liaison positions. The expectation was explicit: certified competencies would produce different outcomes than improvised coordination. As BRMs began operating, they quickly identified a systemic breakdown in intake adjudication and governance continuity that directly impeded their mission.²⁶

Rather than creating a parallel structure, IT Strategy and Planning positioned BRMs to assume responsibility for reconstituting capability intake and adjudication. Existing Capability

Boards had largely ceased to function as consistent decision forums, leaving demand without authoritative pathways for review and disposition. Drawing on the demand-shaping and governance competencies embedded in the BRM certification framework, BRMs were tasked with stabilizing, and where necessary, taking over, these boards to restore intake discipline.²⁷

A. Establishing the BRM Function Within IT Strategy and Planning

The BRM role was deliberately embedded within IT Strategy and Planning to reinforce its enterprise perspective, consistent with the BRM Institute's guidance on organizational positioning. Placed there, BRMs could operate beyond individual projects or systems and focus on capability alignment, sequencing, and value realization. Applying the navigator and orchestrator competencies from the BRM Body of Knowledge, BRMs engaged with mission stakeholders before requests entered governance, to clarify intent, validate need, and surface constraints related to policy, security, workforce, and resourcing.²⁸

BRMs were not granted decision authority. Governance responsibility remained with the Capability Boards and their leadership sponsors. BRMs were held accountable, however, for preparing demand for adjudication and ensuring that submissions entering governance forums were complete, coherent, and aligned to strategic priorities. That distinction preserved governance integrity while improving the quality of information available for decision-making — a direct result of the requirements translation and portfolio management competencies that certified BRMs bring to the role.

B. Assuming Responsibility for Capability Intake and Adjudication

Responsibility for managing the Capability Boards transitioned to the BRMs, reestablishing intake as an active adjudication process rather than a passive collection mechanism. Applying the connector role described in the BRM Body of Knowledge, BRMs ensured that every

request had a defined pathway, an accountable sponsor, and a clear destination for decision-making. Requests no longer existed in an indeterminate state awaiting attention.²⁹

BRMs worked directly with stakeholders to translate ideas into articulated business requirements thereby clarifying scope, identifying dependencies, and distinguishing between immediate desires and underlying mission needs. By enforcing this discipline before board review, BRMs enabled the Capability Boards to focus on prioritization and trade-offs rather than clarification and rework. Over time, the boards recovered their functional relevance as genuine decision forums.

Transparency was central to this approach. Stakeholders received consistent feedback on request status, decision rationale, and next steps. Even when initiatives were deferred or declined, visible adjudication reduced incentives to bypass formal pathways. The BRM Body of Knowledge treats this visibility as more than a customer service function but also a governance discipline. The DCMA experience confirmed it is essential to rebuild stakeholder trust.

C. Operationalizing Intake Through Tooling

To sustain the reconstituted intake model, DCMA migrated IT capability intake into a centralized ticketing system. The migration embedded accountability into the intake lifecycle by capturing requests as structured records tied to specific Capability Boards, governance outcomes, and disposition categories.³⁰

Initial data reflected a surge of previously untracked or stalled requests entering the system, validating the BRM assessment that demand had not diminished but had lacked a functional adjudication mechanism. As legacy requests were evaluated and resolved, intake volumes normalized and settled into a pattern of routine operational demand. The ticketing system enabled clear differentiation between implemented, deferred, consolidated, and closed requests, giving

leadership verifiable evidence that intake was being actively managed rather than allowed to accumulate.

Measured Outcomes: Intake Maturity and Governance Performance

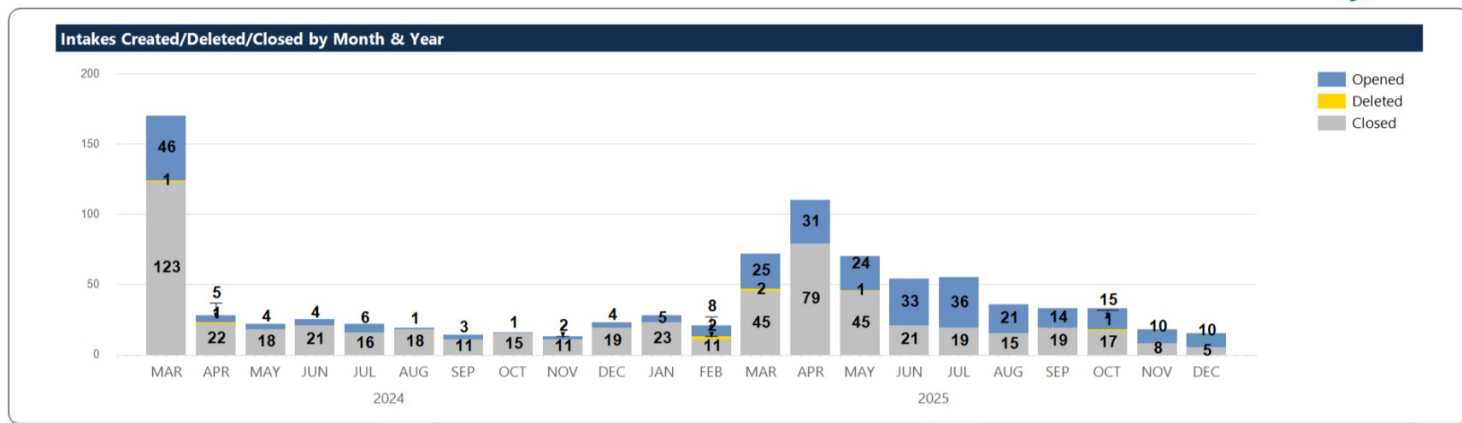
As certified BRM practices and supporting tooling became operational together, DCMA saw measurable changes in how demand moved through the intake and governance lifecycle. The changes did not primarily reflect a demand reduction. The Changes reflected a shift from unmanaged accumulation to active adjudication - with clear ownership, timelines, and outcomes. BRM competencies, centralized tooling managed by the BRM team, and a strong leadership commitment at all levels to the implementation all contributed to that shift.

The initial surge of requests entering the ticketing system represented the release of pent-up demand that had lacked a functional adjudication pathway. As legacy requests were evaluated and resolved, intake volumes normalized and settled into routine operational demand rather than backlog recovery. Eventually, new intakes rose as customers regained confidence in the process. This became a signal that restored governance credibility was driving renewed stakeholder engagement rather than simply a rising demand.

Resolution did not equate solely to implementation. Requests were actively reviewed and dispositioned based on mission value, feasibility, and alignment with enterprise priorities, implemented, deferred, consolidated with related efforts, or closed with documented rationale. Governance effectiveness is measured by decision quality and timeliness, not by approval rates, and the data from DCMA's intake system reflected that standard consistently.



Intake Stats since Ticketing System Migration



Migrated
1,488

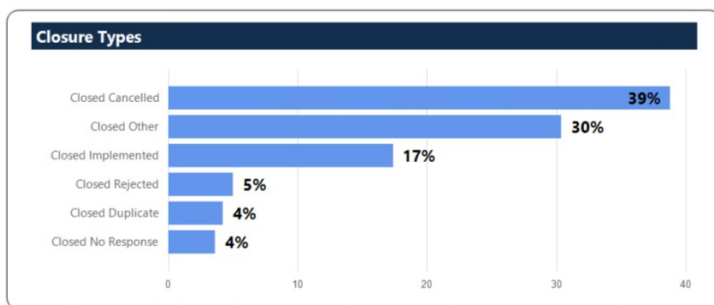
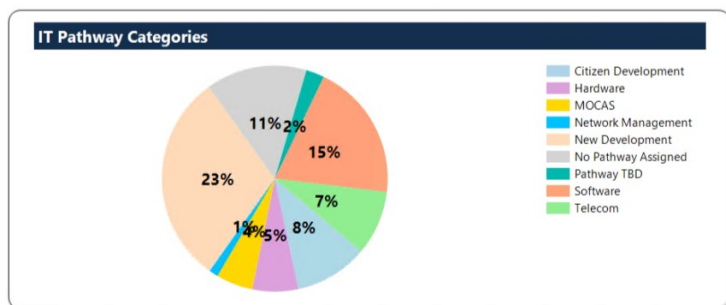
Opened
308

Deferred
32

Deleted
8

Implemented
87

Closed
581



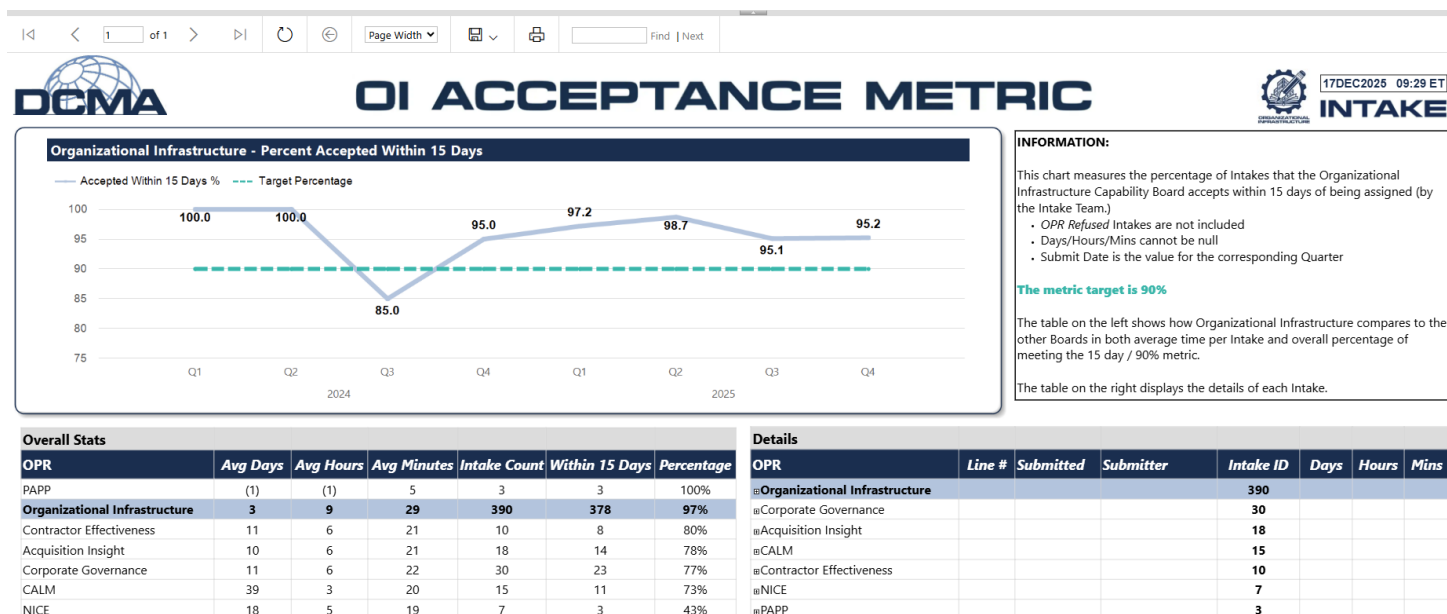
A. Capability Board Performance and Timeliness

The Organizational Infrastructure (OI) Capability Board illustrates how certified BRM engagement translated into improved governance performance. With BRMs managing intake preparation and board execution, requests entering OI arrived consistently scoped, validated, and aligned to defined criteria. The board's work shifted from clarification to prioritization.

Acceptance data shows that OI consistently began working intake requests within the established 15-day target across most reporting periods, even as overall intake volume increased - a standard the board had not met in the two years prior to BRM involvement.³¹ Requests were actively reviewed and assigned a path forward within defined timelines. That performance reflects restored board cadence and accountable governance, not simply faster processing.

B. Restoring Confidence Through Visible Adjudication

Beyond the intake metrics, the most consequential outcome was the restoration of stakeholder confidence. Requests no longer disappeared into opaque queues. Status, rationale, and next steps were visible throughout the lifecycle. Even when requests were deferred or declined, documented adjudication reduced frustration and minimized incentives to bypass formal pathways.



For leadership, intake, and governance performance data enabled more informed oversight. Trends in demand, board responsiveness, and disposition outcomes could be assessed over time, supporting continuous improvement rather than episodic intervention. Intake became a managed system rather than an accumulation of unresolved requests. The shift in situational awareness was enabled in part by the value harvesting competency that certified BRMs are trained to deliver, and visualized using dashboards fueled by data within the ticketing system.

Strategic Effects: From Intake Recovery to Enterprise Alignment

As governance processes stabilized, intake became a source of strategic insight — not just a processing function. BRMs identified recurring capability needs, emerging gaps, and cross-functional dependencies that had been invisible in a fragmented intake environment. This is precisely the strategic partnership role that CBRM certification is designed to develop.

With consistent visibility into demand patterns, BRMs identified recurring capability needs, emerging gaps, and cross-functional dependencies that had been invisible in a fragmented intake environment. That insight supported the development of multi-year roadmaps reflecting not only desired end states but realistic sequencing based on workforce capacity, policy constraints, and delivery risk. Planning discussions moved from reactive prioritization toward intentional alignment of near-term actions with longer-range objectives, a shift the DoD CIO has consistently identified as a priority for defense IT organizations.³²

BRMs also changed how value considerations entered demand discussions. Stakeholders were asked to articulate not only what capability was being requested, but why it mattered and how success would be assessed. That reframing shifted conversations from feature delivery to mission

outcomes, allowing governance bodies to evaluate trade-offs grounded in enterprise value rather than in urgency alone.³³

Roadmaps informed governance decisions, while governance outcomes refined planning assumptions. The feedback loop reduced the likelihood of disconnected initiatives advancing independently and increased confidence that approved efforts supported organizational priorities.³⁴

None of this required additional governance layers or new oversight structures. The shift came from applying certified BRM competencies within existing forums, supported by tooling that made demand visible and traceable. The DCMA experience demonstrates that the shift from reactive demand response to anticipatory planning is achievable — and that the BRM Institute’s competency framework is what makes it durable.

Applicability Across the Department of Defense

The conditions that allowed certified BRM practice to succeed at DCMA are widespread across the Department of Defense. Organizations such as the Defense Information Systems Agency (DISA), the Defense Logistics Agency (DLA), and Service-level IT components face structurally similar challenges: demand signals arriving through fragmented channels, governance boards that convene inconsistently, and limited visibility into how requests translate into decisions and outcomes. None of these organizations lack intake processes; they lack the sustained professional capacity to prepare demand for adjudication and carry it through governance to outcome. The existence of a globally recognized certification and competency framework means the DCMA model is replicable — not as a pilot to be reverse-engineered, but as a profession to be deployed.³⁵

Because the BRM Institute certifies practitioners against a standardized body of knowledge, organizations do not need to invent the model. Certified BRM professionals arrive with verified competencies in demand shaping, governance engagement, portfolio management, and value harvesting. The investment required is in placement, authority, and leadership commitment.

A. Conditions Required for Implementation

Successful adoption requires that senior leaders formally designate demand adjudication as a management priority, not an administrative function delegated to staff. In practice, this means Component Acquisition Executives, Chief Information Officers, and their deputies visibly sponsoring governance boards, attending periodic intake reviews, and treating unresolved demand backlogs as leadership indicators rather than IT-shop concerns. Without that visible commitment, even certified BRMs risk becoming informal coordinators rather than authoritative stewards of the demand lifecycle.³⁶

Clear ownership of demand is equally necessary. Mission stakeholders must be accountable for articulating need, value, and urgency, while IT organizations remain accountable for feasibility, sequencing, and delivery. Certified BRMs function most effectively when these roles are understood and reinforced through governance and when the BRM's strategic partnership function is formally recognized as distinct from project management, business analysis, or IT program coordination.

A reasonable question is why BRM specifically, rather than other governance improvement mechanisms. Strong IT business analyst functions, revamped program management offices, and ITIL service management frameworks each address portions of the demand governance problem — and DCMA has used elements of all of them. What those approaches do not provide is a

practitioner whose primary accountability is the health of the relationship between mission partners and the IT organization across the full demand lifecycle: from need identification through adjudication, delivery, and value assessment. Business analysts scope requirements; program managers execute approved work; service managers maintain operational continuity. None of these roles is designed to own the governance of demand before it reaches any of those functions. That is precisely the gap BRM is built to close, and why certification against a defined competency framework — rather than a reorganized title or reassigned duty — is what produces different outcomes.

Organizations must also establish intake pathways tied to governance forums with defined charter authority, recurring meeting schedules, and documented disposition standards. For components operating under the DoD IT governance framework, this means aligning BRM-managed intake with existing structures such as the Defense Business Systems Management Committee process or Service-level IT Investment Review Boards, rather than creating parallel mechanisms. Requests must have a clear destination, a review cadence, and an expected disposition timeline. Intake mechanisms that exist without authoritative adjudication endpoints, that meet irregularly, lack quorum requirements, or produce no binding decision, will continue to accumulate demand without resolution; regardless of BRM investment.

B. Enablers That Support Success

The most significant enabler is investment in certified BRM practitioners. The BRMP and CBRM credentials ensure that BRMs possess the mission fluency, portfolio management discipline, and communication competencies the role requires. Organizations that attempt BRM without certified professionals find the role defaulting to liaison or project coordination — which

produces activity without governance transformation. The BRM Institute's certification pathway provides a clear development roadmap, whether building internally or hiring externally.

Process discipline upstream of governance is another key enabler. When requirements clarity, scope definition, and dependency identification occur before board review, governance discussions shift from clarification to prioritization. Decision quality improves and cycle time decreases.

Transparency reinforces all of this. Stakeholders engage with formal intake processes when they can see what happened to their request and why. Even unfavorable decisions build confidence when they are timely and clearly explained. The BRM Body of Knowledge treats governance visibility as a strategic competency — one that certified practitioners are trained to exercise consistently.

Several DoD-specific realities shape both the opportunity and the complexity of scaling this model. On the enabling side: the DoD CIO's sustained emphasis on IT modernization and demand discipline creates a policy environment receptive to structured governance investment; existing DevSecOps frameworks in software-intensive components provide a compatible process culture where BRM demand shaping fits naturally upstream of delivery pipelines; and the PPBE reform conversation has increased appetite for mechanisms that link capability investment to demonstrable mission value. On the barrier side: annual budget cycles complicate multi-year BRM workforce development commitments; component-level IT governance authority varies considerably, with some organizations lacking the charter clarity to seat governance boards with real adjudication power; and existing frameworks such as DoDAF and IT Box may create process friction if BRM intake is not explicitly mapped to their stage-gate requirements. These conditions

are not disqualifying, but they argue for implementation strategies tailored to the specific governance architecture of each component rather than a single enterprise mandate.

C. Risks and Failure Modes

Most BRM implementation failures trace to under-investment in professional certification. When organizations assign BRM titles to personnel who lack the competency framework provided by the BRMP or CBRM, the role tends to default to liaison rather than governance integrator. Intake volume may increase without corresponding improvement in decision outcomes.

Tooling adoption without process reform is another common failure mode. Centralized intake systems become digital holding areas when adjudication authority, cadence, and accountability are not clearly defined. Metrics show activity without reflecting meaningful progress.

Cultural resistance presents a third challenge. Stakeholders accustomed to informal access or expedited pathways may resist structured intake, particularly if early implementation does not produce visible results. Sustained leadership reinforcement and early wins are both essential. Certified BRMs — trained in relationship building and communication — are better equipped to manage that transition than coordinators without the professional grounding.

D. Mitigating Risk Through Intentional Design

Most of these risks are addressable through deliberate design choices. Chartering the BRM role with explicit reference to the professional competency framework — and formally integrating it into governance processes — prevents role dilution. Requiring BRMP certification as a baseline for BRM positions, and incentivizing CBRM attainment for senior practitioners, establishes the competency floor that separates professional BRM from informal coordination. A phased

implementation that targets high-visibility demand areas first generates early wins and builds institutional confidence.

Metrics should emphasize decision quality and timeliness rather than volume alone. Measures that track adjudication outcomes, acceptance timelines, and disposition clarity give leadership insight into governance health. When these indicators improve consistently, they confirm that process and leadership investment is translating into governance maturity. The BRM Institute's Body of Knowledge offers specific guidance on relationship maturity assessments and value realization tracking that defense organizations can adapt to their governance contexts.

E. Limitations and Recommended Next Steps

The DCMA case demonstrates a credible proof of concept, but it is a single organization with a specific mission profile, workforce culture, and leadership commitment that may not be uniformly present elsewhere. DCMA's contract management mission produces relatively discrete, traceable demand categories well-suited to the BRM intake model. Components with more diffuse mission portfolios, higher stakeholder dispersion, or weaker IT governance baselines may find implementation more complex. Broader validation through structured pilots in two or three varied components such as a Service-level IT organization, a combat support agency such as DLA, or a headquarters staff element, would help confirm what scales, what requires adaptation, and where the model faces genuine constraints.

Recommended next steps follow directly from these limits. An independent review of DCMA's governance metrics by an external evaluator — a defense audit institution or academic partner — would strengthen the evidentiary basis and give the model credibility beyond practitioner self-assessment. A modest cost-benefit analysis comparing BRM certification investment against measurable reductions in adjudication cycle time and rework would give

decision-makers the economic framing defense budgeting processes require. Finally, DoD CIO-sponsored guidance formally recognizing BRM as an IT governance competency, analogous to existing guidance on IT project management and cybersecurity workforce development, would create the institutional signal that components need to move from isolated experiments to deliberate capability building.

Institutionalizing Trust in the IT Lifecycle

Restoring confidence in the IT lifecycle takes more than better tools or isolated governance reforms. It takes certified professionals with a verifiable competency framework, placed where the governance work actually happens. By embedding BRMs within IT Strategy and Planning and giving them responsibility for intake adjudication, DCMA turned a symbolic activity into a functional decision system.

Trust was the most consequential outcome of that transformation — but it is not sufficient on its own. The capability gap between DoD and the private sector closes when IT organizations can actually absorb and integrate new capabilities at pace. When demand is shaped and adjudicated by practitioners with verified competencies, defense organizations can move closer to commercial cycle time. That is the operational payoff.

The surge implications are direct. Acquisition organizations cannot scale rapidly when IT demand is fragmented and governance is episodic. Certified BRM-enabled demand discipline gives leaders visibility into what exists, what is constrained, and what depends on what — before crisis conditions emerge. That visibility allows execution to accelerate under pressure rather than scrambling to impose structure after the fact. In conditions where the nation depends on its acquisition system to field capabilities faster than an adversary can adapt, the difference between a

governance system that is ready and one that is not is a national security variable, not an administrative one.

DCMA's governance boards did not cease functioning because of insufficient effort or intent. They ceased functioning because no one owned the preparation work and the boards had drifted from planning functions. Certified BRM practice addressed those gaps by reconstituting existing mechanisms and ensuring they were supported by clear professional roles, defined processes, and traceable data.

The gap between technological opportunity and organizational execution in the Department of Defense is not closing on its own. The profession of Business Relationship Management already provides the mechanism to close it. Defense organizations do not need to invent a solution — they need to treat BRM as a professional investment and deploy it at the scale the problem demands.

Endnotes

- ¹ Government Accountability Office, *Weapon Systems Annual Assessment: Programs Are Not Consistently Implementing Practices That Can Help Accelerate Acquisitions*, GAO-23-106059 (Washington, DC: GAO, 2023).
- ² Department of Defense Chief Information Officer, *DoD Information Technology Modernization Strategy* (Washington, DC: DoD CIO, 2019).
- ³ Office of Management and Budget, *Circular A-11*, Section 55, "Information Technology Investments" (Washington, DC: OMB, current edition).
- ⁴ Government Accountability Office, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-471 (Washington, DC: GAO, 2019).
- ⁵ Office of Management and Budget, *Circular A-11: Preparation, Submission, and Execution of the Budget*, Section 55 (Washington, DC: OMB, current edition).
- ⁶ Department of Defense Chief Information Officer, *DoD Information Technology Modernization Strategy* (Washington, DC: DoD CIO, 2019).
- ⁷ Author, practitioner observation and internal organizational experience at the Defense Contract Management Agency (DCMA), FY23–FY25.
- ⁸ Business Relationship Management Institute, *The BRM Discipline* (BRM Institute, updated edition).
- ⁹ Business Relationship Management Institute, *The BRMP Guide to the BRM Body of Knowledge* (Van Haren Publishing, 2013).
- ¹⁰ Business Relationship Management Institute, "Business Relationship Management Professional (BRMP®)," brm.institute, accessed December 2025; APMG International, "Business Relationship Management (BRM) Certification," apmg-international.com, accessed December 2025.
- ¹¹ Business Relationship Management Institute, "Certified Business Relationship Manager (CBRM®)," brm.institute, accessed December 2025.
- ¹² Business Relationship Management Institute, "A Practical Guide to Your Certification Journey: BRMP, CBRM, and MBRM," brm.institute, March 14, 2024.
- ¹³ Business Relationship Management Institute, *The BRMP Guide to the BRM Body of Knowledge*; Business Relationship Management Institute, "BRM Metrics," brm.institute, accessed December 2025.
- ¹⁴ Business Relationship Management Institute, *The BRMP Guide to the BRM Body of Knowledge* (Van Haren Publishing, 2013).
- ¹⁵ Business Relationship Management Institute, *The BRM Discipline* (BRM Institute, updated edition).
- ¹⁶ Business Relationship Management Institute, *The BRMP Guide to the BRM Body of Knowledge* (Van Haren Publishing, 2013).
- ¹⁷ Robert S. Kaplan and David P. Norton, *Strategy-Focused Organization* (Boston: Harvard Business School Press, 2001).
- ¹⁸ Project Management Institute, *Business Analysis for Practitioners: A Practice Guide* (Newtown Square, PA: PMI, 2015).
- ¹⁹ Business Relationship Management Institute, "BRM Capability: Strategic Planning and Roadmapping," brm.institute, accessed December 2025; Business Relationship Management Institute, *The BRMP Guide to the BRM Body of Knowledge*.
- ²⁰ Author synthesis informed by DCMA BRM implementation experience and defense IT governance practice, FY23–FY25.
- ²¹ ISACA, *COBIT 2019 Framework: Governance and Management Objectives* (Schaumburg, IL: ISACA, 2018). The BRM competency framework's emphasis on value realization, portfolio management, and stakeholder engagement aligns with COBIT's governance objectives for managing IT-related demand and overseeing delivery. See also Office of Management and Budget, *Circular A-130: Managing Information as a Strategic Resource* (Washington, DC: OMB, 2016), which establishes parallel federal expectations for IT governance discipline and senior accountable officer responsibility.
- ²² Author, practitioner observation and internal organizational experience at the Defense Contract Management Agency (DCMA), FY23–FY25.
- ²³ Author, internal assessment of DCMA IT intake and governance practices, FY23–FY24.
- ²⁴ Department of Defense Chief Information Officer, *DoD Information Technology Modernization Strategy* (Washington, DC: DoD CIO, 2019).
- ²⁵ Government Accountability Office, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, DC: GAO, 2023); Department of Defense Chief Information Officer, *DoD Information Technology Modernization Strategy* (Washington, DC: DoD CIO, 2019).
- ²⁶ Author, practitioner observation and internal organizational experience at DCMA IT Strategy and Planning, FY23–FY25.
- ²⁷ Author, internal assessment of Capability Board functionality and BRM role evolution, FY23–FY24.
- ²⁸ Business Relationship Management Institute, *The BRMP Guide to the BRM Body of Knowledge*; Business Relationship Management Institute, "BRM Capability: Strategic Planning and Roadmapping," brm.institute, accessed December 2025.
- ²⁹ Author synthesis informed by BRM-led intake governance realignment at DCMA, FY23–FY25.
- ³⁰ Ibid.

³¹ DCMA-generated governance performance metrics for OI Capability Board intake acceptance timelines, FY24–FY25.

³² Department of Defense Chief Information Officer, *DoD Information Technology Modernization Strategy* (Washington, DC: DoD CIO, 2019).

³³ Robert S. Kaplan and David P. Norton, *Strategy-Focused Organization* (Boston: Harvard Business School Press, 2001).

³⁴ Author synthesis informed by DCMA enterprise planning and IT governance integration efforts, FY24–FY25.

³⁵ Government Accountability Office, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, DC: GAO, 2023).

³⁶ Department of Defense Chief Information Officer, *DoD Information Technology Modernization Strategy* (Washington, DC: DoD CIO, 2019).

Disclosure

This paper was developed as a research requirement of the Strategic Acquisition Course (ES 6155) at the Dwight D. Eisenhower School for National Security and Resource Strategy, National Defense University. The views expressed are solely those of the author and do not represent the official policy or position of the Eisenhower School, the National Defense University, the Defense Contract Management Agency, the Department of Defense, or the United States Government.

About the Author

Dr. Tobalina Beck, JD, BRMP, CISM, CISSP, is an acquisition professional at the Defense Contract Management Agency, where she has served in IT strategy and planning roles with direct responsibility for demand governance, capability intake, and governance reconstitution. She is a 2025 cohort member of the Defense Senior Leader Development Program, sponsored by DCMA. The DCMA IT governance experience described in this paper reflects her direct practitioner observation from FY23–FY25. She holds a Juris Doctor and certifications in Business Relationship Management (BRMP®), Information Security Management (CISM), and Information Systems Security (CISSP), and brings a background in law, cybersecurity, and organizational governance to her work in defense acquisition.