Chapter 5

GRC for Public Safety

Understanding Governance, Risk, and Compliance (GRC) for Public Safety

Jason Franks
Senior Cybersecurity & GRC Analyst
Mission Critical Partners

Steve Badgio
Vice President & Director of Co-Managed Information Technology (CMIT)
Mission Critical Partners

Why Is a GRC Program Essential for Public-Safety Agencies?

Public-safety agencies operate in an increasingly complex environment where governance, risk, and compliance (GRC) responsibilities are often fragmented and inconsistently managed. As threats intensify and regulatory expectations shift, agencies must transition from reactive, siloed practices to a unified, organization-wide approach. A well-designed GRC program enhances resilience, strengthens informed decision-making, and builds shared accountability — ultimately improving an agency's ability to safeguard its people, systems, and the communities it serves.

What Is the Current State of GRC in Public Safety?

Modern public-safety organizations face mounting operational pressures, rapidly advancing technologies, and expanding regulatory requirements. Yet many still manage GRC activities in isolated pockets, resulting in inconsistent practices and blind spots that adversaries can exploit. A holistic GRC program replaces these sporadic efforts with a disciplined, coordinated approach that improves preparedness, responsiveness, and long-term strategy.

Improved organizational maturity is a key opportunity. While many agencies maintain strong practices within specific departments, processes often vary significantly across the enterprise. Standardizing policies, aligning risk activities, and implementing repeatable workflows help agencies shift from episodic responses to predictable and sustainable risk management. This consistency supports efficiency, accountability, and resilience.

Success also depends on executive leadership and organizational culture. GRC initiatives cannot succeed without sustained engagement from leadership and broad cultural acceptance of continuous risk management. When leaders champion GRC as a strategic priority, agencies maintain momentum through staff turnover, funding fluctuations, and operational disruptions. Embedding GRC into everyday operations ensures it becomes a habitual practice rather than an occasional compliance obligation.

Finally, agencies gain significant value from anchoring GRC programs to established standards and frameworks. Using structured frameworks reduces ambiguity, eliminates gaps, ensures uniform controls, and helps demonstrate due diligence to regulators and stakeholders. The use of GRC platforms and GRC systems helps agencies centralize and automate many of their compliance processes. Collectively, these improvements strengthen cybersecurity posture and increase organizational resilience.

What Are the Key Opportunities for Improving GRC?

How Can Agencies Adopt a Holistic GRC Approach? – Public-safety agencies traditionally manage GRC in silos — e.g., IT handles cybersecurity, the facilities team oversees physical security, HR manages personnel processes, and leadership engages only intermittently. This fragmented structure creates gaps and periods of heightened vulnerability. In contrast, a unified GRC approach:

- Replaces inconsistent or episodic practices with continuous management.
- Enables proactive planning and rapid threat response.
- Breaks down organizational silos and fosters shared accountability.
- Provides leadership with a comprehensive view of organizational risk.
- Holistic GRC encourages collaboration, clarity, and structured oversight, enabling more effective decisions during both routine operations and crises.

How Can Agencies Increase Organizational Maturity and Consistency? – Many agencies rely on pockets of excellence surrounded by uneven processes. Institutional knowledge often is concentrated in a few employees, leaving programs vulnerable to staff turnover and operational disruptions. Improving maturity helps agencies:

- Move away from reactive, event-driven practices.
- Reduce isolated decision-making.
- Apply uniform standards across departments.
- Institutionalize repeatable, documented processes.
- Prevent organizational drift and policy decay.

Standardization ensures that core practices remain consistent regardless of personnel or external pressures.

Why Is Executive Buy-In Crucial for GRC Success?

Leadership engagement and cultural transformation often determine the success or failure of GRC efforts. Without strong executive support, initiatives stall. Without cultural adoption, even well-designed processes fail to take hold. Effective leadership and culture change enable agencies to:

- Elevate GRC as an organization-wide strategic priority.
- Sustain progress through leadership changes, staffing shifts, and funding challenges.
- Develop a resilient workforce that continuously adapts to evolving threats.
- Embed GRC into daily operations rather than treating it as a compliance checkbox.

GRC thus becomes a shared responsibility that permeates organizational behavior.

How Can GRC Frameworks and Standards Be Used More Effectively? – Public-safety agencies operate within a complex regulatory environment involving federal, state, local, and industry-specific requirements. Many agencies struggle to identify which standards apply and how they intersect. A formal GRC program helps agencies:

- Align with established frameworks such as CJIS[1] Security Policy, NIST[2] SP 800-53, and the NIST Cybersecurity Framework.
- Standardize and rationalize controls across departments.
- Reduce inconsistencies, redundancies, and compliance gaps.
- Demonstrate due diligence to regulators, funding bodies, and the public.

Frameworks provide structure and predictability, which are especially valuable in less-mature environments.

What Are the Common Challenges in Implementing GRC?

How to Overcome "Paralysis by Analysis" in GRC Implementation – The complexity of GRC — cross-department coordination, standards alignment, continuous monitoring, risk assessments, risk registers, and regular policy reviews — can overwhelm agencies. This can lead to significant hesitation, delaying action despite escalating threats. Factors contributing to paralysis include:

- Intimidation caused by perceived complexity.
- Limited personnel and time.
- Uncertainty about where to begin.
- Lack of clear executive direction.

Incremental progress and visible leadership support are essential to overcoming these barriers.

1 Criminal Justice Information Services.
2 National Institute of Science and Technology.

What Are the Dangers of an Inconsistent Approach to Risk Management? – Many agencies manage risk only during major events such as facility construction, system deployments, hardware refreshes, or post-incident reviews. Once the project concludes, risk management and compliance often drops off sharply until the next major event — or disappears completely. This creates a pattern of:

- Intense short-term engagement.
- Long periods of inattention.
- A "check the box" mentality that assumes potential risks have been permanently resolved.

Such inconsistency weakens the agency's ability to maintain a resilient cybersecurity and operational posture.

How to Determine Which GRC Standards and Frameworks Apply – Agencies frequently operate under numerous overlapping requirements with little internal alignment regarding which standards apply. Compliance knowledge often is distributed across departments:

- Legal may understand one set of obligations.
- IT another.
- Operations yet another.

No single group typically owns the full picture. Additionally, standards evolve regularly — for example, expanded CJIS requirements, shifting state cybersecurity statutes, or updated federal guidance. Agencies without dedicated compliance monitoring struggle to keep pace.

Even when agencies know the requirements, prioritizing and sequencing them remains a challenge.

How Is the Evolving Cybersecurity Threat Landscape Affecting Public Safety? – Public-safety agencies face significant cybersecurity risks due to their mission-critical operations. Cyberattackers increasingly target these organizations because disruptions can have severe consequences. Key factors include:

- AI-powered cyberattacks that accelerate phishing, reconnaissance, and exploitation.
- Growing emphasis on the human element as the primary attack vector.
- Expanded attack surfaces as agencies implement new systems and technologies.
- Increased complexity in maintaining defenses across interconnected environments.

Continuous training, monitoring, and modernization are required to stay ahead of adversaries.

What Are the Trends in Public-Safety GRC?

Increased adoption of holistic GRC approaches – Public-safety agencies increasingly will adopt coordinated GRC strategies that eliminate blind spots, support continuous monitoring, and improve situational awareness. This shift will integrate processes, enhance visibility, and enable more-proactive management of risk.

Improved organizational maturity and consistency – More agencies will develop standardized processes and institutionalized workflows. This effort will reduce reactive behavior, promote enterprise-wide alignment, and drive more-consistent decision-making across departments.

Enhanced executive buy-in to drive culture change – Leadership engagement will continue increasing as executives recognize GRC as essential to operational resilience and community trust. As the agency's culture evolves, GRC will become part of daily operations rather than an occasional compliance effort.

Greater use of standards and frameworks – Agencies increasingly will anchor their GRC programs in proven frameworks to standardize controls, identify and eliminate security gaps, and enhance predictability across operations.