Beyond Compliance: Turning Security Risk Frameworks into a Strategic Advantage

Many organisations, particularly government departments, often view security risk frameworks with scepticism. Business leaders may see them as bureaucratic obstacles that slow delivery and add unnecessary "*red tape*." In Australia's highly regulated environment, such measures can be perceived as increasing the burden on non-core functions.

Dealing with resistance to security risk frameworks in business units is as much about psychology and culture as it is about policy and process. The key is to shift the conversation from "*compliance*" to "*shared value*" so that security is seen as enabling the business, not hindering it.

But what if we reframed security from a compliance obligation into a business enabler? What if, instead of enforcing rules, we built capability, adaptability, and opportunity into the way we manage risk? Traditional resilience is about bouncing back after disruption.

This article offers tools to help security risk practitioners address this issue.

Understand the Root of Resistance

Before you can influence reluctant stakeholders, you need to know *why* they are resisting.

- Misconceptions: They may believe security will slow them down or add unnecessary cost.
- Competing priorities: Service delivery, budget constraints, or political pressures may take precedence.
- Past experiences: Previous "*security initiatives*" may have been rigid, irrelevant, or poorly communicated.
- Business unit owners often resist because they see frameworks as rigid and imposed. By starting with *their* people and challenges, you show you are enabling them, not policing them.
- Run short, scenario-based workshops that simulate real risks to their operations. Let them experience how preparedness improves outcomes.

Communicate in Business Language

- Link to business objectives – Show how the framework protects revenue, brand reputation, and customer trust.
- Use relatable scenarios – Replace abstract risk scores with real-world examples of incidents in similar industries.
- Highlight competitive advantage – Position strong security as a differentiator that can win deals or meet client requirements.

Integrate with How They Work

- Co-create controls – Invite business unit leaders to help tailor the framework so it fits operational realities.
- Pilot programs – Start with a small, low-risk area to demonstrate value before scaling.
- Champion network – Identify and empower "security ambassadors" within each unit to advocate for the framework.
- Involving owners in tailoring the framework ensures it fits operational realities, reducing the "*this doesn't work for us*" pushback.
- Invite them to help design controls, with the understanding that these can evolve as business needs change.

Build Capability and Confidence

- Targeted training – Focus on practical, role-specific guidance rather than generic awareness sessions.
- Show quick wins – Demonstrate measurable improvements (e.g., reduced incident response time) within weeks, not months.
- Provide tools, not just rules. Offer easy-to-use templates, checklists, and automation to reduce friction.
- Quick, visible improvements reduce scepticism and build momentum.
- Start with a small pilot in their unit, measure results (e.g., reduced downtime, faster approvals), and publicise the success internally.

Traditional security rollouts aim for compliance. The leadership shift we need should turn its focus to capability, equipping teams to manage uncertainty themselves.

- Compliance is about ticking boxes.
- Capability is about making better decisions under pressure.

When business units see security as a tool for *their* success, not just a corporate mandate, resistance starts to fade. This means reframing security from a necessary obligation to a strategic partner. It means bringing your risk leaders into growth conversations early, not looping them in at the "*approval*" stage. And it means funding frameworks not because you fear the regulator, but because you value the resilience, they give you to move faster than your rivals.

Security is a human challenge before it is a technical one.

- Train situational awareness so teams can spot risks early.
- Use scenario-based exercises to make threats tangible and relevant.
- Encourage adaptive decision-making over rigid rule-following.

When people feel confident in their ability to respond, frameworks become enablers, not obstacles.

Strengthen Culture – Multiplier Effect

- Recognise and reward – Publicly acknowledge teams that adopt and improve security practices.
- Integrate into performance metrics – Make security KPIs part of business unit scorecards.
- Storytelling – Share success stories where security measures prevented costly incidents.
- Owners see that the framework is not static. it improves with their input, making them coowners of its success.
- After any event, run a short, blamefree review and feed lessons back into both the framework and their processes.

Escalate Strategically (When needed)

- Leverage governance – If resistance persists, use formal risk acceptance processes so accountability is documented.
- Executive sponsorship – Ensure senior leadership visibly supports and participates in the framework rollout.

Government Context: The Four Influence Profiles

In public sector settings, business unit leaders often fall into one of four motivator types:

Profile	**Mindset**	**Leverage**
Budget-Constrained	"We have no extra funding."	Prevention saves taxpayer money and protects service continuity.
Service Delivery –Focused	"Security slows us down."	Readiness enables faster, more reliable delivery.
Reputation & Public Trust–Driven	"Our credibility is everything."	Strong posture is a visible sign of good governance.
Change-Resistant	"We've always done it this way."	Adaptability is essential in shifting policy and threat landscapes.

Case Study: HSS Response - Transforming Security from Compliance to Strategic Capability

Context

During the GLNG Upstream Project, Santos and Fluor faced a complex challenge: delivering emergency and critical operational support across vast, remote, and high-risk environments. In response, the HSS Response Team was

created, a centralised capability designed to unify fragmented safety and security functions into a cohesive, mission-aligned framework. The concept was born not from regulatory pressure, but from a strategic vision to protect people, assets, and the project's social license to operate.

Challenge

Initial resistance mirrored what many business units face when confronted with security frameworks:

- Perceived bureaucracy: Teams feared added layers of oversight would slow down operations.
- Fragmented services: Emergency response, security, and medical support were siloed, leading to inefficiencies and unclear accountability.
- Community scrutiny: The project's visibility and legislative obligations demanded a proactive, transparent approach to risk.

Strategic Intervention

The HSS Response concept embodied the principles included in this article:

- Modular Integration: Functions like threat assessment, emergency coordination, and law enforcement liaison were unified under one operational umbrella, mirroring the modular rollout strategy.
- Co-Design and Embedded Presence: The team was embedded within key project sites, working alongside medical clinics and VIIRT units to ensure seamless interoperability. This proximity built trust and reduced resistance.
- Strategic Framing: Security was not sold as compliance, it was positioned as a strategic enabler of workforce confidence, stakeholder trust, and operational continuity.
- Capability over Control: The team did not just enforce rules, they provided tools, training, and real-time support, empowering site leaders to respond adaptively to emergent risks.

Outcome

- Operational Efficiency: HSS Response oversaw 12 camps and 3 hub sites, coordinating 70+ security officers and medical personnel with precision.
- Stakeholder Trust: The concept became a visible symbol of Fluor's commitment to community safety and project integrity.
- Scalable Legacy: Designed with mobility in mind, the framework was built to follow evolving scopes of work, futureproofing the model for other projects.
- Cultural Shift: Emergency drills, scenario-based exercises, and integrated planning transformed security from a background function into a frontline capability.

Legacy Impact

The HSS Response concept did not just meet regulatory obligations, it redefined them. It proved that when security is framed as a strategic, adaptive, and community-conscious capability, resistance fades and resilience flourishes. This case affirms that security frameworks succeed when they are co-authored, mission-aligned, and embedded in the rhythms of real work.

- Security must be embedded, not imposed.
- Co-authorship builds ownership.
- Modular rollout enables scalability.
- Framing determines adoption - mission beats mandate.

By identifying which profile you are dealing with, you can tailor your message to their priorities and move from resistance to readiness.

Security risk is not about surviving the storm, it is about learning to sail so well that you can change course, seize new winds, and arrive stronger than before.

If you want your security risk framework to stick, stop selling compliance. Start building capability, adaptability, and opportunity, and watch resistance turn into advocacy.

- Resilience as a Strategy - Position security frameworks as tools that convert disruption into competitive advantage.
- Transparency Builds Trust - Showcase lessons learned and maturity journeys to build stakeholder confidence.

- Culture as a Multiplier - Embed security into cultural rituals, onboarding, retros, leadership reviews.
- Personal Branding - Encourage security leaders to build visible, values-driven profiles.

Instead of trying to *convince* reluctant owners to accept a framework help position the security risk function as a partner helping them futureproof their business. You are not asking them to "*comply*," you are offering them a competitive edge in a volatile environment.

Ultimately, the success of any security risk framework lies not in its technical precision but in its human adoption. When business units see themselves not as subjects of compliance but as co-authors of resilience, the framework becomes a living strategy, adaptive, empowering, and mission aligned.

By shifting the narrative from control to capability, from enforcement to enablement, we unlock a culture where security is not resisted but revered. This is how we move beyond compliance, by building systems that protect not just assets, but the trust, continuity, and purpose that define our legacy.