The Embedded Security Maturity Playbook

BAD BADGER

Information Security

The Embedded Security Maturity Playbook

A Practical Guide for Aligning IT and Cybersecurity

By Dave Brock, Principal Consultant | BadBadger Information Security

BAD BADGER

Information Security

Introduction

Cybersecurity can no longer operate as a parallel function to IT—it must be embedded. Leaders face growing complexity, tighter timelines, and increasing pressure to deliver both speed and security. When security is treated as a hurdle, it gets bypassed. When it's built into operations, it becomes a catalyst for resilience, trust, and long-term value.

This playbook introduces a practical maturity curve to guide organizations from reactive security postures to fully embedded, operationalized security programs. At each step, we outline what success looks like—not from a compliance checkbox perspective, but from the vantage point of **real business alignment**. It's not about more policies; it's about sharper implementation, shared ownership, and workflows that can withstand real-world pressure.

We draw on direct experience with IT and InfoSec teams navigating conflicting incentives, limited resources, and shifting risks. The most effective teams are those who bridge the divide early and often—designing controls that people will actually use, working from policies that reflect what's really happening on the ground, and embracing automation that reduces risk without adding friction.

The journey to **embedded security** requires being both intentional and for stakeholders to practice ownership with accountability. With the right mindset, alignment, and communication strategies, even small changes can produce big wins. Whether you're building your first intake process or rethinking audit prep, this guide offers practical, tested actions for every maturity level.

In the next few pages, you'll find:

- A three-stage maturity model
- Practical actions you can implement immediately
- Real-world patterns for aligning security with IT
- Milestones to measure progress toward resilience

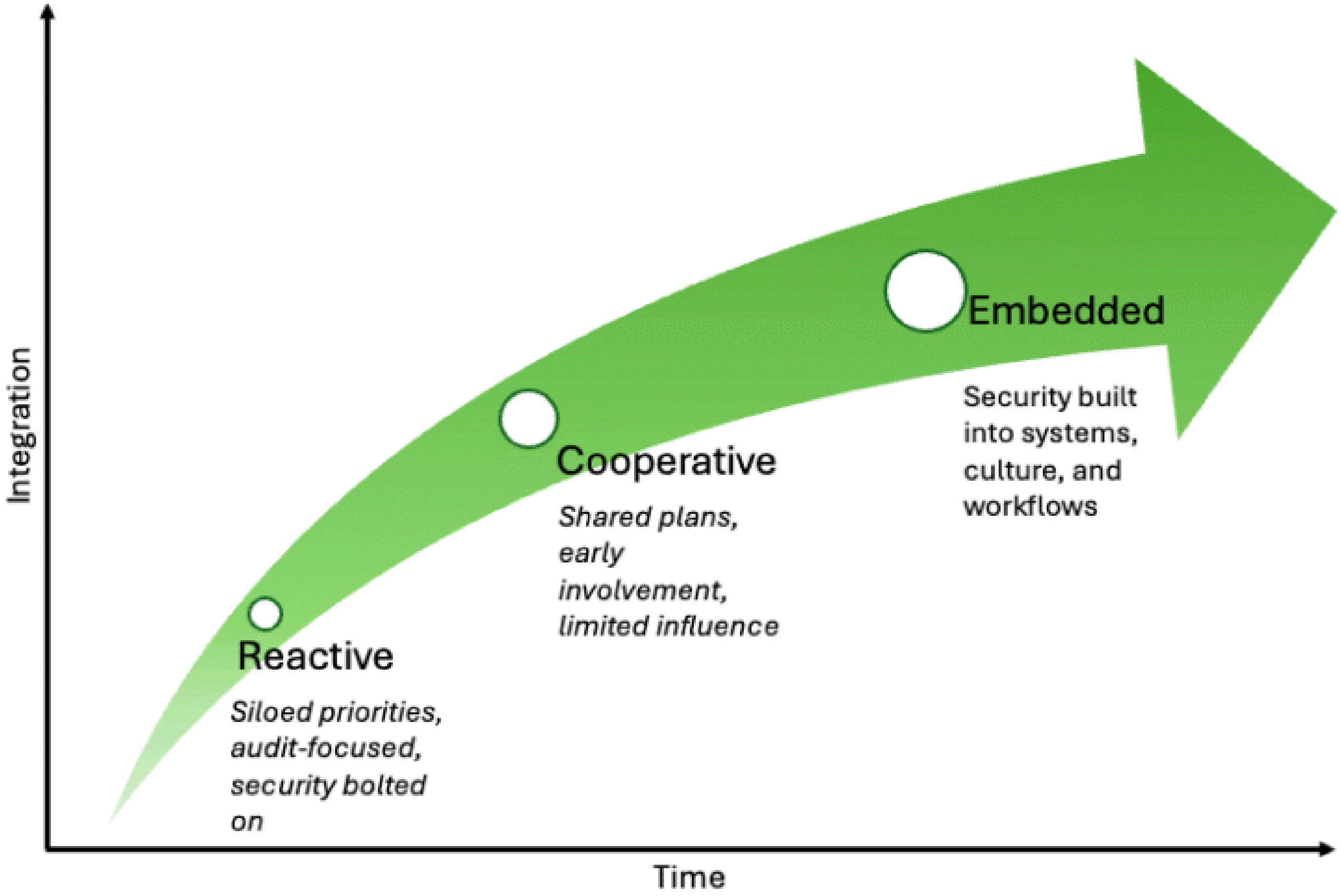
Let's dig in.

The Embedded Security Maturity Curve

Most organizations want stronger security. But real resilience isn't built by layering on more policies—it's achieved by integrating security into how systems are built, operated, and improved.

The Embedded Security Maturity Curve helps organizations understand where they are and what it takes to level up. The journey isn't just about adding more controls—it's about aligning the right people, systems, and decisions under real-world pressure.

Each stage reflects a distinct posture and mindset, with measurable indicators and actionable next steps.


Integration
Time
Reactive
Siloed priorities, audit-focused, security bolted on
Cooperative
Shared plans, early involvement, limited influence
Embedded
Security built into systems, culture, and workflows

REACTIVE

Security is fragmented, after-the-fact, or mostly policy-driven.

- Security is seen as a blocker
- Controls exist on paper but not in practice

- Audits are painful, ad hoc efforts
- IT and InfoSec work in parallel silos
- Risks are identified after systems go live

🔑 *Next step*: Create shared ownership by embedding security reviews in IT workflows and planning processes. Don't aim for perfection—start with inclusion.

COOPERATIVE

Security is part of the process, but not always early enough.

- Security and IT collaborate on initiatives
- Basic controls are aligned with real practices
- Some automation exists, often around compliance
- Risk conversations happen before—not after—deployment
- Policy language is being rewritten by those who implement it

🔑 *Next step*: Increase feedback loops and embed security champions within delivery teams. Shift from periodic reviews to continuous engagement.

EMBEDDED

Security is an operational norm, not a separate function.

- IT and InfoSec operate as one team
- Secure design principles guide build decisions
- Automation supports control enforcement by default
- Documentation reflects current systems and usage
- Audit readiness is a natural byproduct of good operations

🔑 *Next step*: Focus on scalability, cultural reinforcement, and resilience testing. Formalize playbooks, measure effectiveness, and drive security decisions with data.

NOTE:

This curve isn’t a checklist—it’s a lens. Use it to evaluate where your organization stands and identify the necessary conversations to have next.

Operationalizing Embedded Security

From alignment to action—here's how real maturity takes root.

Once organizations understand the value of aligning IT and security, the next question is always the same: *How do we make it real?* The answer isn't more policies. It's operational habits, shared accountability, and process design that support security without hindering delivery.

This stage is where the concept of "embedded" moves beyond philosophy and into practice. Below are five key principles—and practical actions—that any IT or InfoSec leader can begin implementing right away. *Note: It is essential to maintain compliance with organizational security policies when implementing changes. Any violations found during or after the process should be reported in accordance with your policy.*

1. **Create Shared Ownership from the Start**

Start early. The teams designing or deploying systems should co-own the security of those systems, rather than inheriting it as an afterthought. Bring Security into the earliest planning and requirements phases, not just final reviews.

Try this:

- Add a lightweight security intake checklist to your IT request process. (see example in the *Appendix*).
- Make data sensitivity and access risk part of your intake conversation.
- Document who owns execution and who owns risk visibility. Build out your RACIs. Ensure that all documentation is visible to all stakeholders.

2. **Align Controls with Actual Behavior**

The fastest way to kill security culture is to enforce controls that don't reflect how people actually work. Instead, spend time aligning policies and control requirements with the existing systems and habits. This builds confidence and trust.

Try this:

- Sit down with system owners and walk through “how it really works.”
- Identify where existing practices already mitigate risk.
- Tune policy language to reflect reality, not *just* framework phrasing.

3. Automate the Pain Points

Friction is the enemy of adoption. If a control is manual and tedious, users will work around it, even if they agree with the intent. Look for automation opportunities that eliminate bottlenecks and help teams do the right thing by default.

Try this:

- Auto-generate logs or access approvals from ticket systems.
- Embed SAST/DAST tools into CI/CD pipelines for early detection.
- Use policy-as-code to enforce guardrails without creating blockers.

4. Close the Feedback Loop

Security isn’t static—it’s adaptive. And adaptation requires feedback. Whether through post-incident reviews or sprint retros, make sure security lessons are learned, not just documented. IT and Security should review these outcomes together, and adjust.

Try this:

- Include “security impact” as a question in all postmortems.
- Invite delivery teams to provide feedback on the quality of alerts and controls.
- Update threat models and detection rules based on the actual events that occurred.

5. Empower Internal Champions

You don’t need a huge team to drive culture change. Look for security-minded staff within IT who can serve as trusted voices on their teams. These champions can provide early visibility into changes and help spread secure practices from within.

Try this:

- Offer extra coaching and briefings to identified security advocates.
- Include champions in architecture reviews and tool evaluations.
- Celebrate their wins publicly—they help normalize secure thinking.

Security becomes truly embedded when it’s no longer a separate activity—it’s simply part of how things get done. The more your teams internalize these practices, the less effort it takes to stay resilient.

📈 ***Leadership Prompt****:* Choose one of these five areas and pilot it in a current project. Document the before/after experience. Use that story to gain broader buy-in for embedding practices across teams.

Measuring and Sustaining Embedded Maturity

Building embedded security is a milestone, not a finish line. Without measurement and reinforcement, practices can drift into routine checkboxes or misalign with business goals. Mature organizations regularly validate controls' presence, real-world function, adoption, and resilience.

Effective measurement doesn't require perfection—it requires **intentionality, honest feedback loops, and shared accountability** across IT and security. The goal isn't to police compliance, but to illuminate performance, flag weak points early, and ensure security remains a living part of the operation.

How to Measure Embedded Maturity

Use these guiding questions to assess whether your security practices are truly embedded:

- **Are teams consistently applying secure practices without external enforcement?**
- **Can our policies be traced to real behaviors, not just documents?**
- **Are exceptions logged, owned, and used as inputs for improvement, not just tolerated?**
- **Do project post-mortems include security reflection?**
- **When incidents happen, are root causes tied back to process gaps or control failures?**

These questions can form the basis of a quarterly or semi-annual review rhythm.

How to Sustain Progress

Sustainability doesn't come from heavier oversight—it comes from **process reinforcement, cultural buy-in, and visible wins**.

5 Practices to Keep Embedded Security Alive:

1. **Introduce Lightweight Control Health Checks**
   Spot-check whether controls are followed where they matter most (e.g., new system rollouts, privileged access reviews).
2. **Assign Dual Owners (IT + Security) to Key Controls**
   Joint ownership encourages alignment, shared accountability, and better

outcomes.

3. **Use Real Incidents as Teaching Moments**
   After-action reviews should focus on what went wrong **and why**—and lead to targeted improvements.
4. **Report on Positive Security Behaviors, Not Just Gaps**
   Celebrate what’s working. It reinforces culture and boosts morale.
5. **Revisit Relevance Annually**
   Business priorities shift. Controls that made sense last year may no longer align. Review and refresh.

The Maturity Loop: Embed → Measure → Adapt

The most resilient organizations treat embedded security like product development: iterative, responsive, and constantly evolving. Measurement isn’t about scorecards—it’s about staying sharp, reducing risk in motion, and building security that holds even when things go sideways.

Common Pitfalls to Avoid

Even with the best intentions, efforts to operationalize security often stumble—not because leaders don't care, but because certain habits or assumptions go unchallenged. Avoiding these pitfalls can mean the difference between a framework that fades and one that endures.

The key isn't to do more—it's to act with focus, alignment, and credibility. Below are the most common traps organizations fall into when trying to embed security into operations:

1. **Confusing Documentation with Implementation**

Policies written in isolation often fail in the field. If your policies don't match how work actually happens, they'll be ignored—or worse, weaponized against teams who can't realistically follow them.

Remedy: Involve practitioners in writing and reviewing policies. Build from what teams already do well.

2. **Overengineering Controls**

Restrictive controls often lead to friction, workarounds, and shadow IT. Security becomes the enemy, and credibility erodes.

Remedy: Choose controls that are effective and minimally disruptive. Automate enforcement when possible.

3. **Making Security a Gate Instead of a Partner**

When security enters only at the end, it's too late—and teams will find ways around it. Bolt-on security breeds resentment.

Remedy: Embed security into intake, design, and planning—not just review.

4. **Focusing on Passing Audits Instead of Building Trust**

When teams only prepare for audits, security becomes a performance. The goal shifts from safety to compliance theater.

Remedy: Treat audits as a snapshot, not the strategy. Real maturity comes from embedding, not rehearsing.

5. **Neglecting Culture and Relationships**

Even great tools and policies fail when people don’t trust each other or the process. Alignment breaks down in silence.

Remedy: Invest in shared language, open dialogue, and collaborative rhythms between IT and Security.

Final Word on Pitfalls

These missteps are part of the learning curve and not simply a sign of failure. But the sooner you recognize and correct them, the faster your teams can build something that lasts. Security isn’t about saying “no”—it’s about saying “yes, wisely.”

The Leadership Playbook

How to Champion Embedded Security in Any Organization

Security maturity doesn’t just come from better tools or stricter policies—it's built by leaders setting an example, enabling smart choices, and consistently emphasizing what truly matters. Whether you're in IT, InfoSec, or the business side, this playbook offers the posture and practices that transform good intentions into lasting maturity.

What Embedded Security Leaders Do Differently

1. Connect, Don’t Command
Great security leaders don’t lead with controls—they lead with context. They build bridges with IT, product, and business stakeholders to align incentives and priorities.

Action: *Start with their goals. Show how security helps protect and accelerate what matters to them.*

2. Shift From Gatekeeper to Design Partner
Instead of reviewing what others have built, mature leaders co-design from the start. They replace friction with guidance.

Action: *Join intake meetings. Ask design-phase questions like, “What’s the worst that could happen here?”*

3. Make Policy Reflect Practice
When policy is aspirational, it erodes trust. When it’s accurate, it drives consistency and clarity.

Action: *Review one high-friction policy per quarter with frontline users. Adjust based on how they actually work.*

4. Reinforce Culture, Not Just Compliance
Security that’s “someone else’s job” is security that fails. Mature leaders make security a team sport.

Action: *Praise secure-by-default thinking in retros and standups. Share real stories that show how security helped.*

5. Set the Rhythm, Not Just the Standard
Checklists don’t drive maturity—cadence does. Mature leaders create space for recurring conversations, not just annual reviews.

Action: *Create lightweight, recurring touchpoints between security and IT. Quarterly retros. Monthly syncs. Shared dashboards.*

Pro Tip: Lead Through Questions

When in doubt, a question is better than a mandate. Here are some to keep in your pocket:

- “How would this fail under pressure?”
- “What risk are we accepting here—and who owns it?”
- “How could we automate this in a way that helps you, not slows you down?”
- “What’s the easiest way for this control to get skipped?”

Final Word for Leaders

You don’t need to control everything. But you must influence the right things. Embedded security starts with you—not as an authority, but as a facilitator of shared trust, real accountability, and aligned action. When leaders change the conversation, teams change the culture.

Appendix A

IT Project Security Intake Checklist
(Example – 10 Questions)

Purpose: Quickly assess whether the request introduces risk and identify where early InfoSec involvement is needed.

Basic Risk Indicators

1. **Will this involve storing, processing, or transmitting customer or employee data?**
   □ Yes □ No □ Not Sure
2. **Will this system integrate with our existing infrastructure (e.g., SSO, APIs, databases)?**
   □ Yes □ No □ Not Sure
3. **Does the vendor or tool require administrative-level access or elevated permissions?**
   □ Yes □ No □ Not Sure
4. **Has a data classification been assigned for the information this system will handle?**
   □ Yes □ No □ Not Sure

Security Considerations

1. **Is encryption (in transit and at rest) supported and planned?**
   □ Yes □ No □ Not Sure
2. **Will this introduce a new vendor or third-party relationship?**
   □ Yes □ No □ Not Sure
3. **Will the implementation involve new or modified user provisioning or authentication?**
   □ Yes □ No □ Not Sure
4. **Are logging and audit trails included in the implementation plan?**
   □ Yes □ No □ Not Sure
5. **Will the system connect to the internet or be externally accessible?**
   □ Yes □ No □ Not Sure

6. **Do you believe any unusual risks or concerns exist that haven't been captured above?**
   □ Yes □ No If Yes, please describe: ______________________

Next Steps Based on Responses:

- **If 3 or more "Yes" or "Not Sure" responses:**
  ➤ *Flag for Security Review before implementation.*
- **If all "No" and data is non-sensitive:**
  ➤ *Proceed with low-risk implementation, no further review required.*

Appendix B - Embedded Security Self-Assessment Worksheet

Domain	**Reactive** (1 pt)	**Cooperative** (2 pts)	**Embedded** (3 pts)	**Your Score**
Security in Project Intake	Security not included or added late in IT requests	Basic security questions added post-hoc or via informal conversations	Intake checklist includes security questions and is built into standard IT processes	
Control Ownership	Controls created by InfoSec, rarely understood or followed by IT	Controls discussed between teams, but ownership is unclear or split	Controls are co-owned, maintained jointly, and documented clearly in shared systems	
Policy to Practice Alignment	Policies exist but do not reflect real operations	Policies mostly reflect actual practices, with gaps	Policies are written collaboratively, match day-to-day operations, and have regular review cycles	
Collaboration & Trust	Teams work in silos; security is seen as a blocker	Security invited to meetings, but often too late to influence direction	IT and Security collaborate from the start, and trust enables faster, safer decision-making	
Risk-Based Decision Making	Risk decisions are implicit or undocumented	Risk acceptance exists, but ownership and visibility are inconsistent	Risk decisions are documented, visible, and jointly owned with business, IT, and InfoSec	

5–7 points → **Reactive**: Foundational awareness needed. Consider starting with an intake checklist and ownership mapping.
8–11 points → **Cooperative**: Good traction. Focus on making practices consistent and aligning policy with operations.
12–15 points → **Embedded**: Strong alignment. Time to measure and evolve controls, and mentor other teams.

Appendix C

Meeting Objective:

To assess the health, relevance, and adoption of key security controls; identify risks and friction points; and drive actionable alignment between IT and Security.

1. **Welcome & Objectives (5 mins)**

- Brief statement of purpose
- Review of today's agenda
- Assign notetaker (if needed)

2. **Highlights & Wins Since Last Review (10 mins)**

- Major security and operational improvements
- Notable incident mitigations or audit outcomes
- Any "controls in action" success stories

3. **Control Health Check (30–40 mins)**

Use a control list or shared worksheet.

For each control:

- Owners
- Operational? (Y/N)
- Reviewed this quarter? (Y/N)
- Gaps Identified
- Action Required

Discussion prompts:

- Is this control still needed?
- Is it functioning as designed?
- Is ownership and accountability clear?
- Are users bypassing it? Why?

4. **Policy/Practice Misalignment (10 mins)**

- Are any policies outdated or ignored in practice?
- Where are teams relying on informal processes?

5. **Upcoming Projects & Risk Forecast (10 mins)**

- Identify upcoming systems, migrations, or tooling that will affect controls
- Highlight key risks or resource gaps anticipated in the next quarter

6. **Action Plan & Owners (10 mins)**

- Confirm updates to documentation
- Assign owners and deadlines for remediation or improvement tasks
- Identify controls needing escalation or budgetary review

7. **Wrap-Up & Next Steps (5 mins)**

- Set next meeting date
- Circulate notes and accountability tracker
- Confirm any leadership briefings or compliance updates needed

Optional Add-ons:

- Demo of a new control
- Micro-training (e.g., how to validate logs, audit trails, etc.)
- Guest team lead shares how they implemented a control successfully

BAD
BADGER

Information Security