Beyond the Report: Why Penetration Testing Is a GRC Responsibility

Brandon Finton, MS, CISSP, CISM
Orion Secure

What GRC Really Means

- Governance = Who decides and how
- Risk = What could go wrong and how bad it could be
- Compliance = Proving we do what we say

The Current State of Pen Testing

- Often treated as an annual, one-off exercise
- Results delivered in a technical PDF report
- Reports stored in file shares and quickly forgotten
- Narrowly viewed as a technical exercise

Why This Is a Problem (for Organizations)

- Same issues recur year after year
- Leadership often left in the dark
- Compliance checkboxes are met, but risks persist
- Disconnect between IT, security, and business teams

Why This Is a Problem (for Pen Testers)

- Reports are too technical: screenshots, CVEs, exploit details)
- Impacts are described in abstract, technical language
- Business leaders can’t act on jargon-heavy findings
- Findings often get **ignored or minimized** because they don’t connect to business risk

What’s Really Going On

- Technical findings are symptoms
- Governance is the root cause
- Without translation, both sides fail

This is why we need to integrate GRC

Two Case Studies

- Let’s consider the *technical* problem
- And then try to map that to a governance gap

Hint: “governance” usually means “process” or “communications”

Case Study: Healthcare

Finding: Reused, easy to guess passwords

Technical issue: Poor password policy

Governance issue: No validation of policy, possible change control gaps (default passwords), lack of proper risk management to tie to risks (patient safety, etc.)

Case Study: Software Vendor

Finding: Predictable codes, SQL injection, no tenant isolation, customer reported issues, “whack-a-mole” issues

Technical issue: Lack of secure coding practices

Governance issues: Leadership is either not informed, or engaged in business compromising issues

What’s Really Going On

- Technical issues are often symptoms
- Governance failures are the root cause
- Fixing only the symptom means the problem returns

Closing the Loop

- Broken cycle: Test → Report → Forgotten
- Improved cycle: Test → Risk Register → Owner → Reporting → Review
- Keeps findings visible and actionable

Roles and Responsibilities

- Analysts/Engineers: Identify, remediate, provide context
- Managers/Security Leads: Translate findings into risk language
- GRC/Compliance: Track, escalate, tie to frameworks
- Executives/Board: Fund, prioritize, or accept risk

Reporting That Works

- Translate technical findings into business risk language
- Example: 'SQL injection' → 'Customer records at risk'
- Metrics that matter: unresolved findings, repeat issues, trend analysis
- Simple dashboards beat buried reports

Frameworks and Structure

- Map findings to NIST CSF, ISO 27001, CIS Controls
- Adds credibility for audits and compliance
- Helps align IT operations with business risk priorities

Practical Quick Wins

- Log pen test findings in a simple risk register (Excel works great)
- Include findings in quarterly reviews or risk meetings
- Assign findings to business owners, not just IT staff
- Track repeat issues to identify governance gaps

Pitfalls to Avoid

- Treating pen tests as one-time events
- Burying reports in IT silos
- Not identifying business risks
- Reporting only to auditors instead of leadership
- Fixing symptoms instead of addressing root causes

Final Takeaways

- Pen tests aren’t just technical - they are governance tools
- Findings should drive organizational decisions, not just tickets
- No matter your role, you can help close the loop between testing and governance