TS Security Solutions: Governance, Risk, and Compliance (GRC) Portfolio

A Real world GRC strategy approach backed by policy, risk, and compliance expertise

About Terious Stephens & TS Security Solutions

Terious Stephens

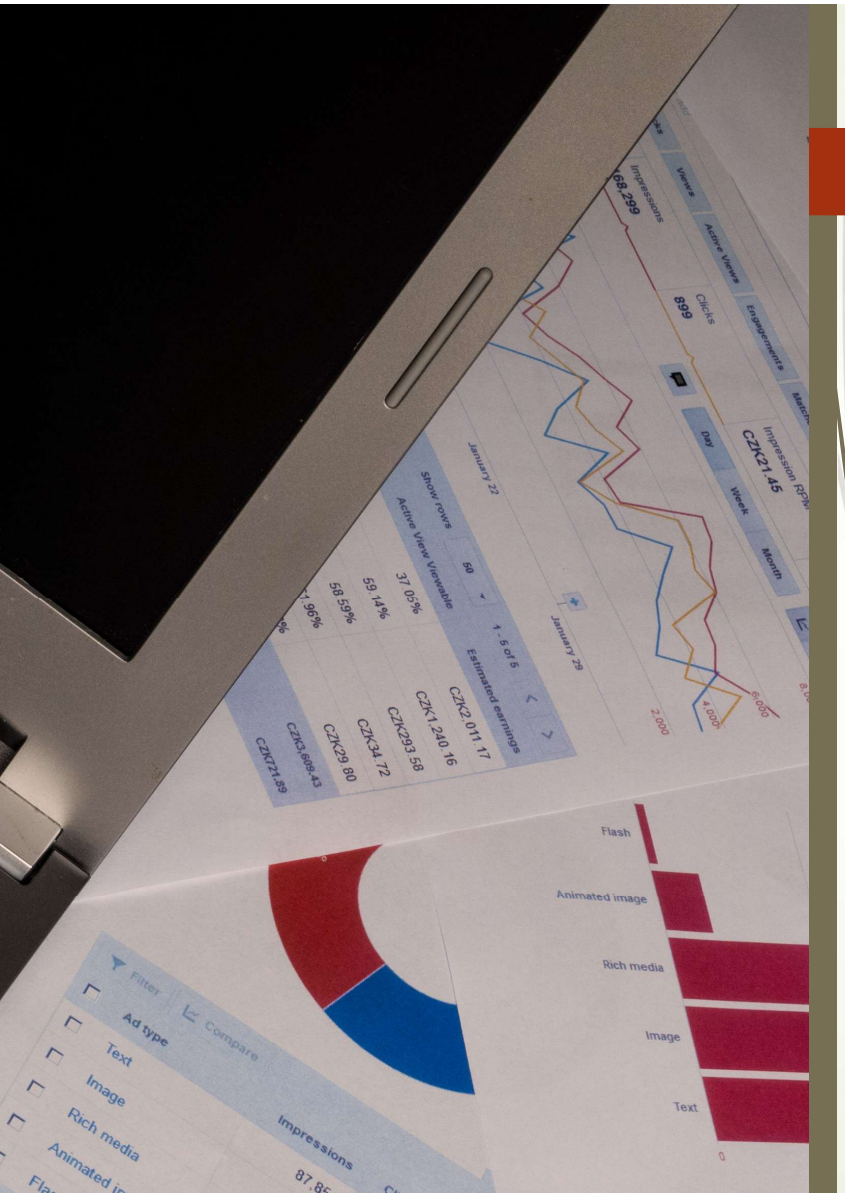
- IT Professional with 15 years of experience in IT
- Specializes in support, systems administration, data management, and information security
- Strengths: Security documentation, risk assessment, control mapping, GRC frameworks, policy creation

TS Security Solutions

- Sample cybersecurity consulting and documentation firm that specializes in creating actionable GRC strategies for small to mid-sized organizations.
- The mission of the company is to deliver scalable, compliant, and secure solutions through clear policy, risk insights, and incident preparedness.

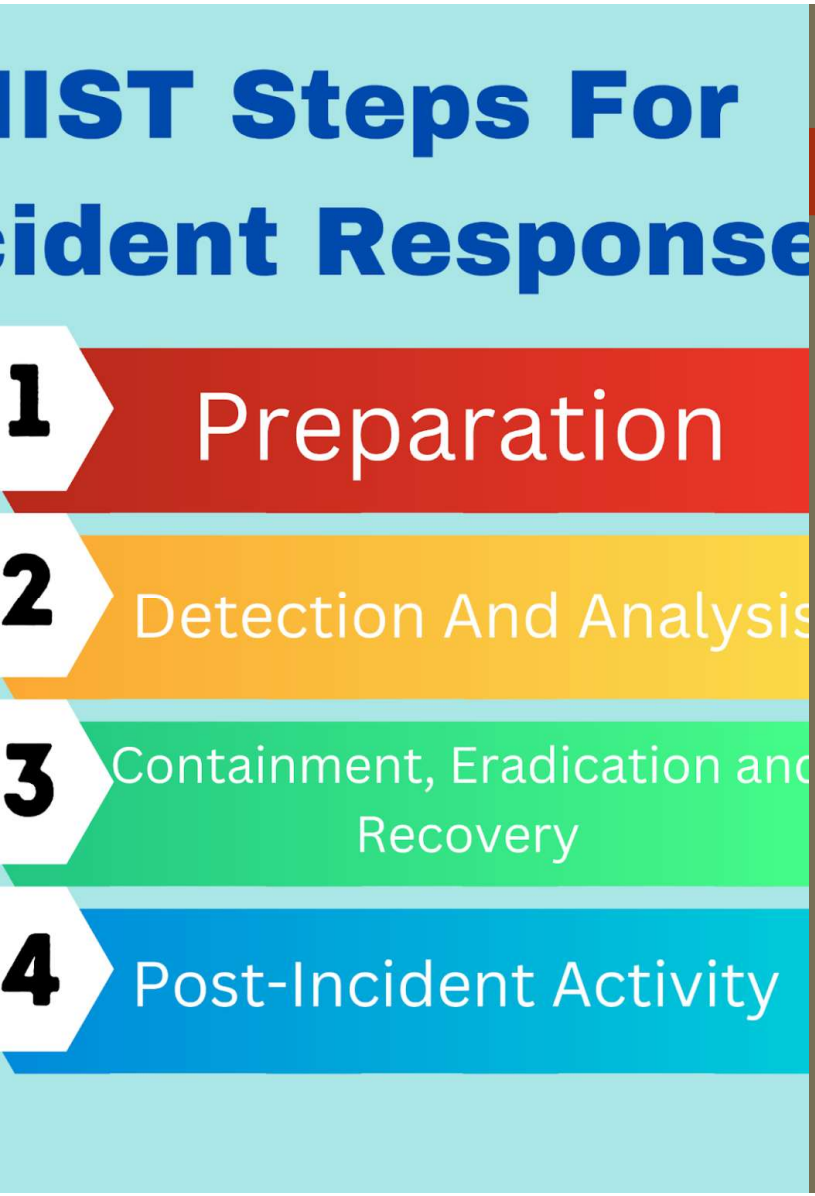
GRC Deliverables Overview

- Acceptable Use Policy – Establishes safe and responsible user behavior
- Information Classification and Management Policy – Defines data sensitivity tiers and handling
- Risk Management Policy – Outlines TS Security Solutions' approach to enterprise risk
- Risk Assessment Report – A practical evaluation of threats, vulnerabilities, and control gaps
- Incident Response Plan – Provides structure for fast, effective response to security events
- Data Retention and Disposal Policy – Aligns data lifecycle with compliance and security needs
- Risk Scenario: SecureMail Gateway Assessment (sample assessment) – A use-case applying real controls to a simulated client system



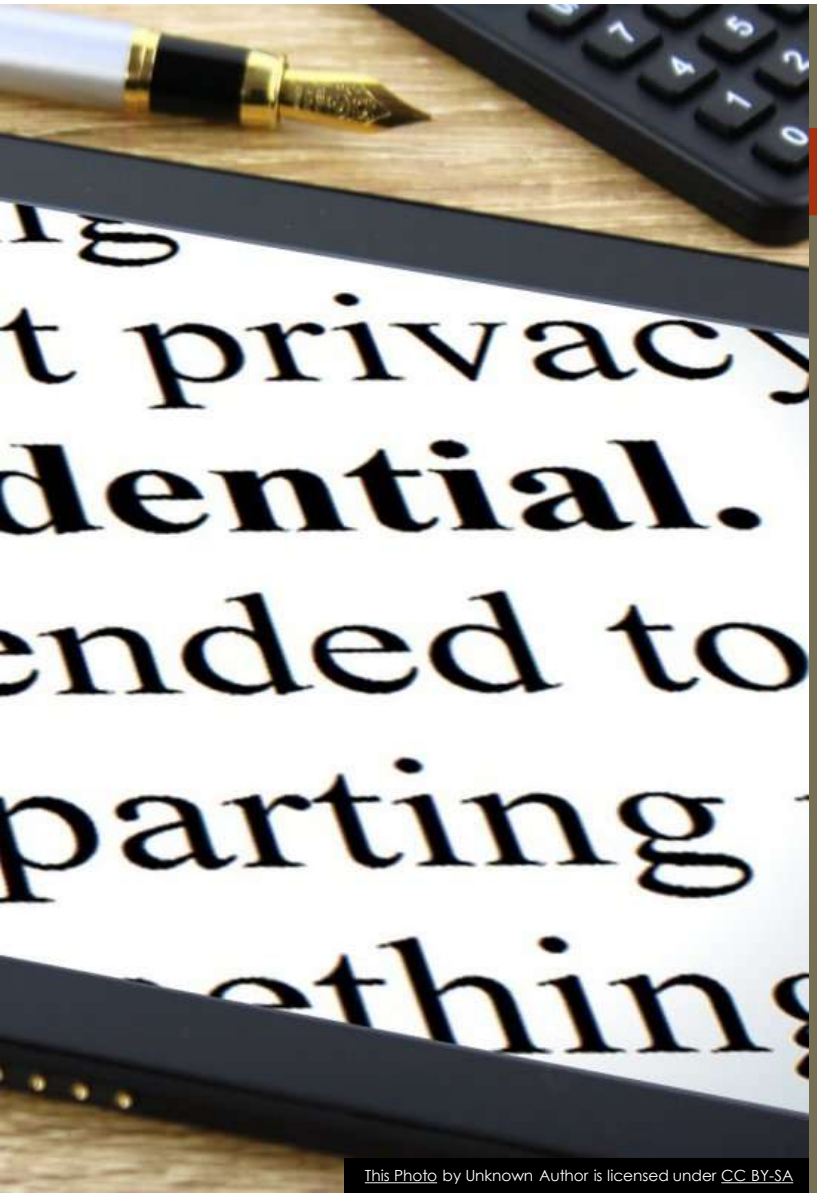
Risk Management Approach

- At TS Security Solutions, we believe risk should be both visible and actionable. Our approach begins with stakeholder interviews and ends with an updated, prioritized risk register.
- Methodology includes qualitative analysis, likelihood and impact scoring, and alignment with NIST SP 800-30 and 800-53 controls.
- Risks are not just documented, they're scored, tracked, and assigned mitigation steps.
- Deliverables include a matrix view of risks, scoring tables, and mapped NIST control IDs for every finding.



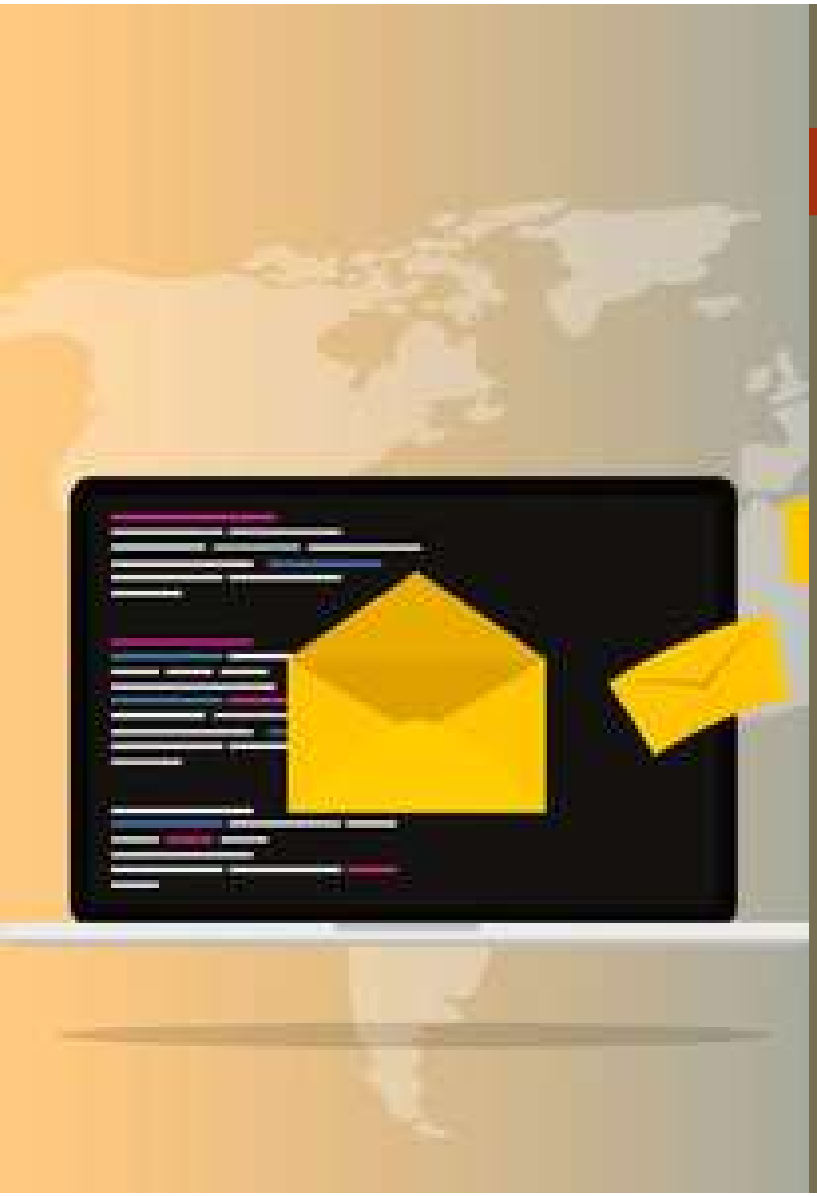
Incident Response Framework

- Cyber incidents are inevitable, and chaos is not. Our Incident Response Plan, or IRP, follows a structured, actionable lifecycle:
  - Preparation: Building playbooks and identifying roles
  - Detection and Analysis: Triage, validate, assess scope
  - Containment: Short and long-term containment actions
  - Eradication and Recovery: Clean the system, restore backups and close vulnerabilities
  - Lessons Learned: Conduct post-mortem, update documentation, train staff
- This IRP is mapped to NIST SP 800-61 Rev. 2 and written with small security teams in mind, with it being easy to scale and fast to follow.



Data Classification & Retention Policy

- Handling sensitive data starts with **labeling it properly** and ends with **disposing of it securely**.
  - Classification levels: Pubic, Internal, Confidential, and Restricted
  - Each data type is tied to specific handling rules and retention timelines
  - Retention periods were designed around regulatory requirements, namely PCI and HIPAA, and practical storage policies
  - Disposal follows NIST SP 800-88, using digital shredding or hardware destruction procedures depending on sensitivity level
- This policy ensures organizations don't just store data securely, they get rid of it correctly as well.

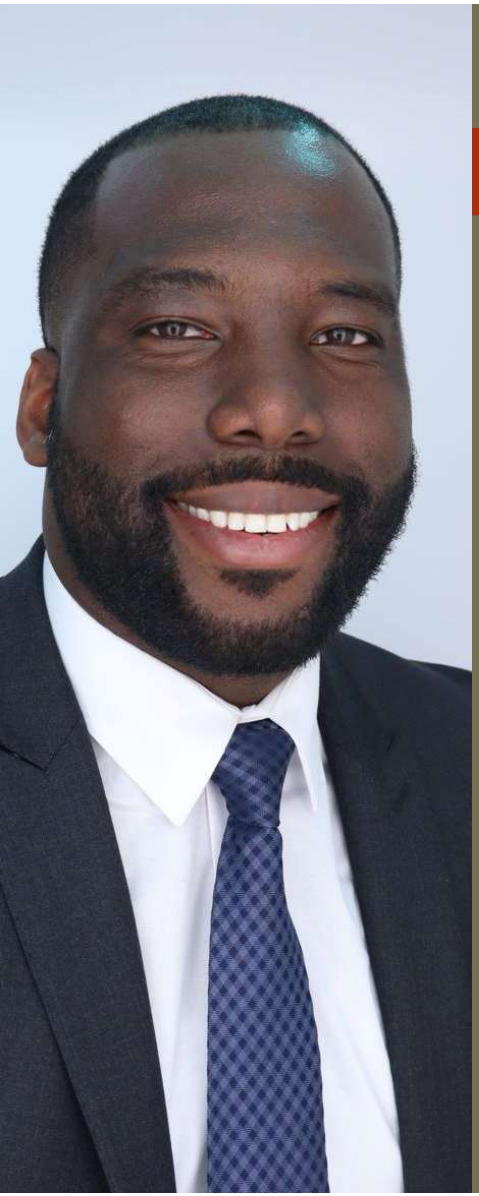


Scenario Summary – SecureMail Gateway (sample)

- The SecureMail Gateway sample assessment illustrates the methodology that TS Security Solutions uses, in action.
- Objective: Evaluate a secure email system for risks related to encryption, access control, and monitoring
- Findings:
  - Lack of encryption at rest
  - No centralized logging or SIEM integration
  - Weak user provisioning processes
- Recommendations:
  - Enables AES-265 encryption
  - Centralize logs and alerting
  - Apply role-based access controls and conduct periodic reviews
- Outcome: Risks categorized, mitigation prioritized, and controls mapped to NIST (AC-2, AU-6, SC-12)
- This write-up helps bridge the gap between theory and the day-to day reality of GRC consulting.

Compliance & Framework Mapping

Document/Policy	NIST 800-53	ISO 27001	HIPAA Compliant	PCI DSS
Acceptable Use Policy	AC-1, PL-4	A.6, A.7	✅	Req 12
Information Classification Policy	MP-5, SC-12	A.8	✅	Req 3
Risk Management Policy & Report	RA-1 to RA-5	A.15	✅	Req 12
Incident Response Plan	IR-1 to IR-8	A.16	✅	Req 12
Data Retention & Disposal Policy	MP-6, SI-12	A.11	✅	Req 9
Risk Scenario (SecureMail)	Control Mapped	A.17	✅	✅



What Makes Me a Candidate?

I bring more than just years of IT experience. I bring heart, perspective, and a grounded understanding of how governance, risk, compliance, and information systems come together to protect what matters most. Throughout my career, I've seen firsthand how the right controls and the right mindset can make or break an organization's future.

This work isn't just technical to me, it's very personal. I treat every company's data, name, and people like they were my own. That means building frameworks that are usable, reliable, and accountable. Whether I'm crafting a policy or evaluating a system, I aim to bring clarity, calm, and confidence to every GRC initiative I touch.

Protecting people and businesses through better information systems is the mission I show up for every day.

My Contact Info

Email: teriousstephens@gmail.com

LinkedIn: https://www.linkedin.com/in/terious

Phone: 404.819.4385

GitHub: https://github.com/tstep689