Best Practices to Simplify Your Information Security and Compliance Program

Presenter: Brent Hobby, GRC Subject Matter Specialist

Carolina Technology Conference
October 1st, 2014

tracesecurity

GRC Simplified... Finally.

Agenda

tracesecurity
GRC Simplified... Finally.

- **Today's webinar will explore:**
  - What it really means to be compliant
  - Why compliance management continues to burden organizations
  - How organizations can best streamline and simplify internal operations to address them
  - What role a continuous internal risk management process plays within an organization's holistic information security and compliance program

tracesecurity
GRC Simplified... Finally.

Adhering to all relevant laws, rules, policies, and contracts

- **The bar has been raised**
  - Regulations and customer expectations have increased the focus on compliance and risk management within organizations
  - Companies are expected to commit to risk management solutions and to create an ethical culture of compliance and risk management
- **It's not easy**
  - Many organizations rely on point solutions and manual processes
  - The higher bar is a significant management challenge
  - There's no easy way to direct appropriate resources to implement a long-term operational risk management program
- **There's no finish line. You are never done. You can never rest.**

Compliance Management Hurdles

tracesecurity
GRC Simplified... Finally.

- **Culture & Business Climate**
  - Management and Organization
  - Ways differ across the country and world
- **Regulation**
  - The pace and volume of regulatory change is accelerating
  - Regulations can differ dramatically geographically
- **Technology**
  - Much of "security" is good IT management
  - Constant stream of new products
- **Information & Solution Overload**
  - Whitepapers, guidance, solution leap-frogging
  - Record keeping (evidence)

Compliance is Not Security

tracesecurity
GRC Simplified... Finally.

Why Compliance?

1. Identify and understand your risks and potential exposures
2. Manage risks that may impact the organization
3. Integrate into larger frameworks

Security is Constant Vigilance

- Security: the sustained ability to pay attention
- Compliance: the ability to prove you're paying attention
- Audit: a third-party ensuring that you are paying attention

The Role Risk Management Plays

tracesecurity
GRC Simplified... Finally.

- **Risks are the things that may change business conditions**
- **Risk Management is the process of identifying, assessing and monitoring those things and using this information to guide decisions and actions**

Risk Management is *Required*

- **Regulations**
  - SOX (Audit Standard 5)
  - HIPAA
  - Gramm Leach Bliley
  - FISMA/FedRAMP
  - Federal Trade Commission Rulings
- **Standards**
  - PCI DSS
  - ISO 27001/ISO 27002
  - SOC 2
  - CobiT
  - NIST Special Publications

tracesecurity
GRC Simplified... Finally.

Compliance is a Journey, Not a Destination

- **Understand the business goals and have a roadmap**
- **Have policies and programs**
- **Establish a risk management loop**
  - Conduct a compliance-informed risk assessment
  - Put remediation plans in place to address risks
  - Remediate and report
  - Use the intelligence!
- **Repeat the risk management loop (forever)**
- **Audit**

Best Practices

tracesecurity
GRC Simplified... Finally.

- **A compliance informed risk assessment is one based on standards and guidance appropriate for your organization**
  - PCI DSS
  - ISO 27001/ISO 27002
  - CobiT
  - NIST Special Publications
  - FISMA
  - FFIEC
  - GLBA

What You Need

tracesecurity
GRC Simplified... Finally.

- Leadership buy-in
- A consolidated set of regulatory, standard, and contractual requirements
- Written policies and procedures
- The ability to train everyone
- Associated controls to inform IT operations
- An efficient process to self-assess, record findings and manage remediation efforts
- A process to maintain compliance after remediation (continuous monitoring)
- Reporting capabilities for everything above
- A method to feed gathered intelligence into the decision making process

What's Next?

tracesecurity
GRC Simplified... Finally.

- **Don't wait for the previous list to be complete. It never will be. Start anyway.**
- **Keep your goals and the big picture in view and in perspective.**
- **Spread the word. Educate everyone and keep at it!**
- **Deal with what you find, when you find it.**
- **Things happen, but they too shall pass.**
- **Never get caught twice.**

Where Can I Get Help?

tracesecurity
GRC Simplified... Finally.

- **There are tools and providers to help, but keep it simple.**
- **IT Governance, Risk and Compliance (GRC) tools can help by providing:**
  - Standardized assessment framework
  - Consolidated view of requirements
  - Consolidated view of the controls linked to those requirements
  - Centralized repository for documentation and evidence
  - A way to regularly generate reports

Key Takeaways

tracesecurity
GRC Simplified... Finally.

- Keep it simple
- Have policies and programs
- Compliance standards help you assess the risk to your data
- Security protects the data
- A lot of security is really IT management
- Compliance measures the effectiveness of your security program
- Audit confirms compliance (Audit is your friend)
- Data protection is a never ending journey
- Things will change.

Questions?

tracesecurity
GRC Simplified... Finally.

traceCSO
your Cloud Security Officer

The power over information security and compliance is yours.

Learn more and request a TraceCSO Demo.
info@tracesecurity.com

Thank You

tracesecurity

GRC Simplified... Finally.

www.tracesecurity.com