From Scavenger Hunt to Competitive Advantage

Tennelle Anderson, CISSP, CISA, CPA
Secure Digital Solutions
Presentation Overview

• Role of Third Party “Audits”
• “Audits” are Here to Stay!
• Keys to a Successful “Audit”
• 5 Recommendations to Achieve Competitive Advantage
• Conclusion
Role of Third Party Audits

Tweet along: #Sec360 www.Secure360.org
Role of Third Party Audits

Service Providers
Generate critical revenue streams

- Client/Customer audits
- SOC 1, 2, 3
- HiTRUST
- PCI QSA
- Safe Harbor/Privacy Shield

Regulated industries
Stay in Business

- OCC
- Federal Reserve
- State banking examiners
- State Depts. of Insurance
- OCR
- CIP
Audits are here to stay!

• Explicit compliance requirements for oversight of third parties
• Third parties have proven to be easier targets
• Increased legal liability for “upstream” organizations
• Costs of breaches are rising
Keys to a Successful “Audit”

• Meet the Deadline
• Give “Quality” Responses
• Be Flexible
5 Keys to Competitive Advantage

• Make it Business-as-Usual
• Get Organized
• Make it Repeatable…and Fast
• Provide “Quality” Information
• Demonstrate Effectiveness - Make it Measureable
Make it “Business-as-Usual”

• Assign responsibility to a designated group of individuals
• Have a mechanism to “funnel” all requests to that group
• Provide education to frequently impacted groups
Get Organized

• Know your Subject Matter Experts
• Become familiar with your company’s intranet
• Gain access to IT’s departmental procedures

Tweet along: #Sec360 www.Secure360.org
Make it Repeatable…and Fast

• Consider a third-party report on controls or shared assessment
• Organize and store the information you gather
• Identify “Good Names to Know”
• Determine the most effective (and secure) way to share documentation
Make it Repeatable…and Fast

• Consider a third-party report on controls or shared assessment
• Organize and store the information you gather
• Identify “Good Names to Know”
• Determine the most effective (and secure) way to share documentation
Make it Repeatable…and Fast

• Consider a third-party report on controls or shared assessment
• Organize and store the information you gather
• **Identify “Good Names to Know”**
• Determine the most effective (and secure) way to share documentation

Tweet along: #Sec360 www.Secure360.org
Make it Repeatable…and Fast

• Consider a third-party report on controls or shared assessment
• Organize and store the information you gather
• Identify “Good Names to Know”
• **Determine the most effective (and secure) way to share documentation**
Provide “Quality” Information

• Yes/No answers are likely unacceptable
• “No” vs. “No, but…”
• Less is Usually More
• Describing Policies vs. Practices
• Follow-ups
• Responding to Findings
Provide “Quality” Information

- Yes/No answers are likely unacceptable
- “No” vs. “No, but…”
- Less is Usually More
- Describing Policies vs. Practices
- Follow-ups
- Responding to Findings
Provide “Quality” Information

• Yes/No answers are likely unacceptable
• “No” vs. “No, but…”
• Less is Usually More
• Describing Policies vs. Practices
• Follow-ups
• Responding to Findings
Provide “Quality” Information

- Yes/No answers are likely unacceptable
- “No” vs. “No, but…”
- Less is Usually More
- Describing Policies vs. Practices
- Follow-ups
- Responding to Findings

Tweet along: #Sec360 www.Secure360.org
Provide “Quality” Information

• Yes/No answers are likely unacceptable
• “No” vs. “No, but…”
• Less is Usually More
• Describing Policies vs. Practices
• Follow-ups
• Responding to Findings
Provide “Quality” Information

• Yes/No answers are likely unacceptable
• “No” vs. “No, but…”
• Less is Usually More
• Describing Policies vs. Practices
• Follow-ups
• Responding to Findings
Make it Measureable

Data Examples
• Number of requests
• Average turnaround time (in business days)
• # questions in questionnaire
• # documents requested
• # on-site audit days
• # of findings opened
• # of findings closed
• Average time to close findings
• Questions typically answered “No”

What is your story?
• Need additional resources or a tool
• Need to improve security controls to meet business partner requirements

Tweet along: #Sec360 www.Secure360.org
Conclusion

Don’t rely on heroics!
Questions?

Tennelle Anderson
tanderson@trustsds.com
www.Trustsds.com
www.TrustMAPP.com

Tweet along: #Sec360