Roadblocks, Silos, and Changes Oh My!!

Leading Others Down the Yellow Brick Road

NCHIMSS - April 2016

Introductions

Chris Johnson is currently the Information Security Manager for Systems Maintenance Services (SMS), with more than 10 years of experience in the Information Security and Privacy domains. His areas of expertise include: policy, governance, training and education, GRC solutions development, and Information Security program design and management. Chris was a founding member of the Carolina's Archer user group, and serves on the Board of Advisors for eGRC.com.

Jason Smith is an IT Security and Compliance consultant at Internetwork Engineering, with several years of experience in IT, IT Security, and Compliance. He has worked in retail, government contracting, telecom, state and local government, and banking to ensure secure and compliant environments. He has also worked as an adjunct instructor teaching both IT and Security curriculum.

Addressing Healthcare's Unique IT Needs to Create Positive Results

IE's engagement framework is designed to support these key objectives and to ensure that technology projects are tightly aligned with business goals and exceed organizational thresholds for project adoption.

By helping clients move quickly from ideas to execution, IE can accelerate time-to-market and help to create competitive advantage by quickly realizing project benefits. To help businesses and organizations outperform their peers, IE offers a complete lifecycle approach focused on three primary objectives.

- **Revenue Growth**
- **Risk Reduction**
- **Cost Containment**

A QUICK HISTORY ON SMS

WHO WE ARE

Systems Maintenance Services (SMS) offers an adaptive suite of IT hardware support services developed to meet the unique requirements of an organization's evolving infrastructure.

The SMS service portfolio includes a wide range of cost-effective offerings such as break/fix, maintenance, remote hands, datacenter migrations, IT asset deployments and disposition.

These services are provided worldwide via a network of SMS-owned and affiliate service centers located near most major cities in North America, Asia and Europe. Founded in 1981, SMS is one of the world's foremost global providers of multi-vendor IT service solutions.

Overview

- Following the Yellow Brick Road to Build Your Information Security Program

- 7 Steps to Implementing an effective Information Security Program

- Top 5 Lessons Learned

Just Follow the Yellow Brick Road?

If only Information Security
were that easy!!!

The Top 5 Similarities Between an Information Security Program and the Wizard of Oz

#5: The yellow brick road is not all it's cracked up to be

#4: Sometimes, you will wish someone would drop a house on you

#3: In order to succeed, you will need brains, courage, and heart

#2: It takes a team, and is never a one person effort

#1: You already have what it takes to succeed

States of Disarray

Typically an Information Security Program (ISP) is in one of the following four states:

"The Fresh Start"

"The Fixer Upper"

"The Dream Home"

"The Haunted House"

“The Fresh Start”

As the name suggests, the Information Security Program is developed by building with a clean slate. Often times, this means that the program is new to the organization.

Key Points:

- Other than “The Dream Home”, this is the best place to begin when building the Information Security Program.
- Because you are starting fresh, your program can easily be tailored to fit with your organizations culture.
- When compared to “The Fixer Upper”, it may take longer to build your program, however, your program will be fresh in everyone’s mind, thus making it easier to maintain once it is up and running.

“The Fixer Upper”

Many organizations fall into this category. Programs are built, and over time they fail to maintain and correct issues that arise. While not the most optimal, there may still be a good foundation, but there needs to be adjustments along the way.

Key Points:

- The work may be tough, but you can quickly flip your program with a little elbow grease.
- This is the perfect time to re-evaluate the effectiveness of your program, and learn how to manage it appropriately.
- Learn from your past mistakes. Find the root cause of why your program has become stale or unmanageable, and ensure that the right leaders are aware of your plan to fix it.

“The Dream Home”

Everyone wants a dream home, but having a dream home is not all it’s cracked up to be. You still have to pay for it, and when things break, they may be more costly to fix. Regardless, if your program looks like a dream home, you must work diligently to keep it that way.

Key Points:

- Every organization will have a different view of what their dream home should look like. Just as in everyday life, your dream home must be realistic. Depending on the maturity and size of the company, everyone will have a different “style” and “size” to their program.

- The bells and whistles are nice, but are they really necessary?

“The Haunted House”

Haunted Houses are lots of fun to walk through, but no one wants to live there. The same goes with your Information Security Program. Sometimes the program is far to gone to be repaired, and you must tear it down, and start over.

Key Points:

- Starting from scratch may seem like the easiest thing to do, but it can be extremely risky and expensive. Much planning is required to ensure that the critical aspects of your program remain intact while you work on cleaning out the cobwebs.

- The scariest part of dealing with a haunted house, is finding the ghosts, goblins, and skeletons that have been hiding in the closets. Be prepared to deal with these swiftly and directly. You can’t sweep them under the rug, they will come back to haunt you and your checkbook!!!

What Constitutes an Effective Information Security Program?

To be effective, you must have 3 parts:

- A Solid Foundation
- Strong Supporting Pillars or Principles
- A Roof for Protection

SEVEN STEPS FOR BUILDING AN EFFECTIVE INFORMATION SECURITY PROGRAM

Step 1: Gather Executive Support

- The Leadership team sets the tone for strategic decisions. If the program is not integrated with the strategic direction of the organization, then it will never be a priority for the employees.
- Through the formation of an Information Security Oversight Committee or Council, the Leadership team should be made aware of the progress of the program, as well as be made aware of any threats, risks, or potential issues.
- The Information Security Council helps to set the strategy of the overall Information Security Program, while providing proper oversight and direction.

Step 2: Plan to Succeed

The journey of building an Information Security Program is not a simple task that requires clear and concise planning and direction.

Key Points:

- Know what the end state will look like. This doesn't mean you will know all of the details, but you should at least have goals in mind.
- Understand your stakeholders. They are the key to the success of the Information Security Program. Document their role, and their impact to the program.
- Maintain a detailed list of processes that the program will manage. These must be fully documented and reviewed periodically.
- Create a Roadmap and stick to it.

Step 3: Create an Brand for the Program

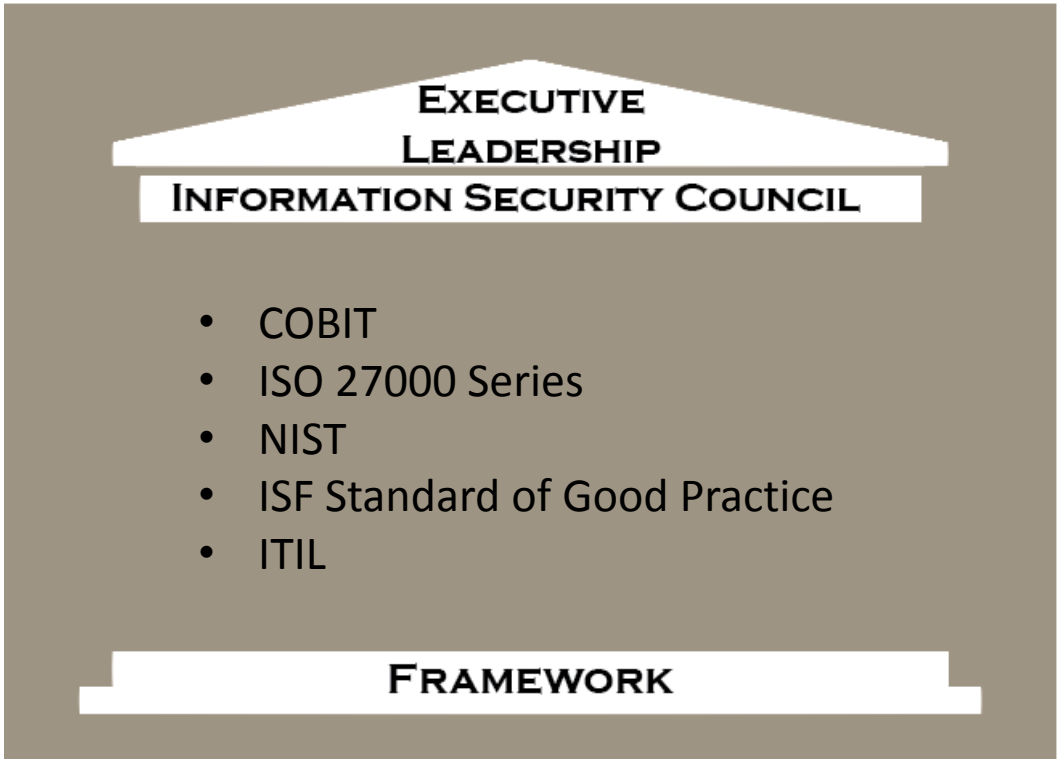
- By creating a unique Identity for the Information Security Program, your employees will learn to accept and understand the benefits and goals of the program.
- Finding ways where you can embed your messaging is crucial to the ongoing success of the program.

The SMS Information Security Branding Logo

Protecting Our Most Valued Assets

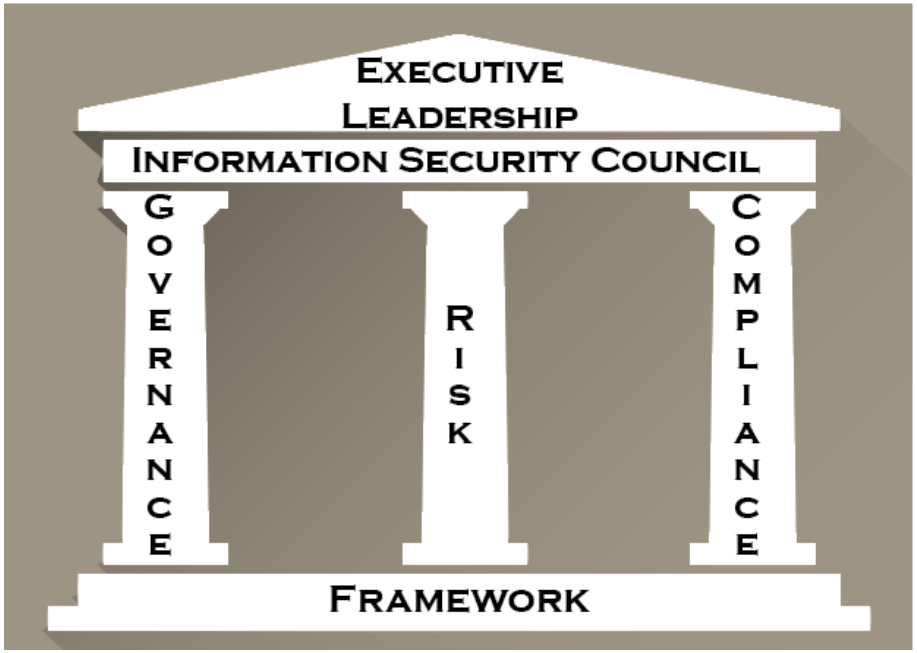
Our Staff | Our Clients | Our Company

Step 4: Form a Strong Foundation



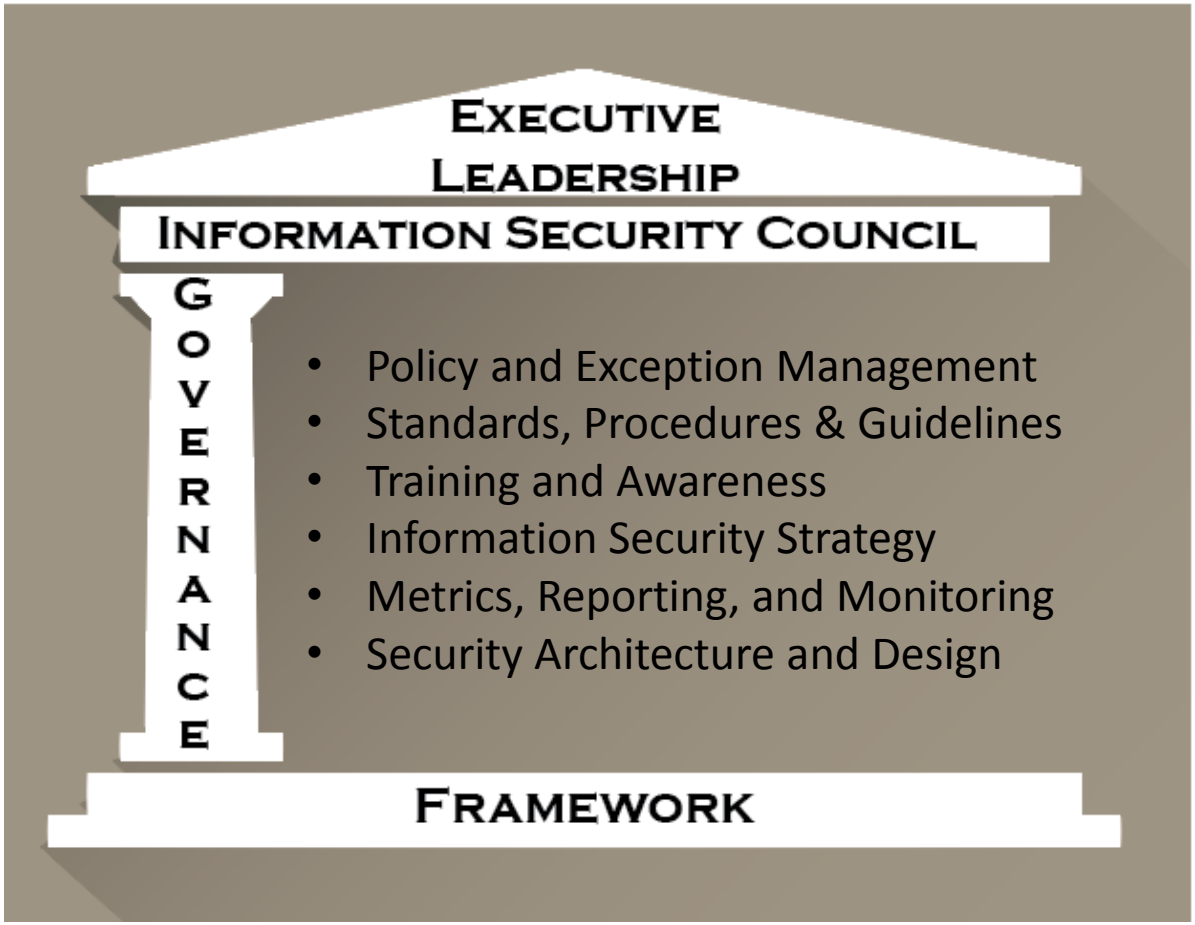
Find a successful framework that is right for your organization. There is no right or wrong answer here. Every organization will take a different path to get to the same goal.

Step 5: Build Your Supporting Principles



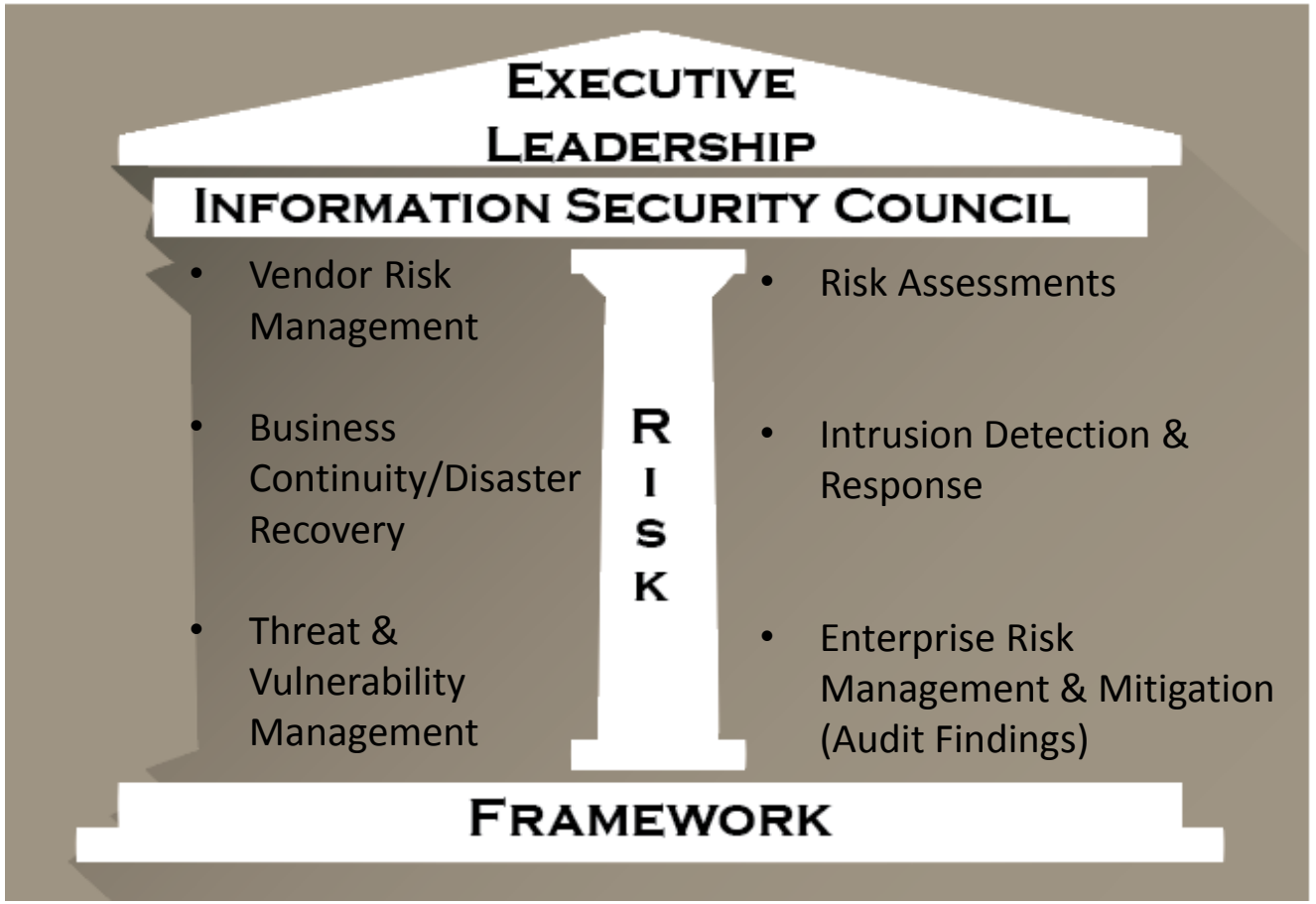
While there are many ways to create supporting principles or pillars, the easiest is to follow the Governance, Risk, and Compliance (GRC) model. This will allow you to compartmentalize your internal and external processes into specific areas for growth.

Step 5: Build Your Governance Program



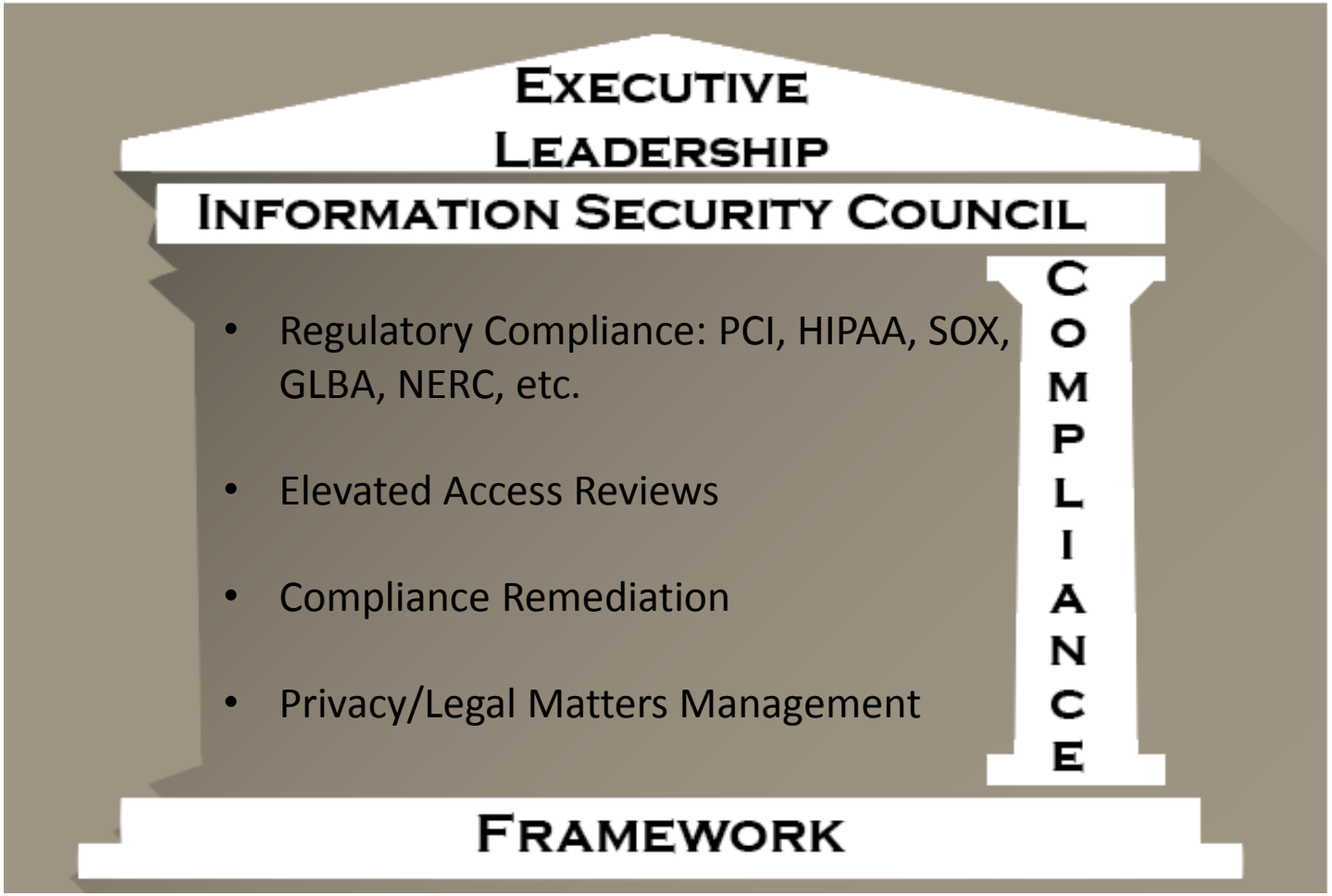
Common Governance Processes

Step 5: Build Your Risk Program



Common Risk Processes

Step 5: Build Your Compliance Program



Common Compliance Processes

Step 6: Measure, Report, and Monitor

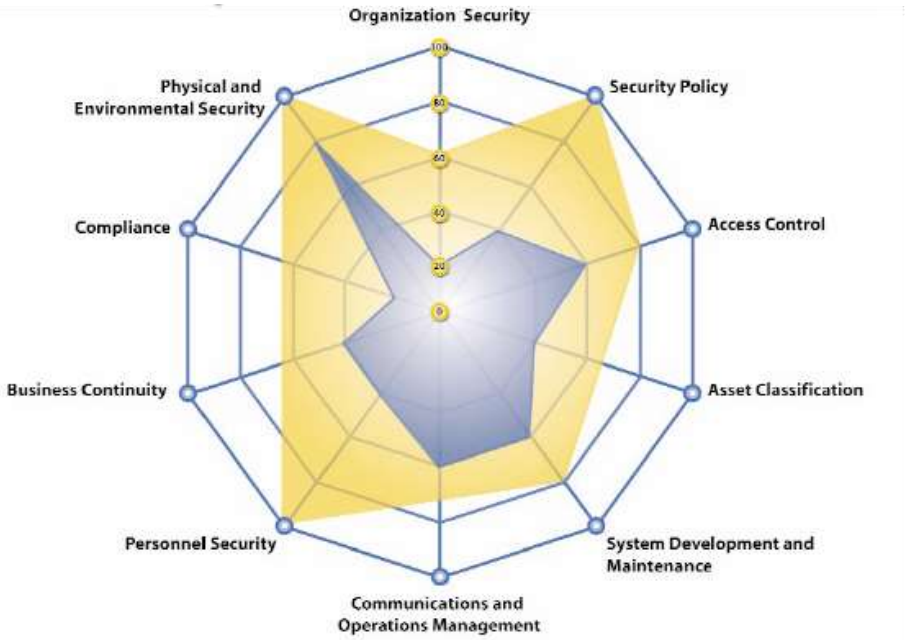
One of the most important aspects of your Information Security Program is the creation of dashboards and reports. While there are many tools available to help manage the overall program, Archer is the GRC tool shown here.

Key Points:

- Regardless of your tool of choice, find a way to do real time reporting of your overall program.

- Ensure that your reports and dashboards are clean and easy to understand. This is critical for the Leadership team, as they are providing oversight into your program, and are expecting to see.

Step 7: Adapt and Mature



There are many methods to ensuring that your Information Security Program is effective. One simple method is by using a Radar (Spider) Diagram to show each area that your program covers, and the current and expected maturity levels.

Key Points:

- Conducting an assessment early on is important, as this will create a baseline for your program.

- As the threat landscape changes, you must also adapt your program, in order to show consistent maturity.

TOP FIVE
LESSONS LEARNED

#5: You Can Lead a Horse to Water….

- Information Security is like the speed limit…it is frustrating, yet it is there for a reason.
- Getting employees onboard with the Program is one of the most challenging aspects of the entire program.
- You must understand your culture, and adjust your program so that your employees understand why it is there, and how it can benefit them.
- Mistakes will be made, therefore, anticipate the defeat, but celebrate the victories.

Whoever said that you can lead a horse to water, but you can't make him drink, must have been building an Information Security Program.

One Interwoven Message

At SMS, we have a monthly program that we promote. Each month covers a different topic, in many different types of media:

- Videos
- Games
- Blogs
- Newsletters
- “Munch and Learn” Sessions
- Prize Giveaways!!!

Games & Videos

Games

You've already lost one laptop, Agent Smith. Your job's on the line if it happens again. Make wise choices this time, and it's mission accomplished.

Compete with our contestants for a spot on the Friend Finder All-Star List. Earn your spot by showing you're savvy when it comes to making friends online.

A techie spy and his cunning crew are out to get your personal information. Stop them cold by proving you're ready to protect yourself online.

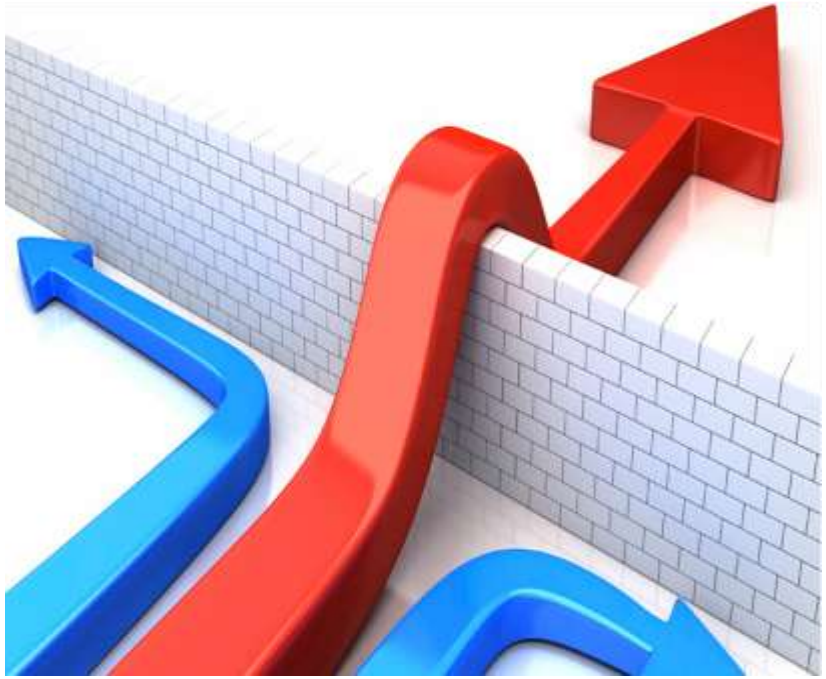
Protect your computer from spyware and viruses that can cause it to run slowly or give fraudsters access to your personal information.

Feedback Forms

5 Stars	Good content from a "fresh" and entertaining media outlet. Good job, Chris and team!
5 Stars	Good information on what the different types of threats may be and the new up and coming threats such as SMIphishing.
5 Stars	This is all great information and the video explains it quite well. I would like to add two things to help people decide what is SPAM or PHISH-ing and what is not. #1 - You never "WIN" anything that you didn't enter or apply for directly. Take that as a red flag and that should take out the majority of the e-mails you receive claiming you won or have been selected for a prize. #2 - your Bank of financial institution will NEVER ask you for account information or personal details on-line unless you're on their secure site specifically. Be safe out there everyone, and when in doubt DELETE... Don't open...

#4: Never Let Obstacles Get in Your Way

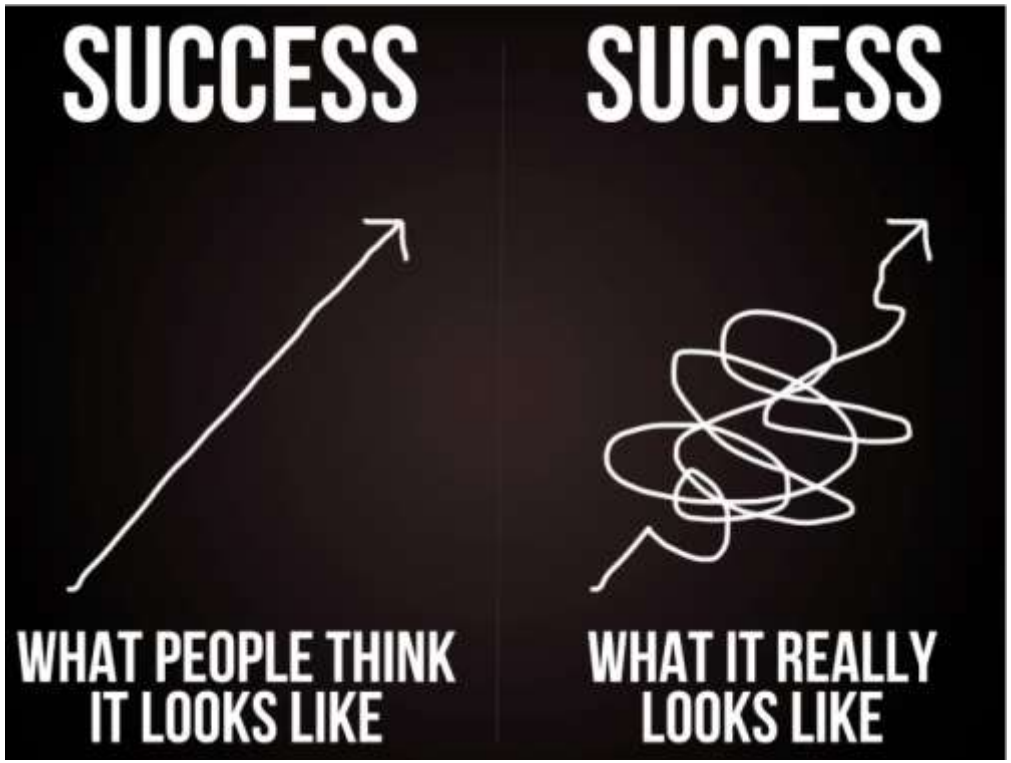
- There will always be obstacles in your way, you must be able to move past these, instead of letting them stop you.
- Always remember that Information Security is not a project, but an ever evolving Program.



You can choose to let it define you, confine you, refine you, outshine you, or you can move on and leave it behind you.

--Unknown

#3: Success is Not Easily Measured



- There will be many twists and turns along the way.
- It is never as easy as you think it will be.
- It takes dedication, passion, and endurance to build an effective Information Security Program.
- Most importantly…

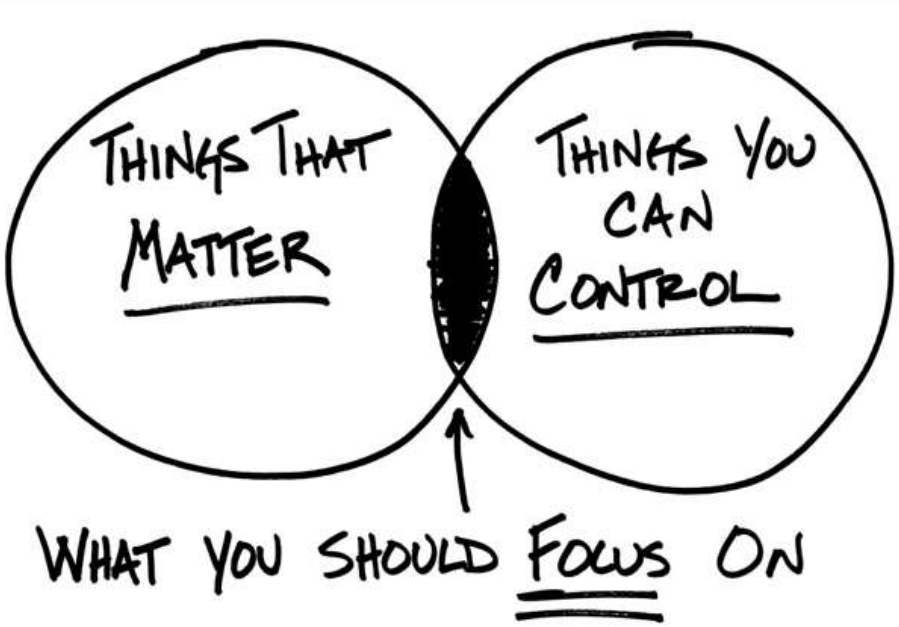
Do Not Get Discouraged!!!

Success isn't measured by what you achieve, it's measured by the obstacles you overcome.

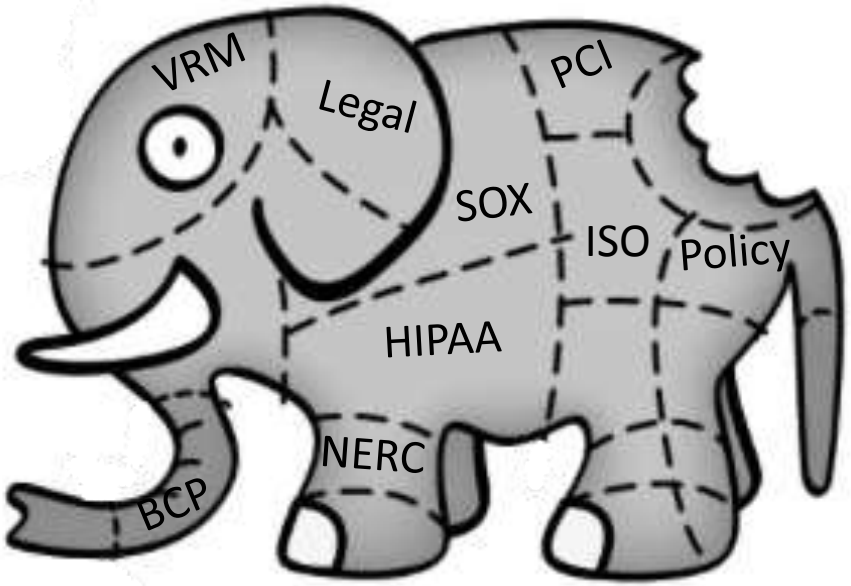
--Ethan Hawke

#2: Keep a Focused Perspective

- Regardless of what is going on around you, never lose focus for you program.
- Always look for ways to help your program grow and mature.
- Be clear in your direction, and stick to your roadmap.



#1: Don’t bite of more than you can chew



- Rome wasn’t built in a day, and neither will your Information Security Program
- It is easy to get inundated with the amount of work, however, take it slow and complete it one step at a time.
- Ensure that your program meets the needs and requirements for your organization.
- Don’t over complicate things.

Questions?

Contact Info:

Chris Johnson - cjohnson@sysmaint.com
Jason Smith - jsmith@ineteng.com