ASSURE IT
ASSESS • VALIDATE • CONSULT

Risk Assessment Primer

Preparing for and effectively participating in an information systems risk assessment

3265 GATEWAY ROAD, SUITE 650 BROOKFIELD, WI 53045 / P: 262.373.7100 / INFO@SYNERCOMM.COM / SYNERCOMM.COM

About Me

- Bill Curtis (CISSP, CISA, QSA, CCSP)
  - Husband, dad, and grandpa
  - Army Vet
  - Michigan native living in WI by way of IN, AZ and GA
  - 32+ years IT/IS
    - Army
    - Allen Bradley / Rockwell Automation
    - Bucyrus / Caterpillar
    - SynerComm

Agenda

- Risk Assessment Readiness
- Controls Environment Awareness

Let's Begin With a Premise

- You cannot manage what you do not understand.
- You cannot secure what you are not managing.
  - IT risk is no exception
- Securing an organization's systems and data requires a clear understanding of information systems value and risk both inside and outside of IT.

Step 1: Consider the Players

- Aligning IT, IS, SDO, and leadership will strengthen information systems' value and inherent information security situational awareness. An awareness I would argue is incorrectly shouldered by IT.
- Only as strong as the weakest link.

Step 1: Consider the Players

- Information Technology
- Information Security (Compliance)
- System and Data Owners (Business Unit(s))
- Leadership

Step 2: Consider your Assets

- IT risk can be demystified, simplified, and identified
- IT risk by way of information system assets
  - tangible assets
  - information assets

Step 2: Consider your Assets

- Tangible Assets:
  - Process, transmission, storage, and/or security of data
  - Possess characteristics that can (will) influence the asset's risk profile
  - Each organization must consider their own list of characteristics

Step 2: Consider your Assets

- Information Assets:
  - Identify the type of data an asset is processing, transmitting, and/or storing
  - Possess data types that can (will) influence a tangible assets risk profile
  - Each organization must consider their own list of data types

Step 2: Consider your Assets

Tangible Asset Characteristic	Information Asset Data Type
Critical for Operations	Personally Identifiable Information (PII)
Is Public Facing	Payment Card Information (PCI)
Is Vendor Managed	Protected Health Information (PHI)
Requires Authentication	Organization Financial Data
Maintains Data Protected by Regulations	Intellectual Property (IP)
Granted a Security Exception	IT Security Data

Step 3: Prepare for the Risk Calculation

- Inventory your assets
- Determine asset characteristics
- Determine asset data use
- Calculate inherent risk

Step 4: React to the Calculation

- Tag assets to extend analysis
- Consider high IR score vs. high average IR score
- Facilitate effective risk management conversations

CONTROLS

Controls Designed to Control

- Wrapped around assets, data, processes, and people
- Strengthen CIA:
  - Data strategy
  - Network segmentation
  - Log collection, monitoring, and meaningful alerting
  - Access control (least privilege, MFA, password+)
  - Sequencing back office functions (effective end user)

Controls Authority

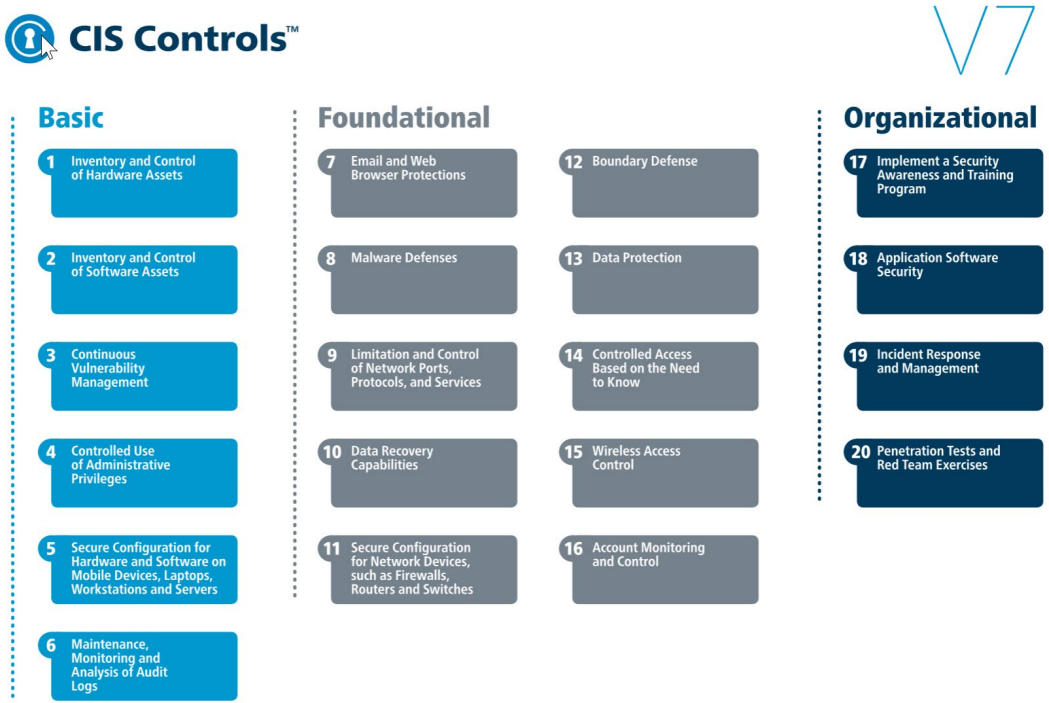
- Leadership directive
- Business adoption
- Compliance necessity
- Because it’s the right thing to do

Controls 101

- Inventory and manage your controls
- Understand your controls
  - What function is the control serving (purpose)
  - What risk is the control addressing (value)
  - Has the control been validated (tested)
  - Is the control documented (awareness)

Controls Launch

- CIS Top20



THANK YOU

(questions)