LegalSEC Update: A Security Trifecta

Thursday, August 22, 2013
10-11:30 am
Neapolitan Ballroom, I-II

#SPEC12

i/+^ 2013 the catalyst

#SPEC12

Logistics

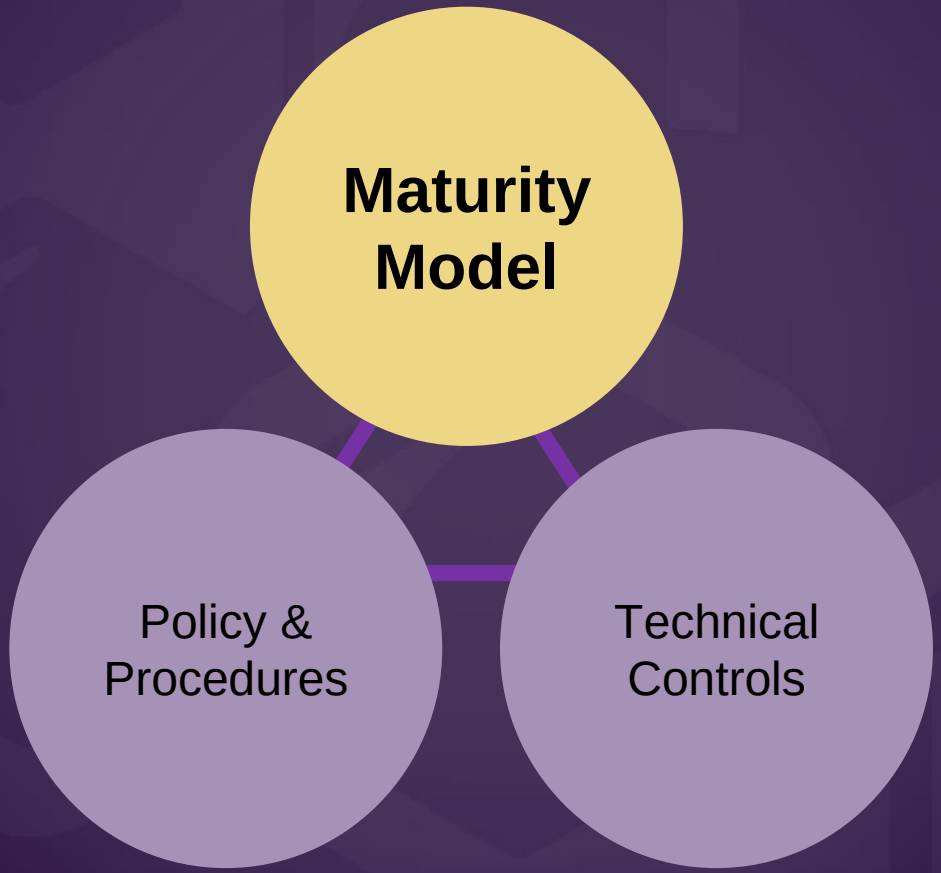
- Session Description: Just over a year ago, ILTA announced the LegalSEC™ initiative, which is dedicated to improving and enhancing information security in law firms. The three branches of LegalSEC include the Maturity Model, Policies/Procedures and Technical Controls. The team leads from each branch will share a review of accomplishments to date, the future roadmap and how you can contribute to the overall success of LegalSEC.
- Todos: Get job bank populated with LegalSEC choices

Introductions

- Bob DuBois, Board Liaison
- LegalSEC initiative
- New Board Liaison - Michelle Gossmeyer
- LegalSEC Chair - Judi Flournoy

State of the Union

- Judi Flournoy
- What we've done and where we're headed
  - Why we created it?
    - Carlos
  - LegalSEC Summit Conference, 2013
  - LegalSEC Summit Conference, 2014, going to two days, dates, location?
  - Looking forward
    - Sharing some LegalSEC content with non-ILTA members
      - ALA - Tim/Judi - ALA Conference
  - Role of the volunteer in LegalSEC
- Sections of LegalSEC:
  - Maturity Model: Tim Golden
  - Policies and Procedures: Kevin Moore



Maturity Model Update

Why a legal industry information security maturity model ?

Maturity Model - Team

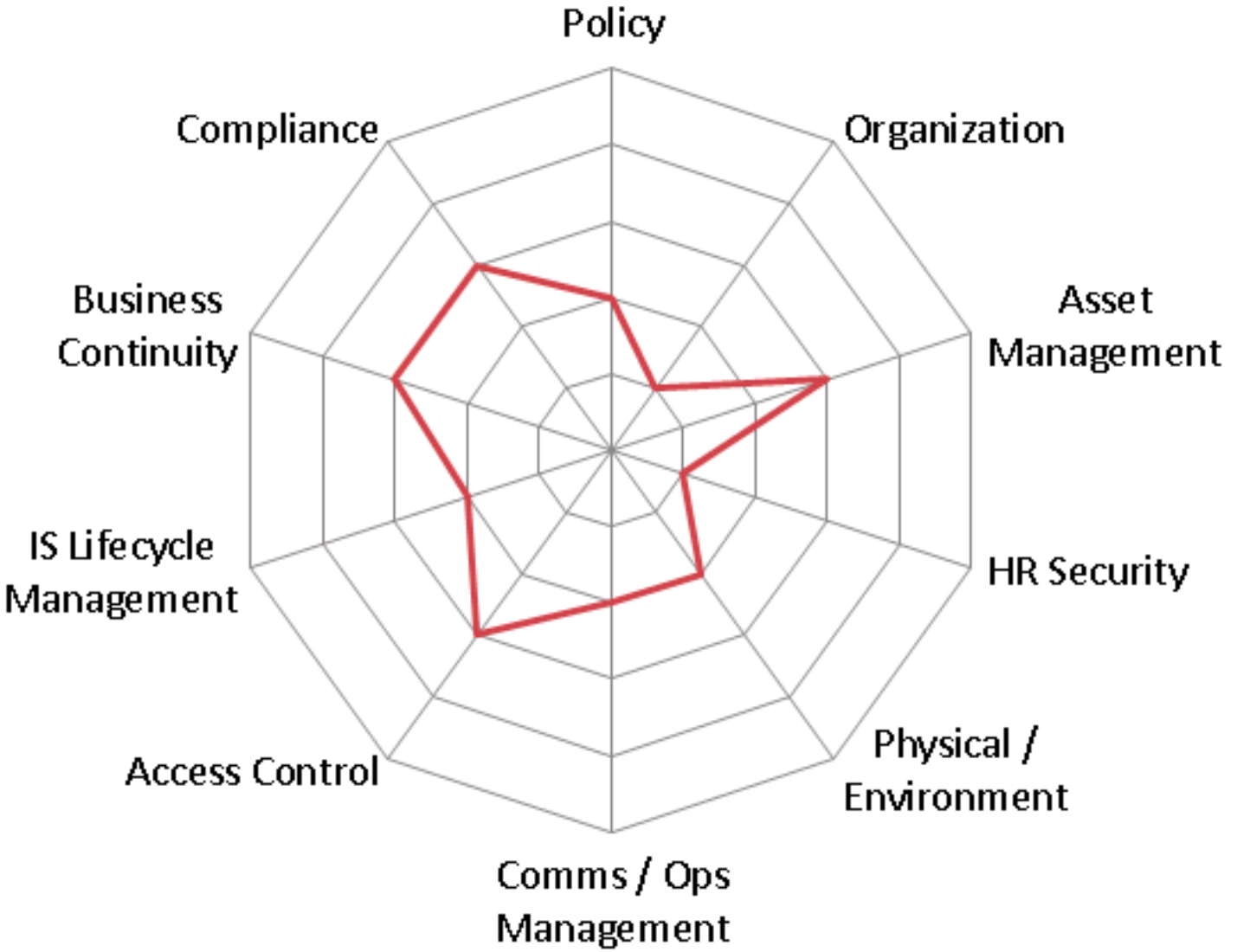
Tim Golden Mgr, EA & IT Governance	McGuireWoods LLP
Mike Santos Dir., IT Architecture & Governance	Cooley LLP
Joe Daw Information Security Manager	Jones Day
Joel Lytle Director of Information Security	Jackson Walker L.L.P.
Vern Cole Security Architect	Perkins Coie
Kenneth Lyons Sr. Mgr., IT Engineering & Security	O'Melveny & Myers LLP
Dave Ries Member	Thorp Reed & Armstrong, LLP
Jeff Hanson Mgr, Information Security	McGuireWoods LLP

Maturity Model - The Process

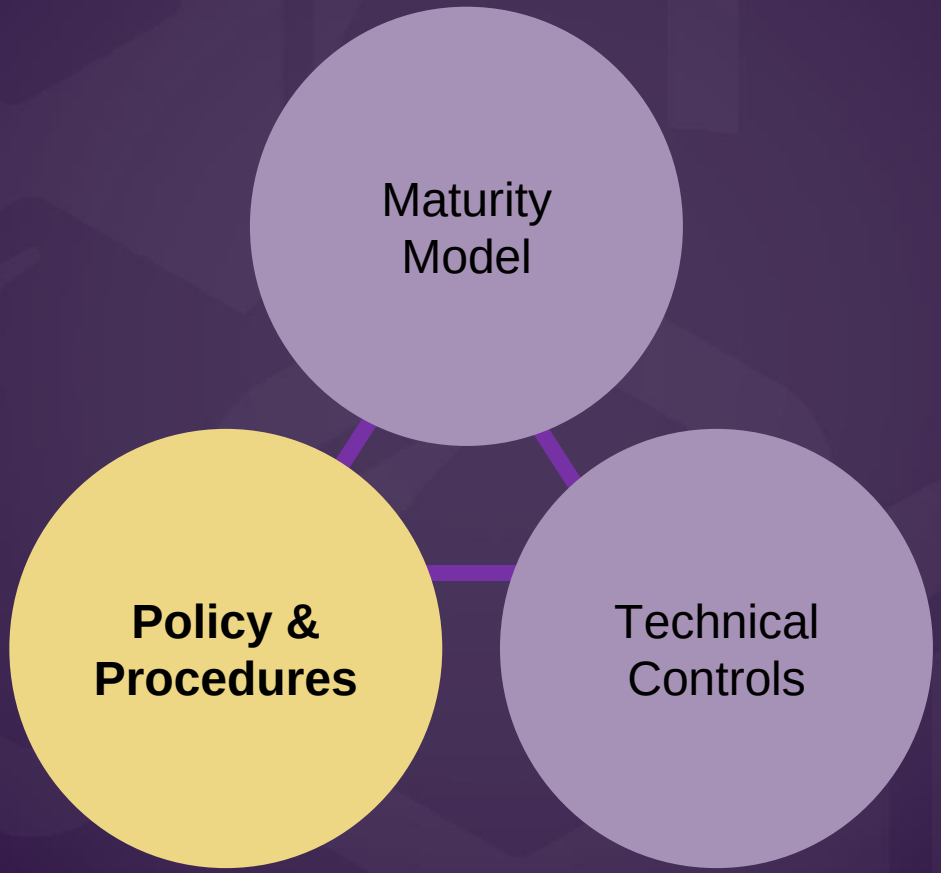
Maturity ModelQuestionnaire

Maturity ModelCapabilities

Maturity Model: Sample Results



Maturity Model - Next Steps



Policy & Procedures Update

Policies and Procedures

- Kevin Moore
  - Business Plan
  - Provide Information Security Templates for policies and procedures which incorporate security standards such as ISO 27000, NIST, PCI, etc.
    - Team members (firm size to show scope of inclusion)
    - How we approached the selection and creation of policies
    - What the purpose of the section is
    - What deliverables we currently have
    - What deliverables are coming

Policy Team

Team Members

- Sherri Vollick - IT Security Manager, Holland & Knight, 1064 atty
- Brian Clayton - CIO, Taft Stettinius & Hollister LLP, 330 atty
- Pat McCormick - ?, Fulbright, xx atty
- Robert Barker - IT Director, Baird Holm LLP, 80 atty

Policies

Initial Draft Templates - Completed

- Password Policy
- Acceptable Use
- Mobile Device
- Extranet

Template Design

Acceptable Use Policy

LegalSEC™

1.0 Overview

Acceptable Use Policy is not to impose restrictions that are contrary to <Firm Name>'s established culture of openness, trust and integrity. IT is committed to protecting <Firm Name>'s partners, associates, employees (including contractors and vendors) and the firm from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing access to <Firm Name> network services such as electronic mail, voicemail, personal file directories, computer systems, server and web browsing, are the property of <Firm Name>. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every <Firm Name> employee and affiliates who deal with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of all firm resources at <Firm Name>.
<Firm Name> expects all users to exercise common sense and good judgment before sharing or disseminating information.
<Firm Name>'s IT resources are primarily for conducting business but may be used for some limited non-business purposes.
Users may not use such resources in a way that impacts job performance, disrupts business use, subjects <Firm Name> to risks including virus attacks, compromise of network systems and services, and legal issues or potential liability or damages <Firm Name>'s reputation or clients.

3.0 Scope

This policy applies to all Employees, Non-Partner Attorneys, and Partners including contractors, consultants and temporary employee (hereafter, referred to as "employee" or "user") at <Firm Name>.
This policy applies to all equipment that is owned/leased or setup to access <Firm Name> resources.

4.0 Policy

Future Policies

Future Policy Templates

Access Control

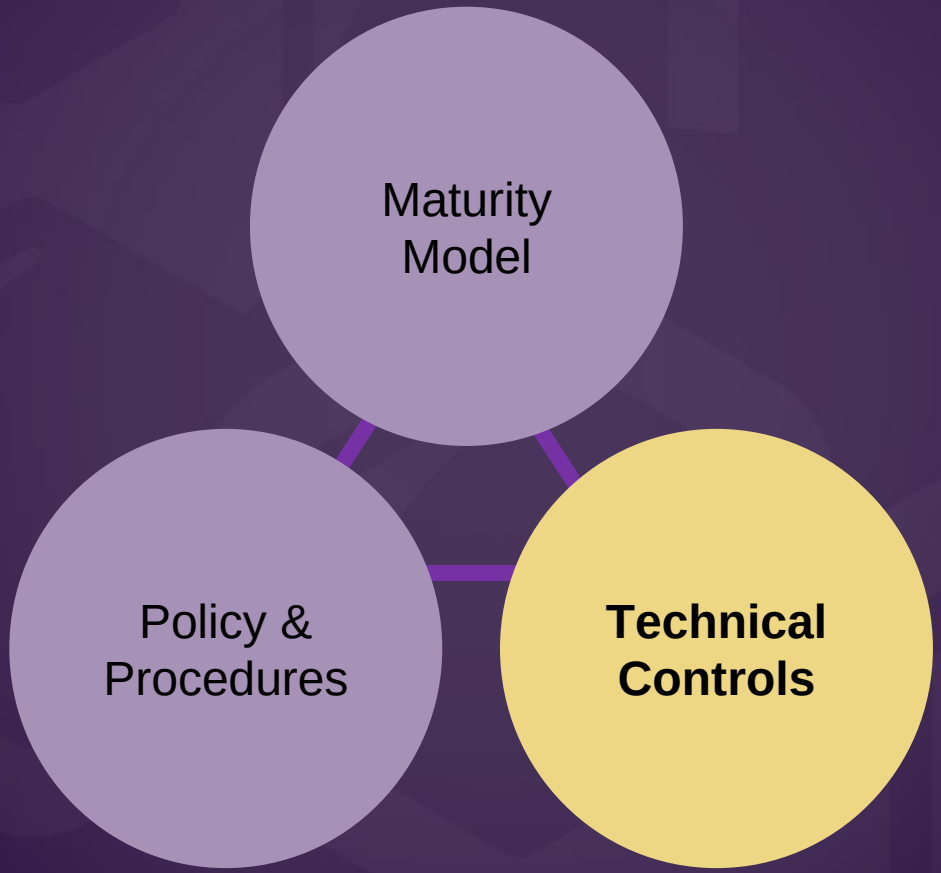
Patch Management

Traveling with Electronic Device to Foreign Countries

Social Media

Inventory of Assets

Disposal and Destruction Policy



Technical Controls Update

Technical Controls

- Jamie Herman
  - Business Plan
    - Who are the team members
    - What do we mean by control objectives?
    - Control objectives roadmap
    - How it all fits together
- Looking at the tools to implement a baseline for security
  - Patch management
  - Access control
  - Application whitelisting
  - Managed security

Technical Controls Team

Paul Kunas

- Director of IT Security - Sidley Austin - 1700+ attorneys

Jeffrey Kunz

- Senior Network Engineer - Foley & Lardner - 800 attorneys

Gregory Burwell

- IT Manager - Bulkley Richardson - 50 attorneys

Scott Ashton

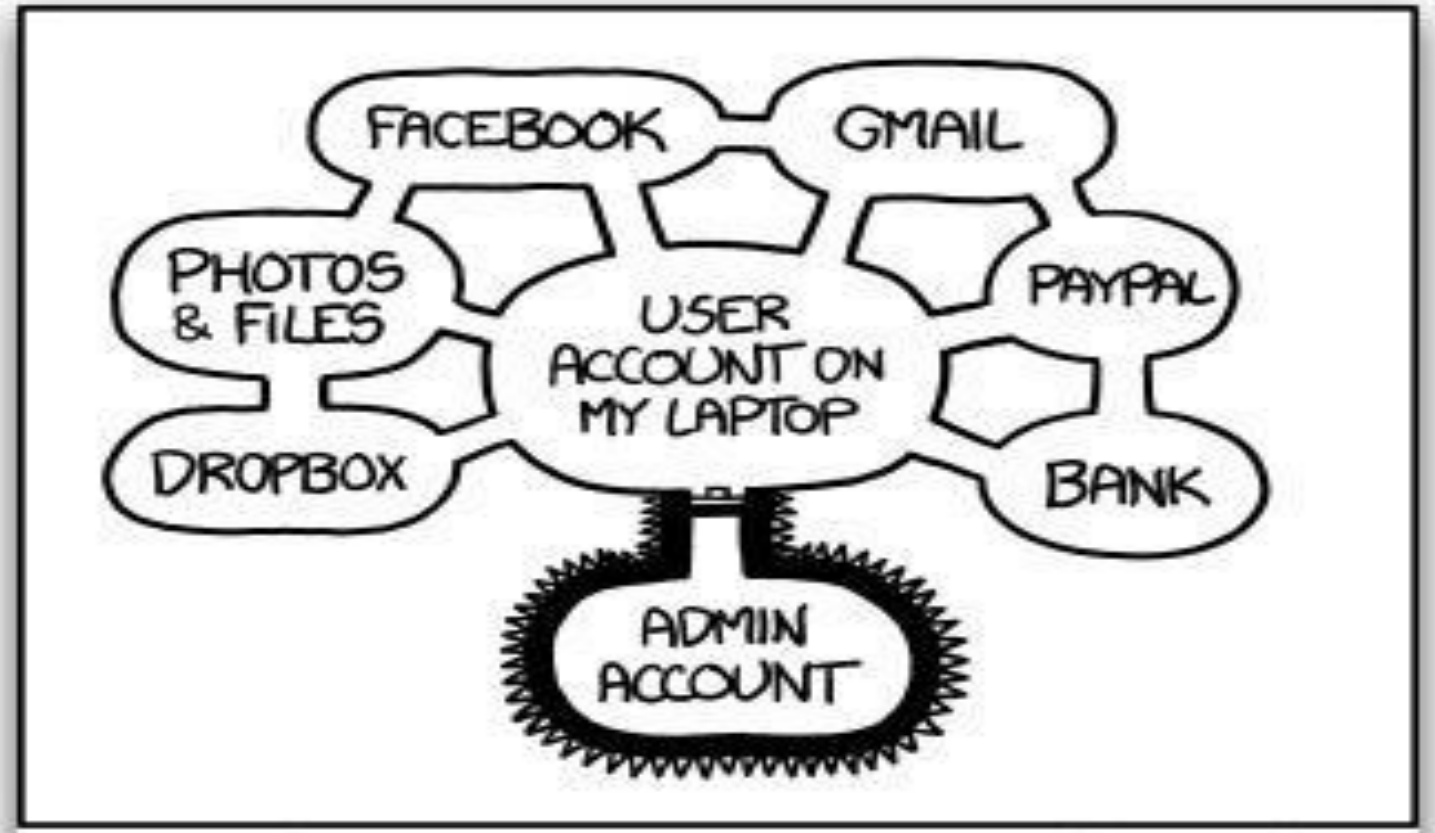
- Information Security Manager - Debevoise & Plimpton - 600 attorneys

What are control objectives?

- Not a “product”
- Establish a baseline for controls across entire firm
- Manage risk mitigation through proper communication and implementation
- Support policies with the appropriate controls; physical, operational, and technical

Control Objectives Roadmap

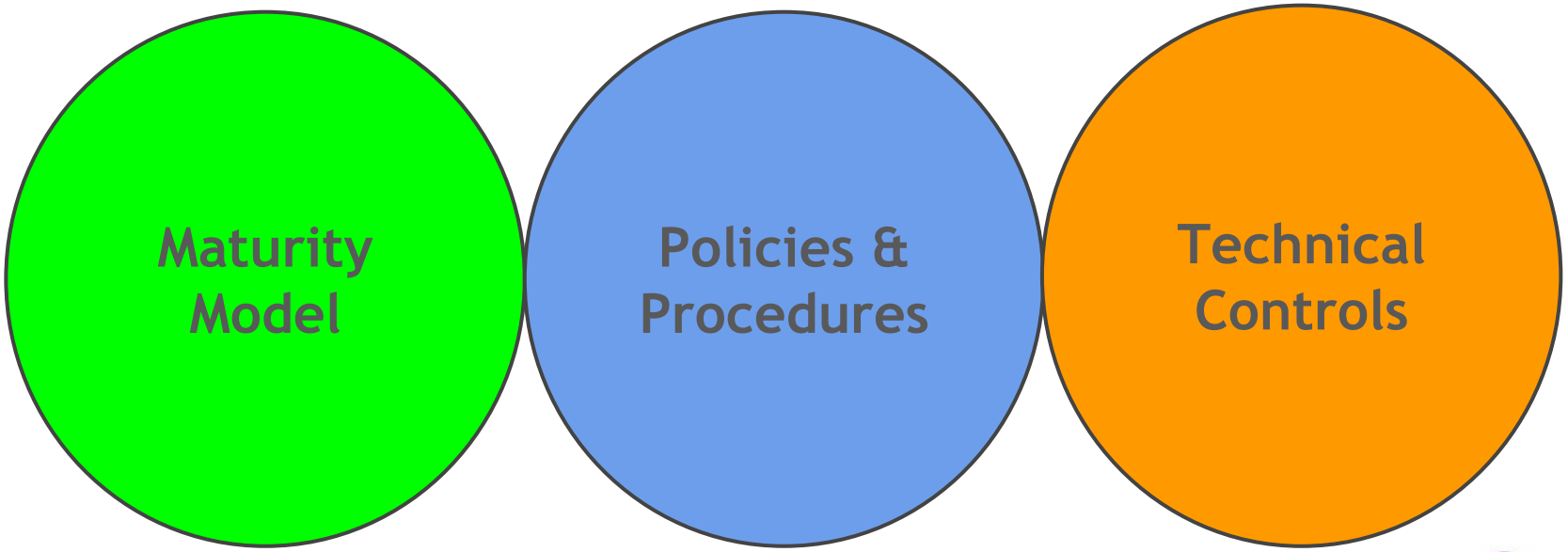
- Access Control
- Application Whitelisting
- Patch Management
- Network Access Control
- Configuration & Asset Management
- Managed Security



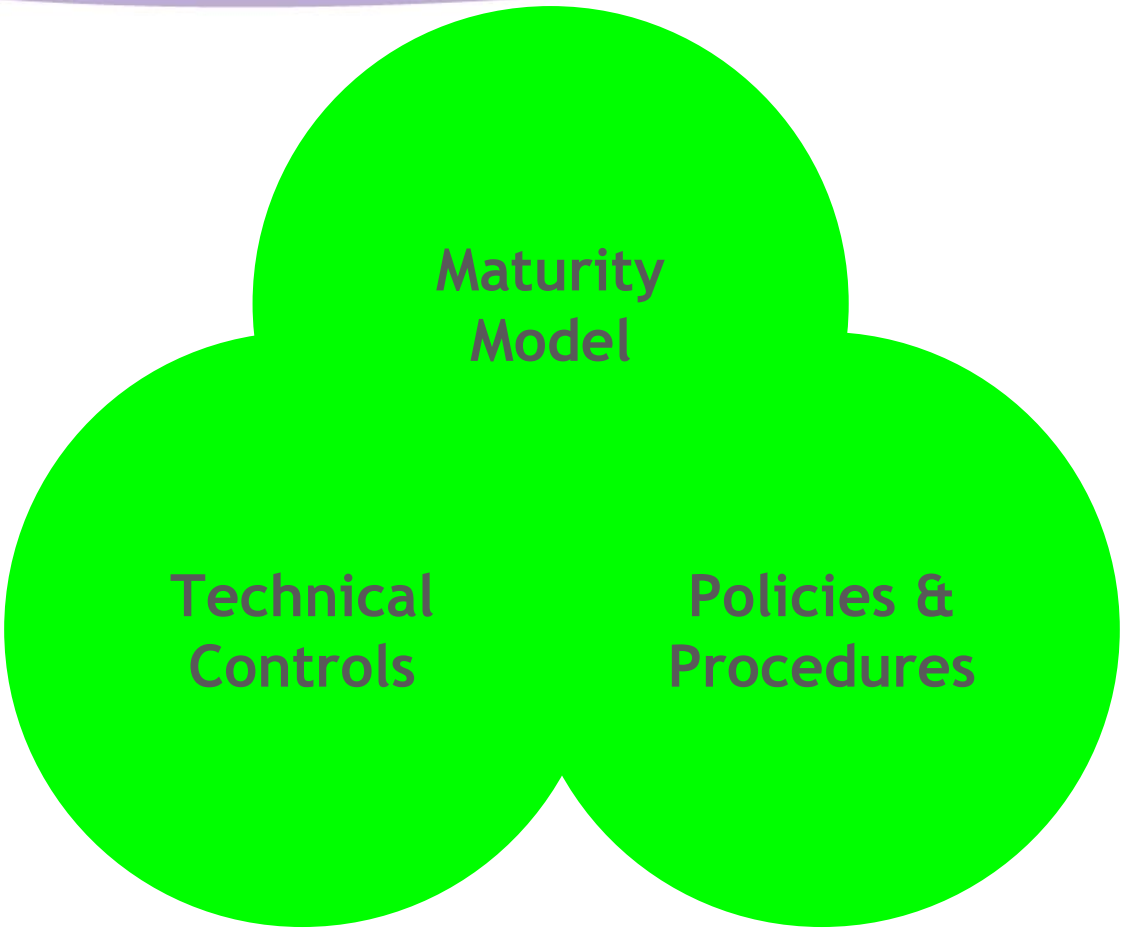
IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

Perception



Reality...Working Together



Discussion

- External influences:
  - ABA Rules
  - HIPAA Compliance Deadline
  - Client Audits
  - Requests for Documentation of Processes
- Integrating efforts with other initiatives e.g., G100
- Emerging Role of Security Manager and Staff

Volunteer Opportunies for LegalSEC

Volunteer Website: Members/Get Involved in ILTA http://www.iltanet.org/specialpages/Volunteer-Job.aspx

- LegalSEC Conference 2014 Team Members
- LegalSEC Team Members