October 6, 2015

Effective Strategies for Managing Cybersecurity Risks

Larry Hessney, CISA, PCI QSA, CIA

Everybody's Doing It !

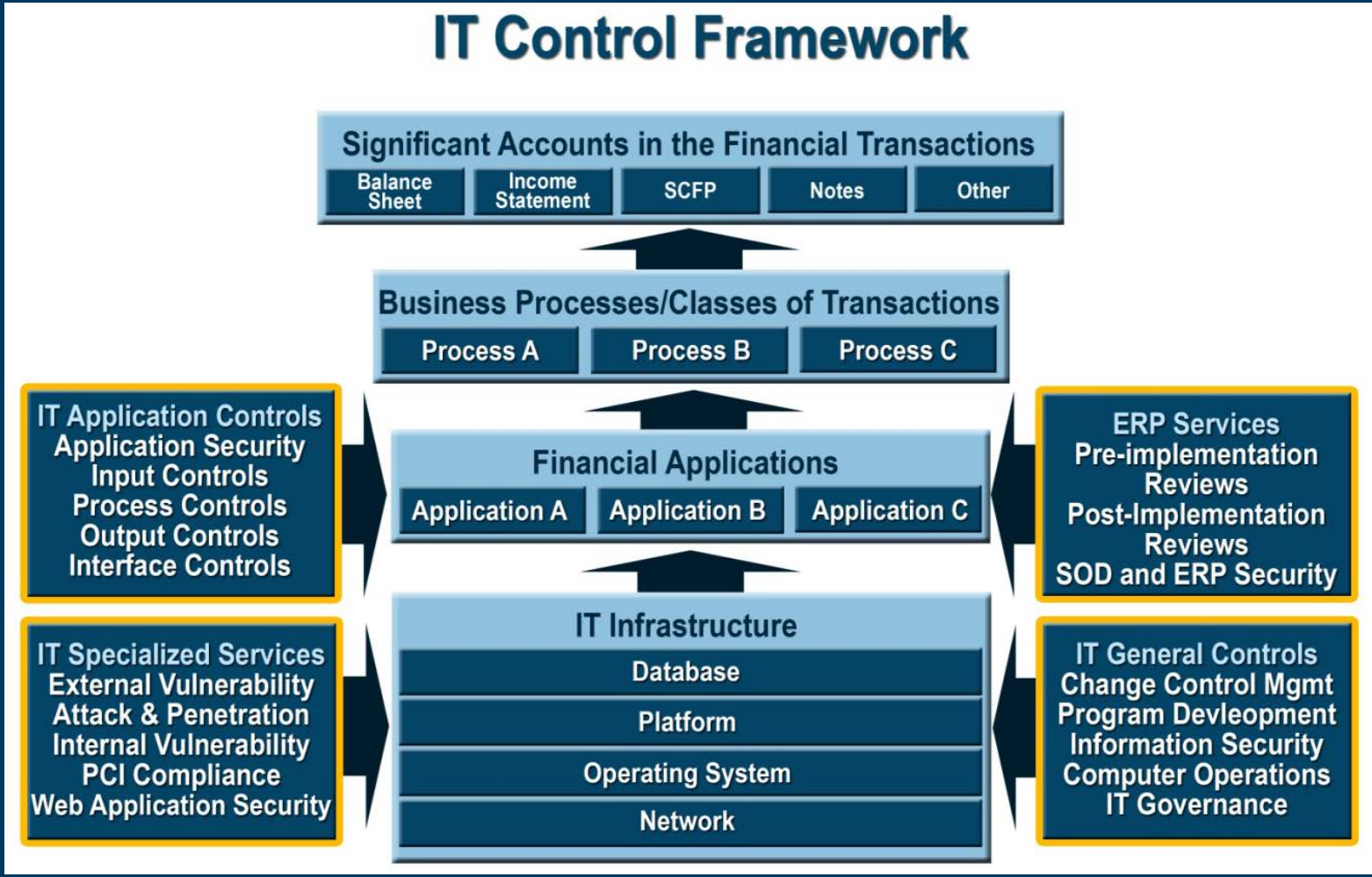
Top 10 Cybersecurity Risks

- Storing, Processing or Transmitting Sensitive Data
  - Non-public Personally Identifiable Information (PII)
  - Protected Health Information (PHI)
  - Credit Card Holder Data (CHD)
- Employees – intentional and unintentional actions
- Weaknesses in your IT Risk Assessment and InfoSec Planning
- Weaknesses in your Information Security Program
- Weaknesses in your Vulnerability Management Program
- Weaknesses in your Web Applications
- Weaknesses in your perimeter e-security layers
- Weaknesses in your internal e-security layers
- Weaknesses in your Change Management, e.g. patches and updates
- Access by Third Party Vendors

Most Effective Strategies to Overcome the Top Cybersecurity Risks

- Annual IT/InfoSec Risk Assessment and Planning
- Adopt and implement an IT Security Framework
- Conduct Regular Audits and/or Compliance Reviews
- IT Security Policies and Awareness Training
- Effective Vulnerability Management and Penetration Testing Program
- Web Application Security Reviews
- Proactive Third Party Vendors Security Compliance Programs

IT Risk Assessment Framework



IT Risk Universe and Risk Assessment

Information Asset	Inherent Risk					Business Criticality					Composite Risk Rating	Control Environment						Residual Risk Rating
	Threats & Vulnerabilities	Threat / Vuln Rating	Data Characteristics	Data Char Rating	Inherent Risk Rating	Financial	Operational	Strategic	Legal / Regulatory	Business Crit Rating		Process & App Control	Plan & Organize	Acquire & Implement	Deliver & Support	Monitor & Evaluate	CobiT Control % Mitigation	
Technology Service Provider Management	1, 2, 5, 6, 7, 8	6	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	10	16	3	2	1	3	9	144	M	W	M	W	W	35%	93.60
Core Applications	1, 2, 5, 6, 7, 9, 10	7	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	10	17	3	3	3	2	11	187	S	W	M	M	S	55%	84.15
SDLC and Program Change Controls	1, 5, 6, 7	4	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	10	14	3	3	2	1	9	126	M	M	M	M	W	35%	81.90
Internet Banking Controls	1, 3,4,6,7,9	6	1, 2, 3, 4, 5, 6	6	12	2	2	3	3	10	120	W	M	M	W	W	35%	78.00
External Network Security	1, 2, 5, 6, 7, 8, 10	7	1, 2, 3, 4, 5, 6, 7, 9, 10	9	16	3	3	3	2	11	176	M	M	M	S	S	60%	70.40
Internal Network Security	1, 2, 5, 6, 7, 8, 9, 10	8	1, 2, 3, 5, 6, 7, 9, 10	8	16	3	3	2	2	10	160	S	M	M	M	S	60%	64.00
ATM Network Compliance	1, 2, 6, 7, 10	5	1, 2, 3, 4, 5, 6, 7, 9	8	13	2	3	2	2	9	117	M	M	M	M	M	50%	58.50
Systems Administration	6, 7, 9	3	1, 2, 3, 5, 6, 7, 9	7	10	3	3	2	2	10	100	M	M	M	S	W	50%	50.00
Physical Security and Environmental Controls	1, 2, 7, 8, 9	5	1, 2, 3, 4, 7, 9	6	11	1	2	2	1	6	66	M	S	M	M	W	50%	33.00
Mobile Computing Devices / Removable Media	1, 5, 6, 7,10	5	1, 2, 3, 4	4	9	2	2	2	2	8	72	S	W	M	M	S	55%	32.40
Business Continuity Planning	2, 6, 8, 9, 10	5	2, 4, 7 ,9 , 10	5	10	2	3	2	1	8	80	M	M	S	S	S	65%	28.00
Compliance Review (GLBA)	7	1	1, 2, 3, 4, 5	5	6	3	3	1	3	10	60	M	S	M	M	M	55%	27.00
IT Governance (Management and Administration)	5, 7	2	4, 5, 7, 9, 10	5	7	2	2	2	2	8	56	S	S	M	M	M	60%	22.40
Desktop Management and Support	1, 5, 6, 7	4	4, 5, 7, 9, 10	5	9	1	2	1	1	5	45	M	M	M	M	S	55%	20.25

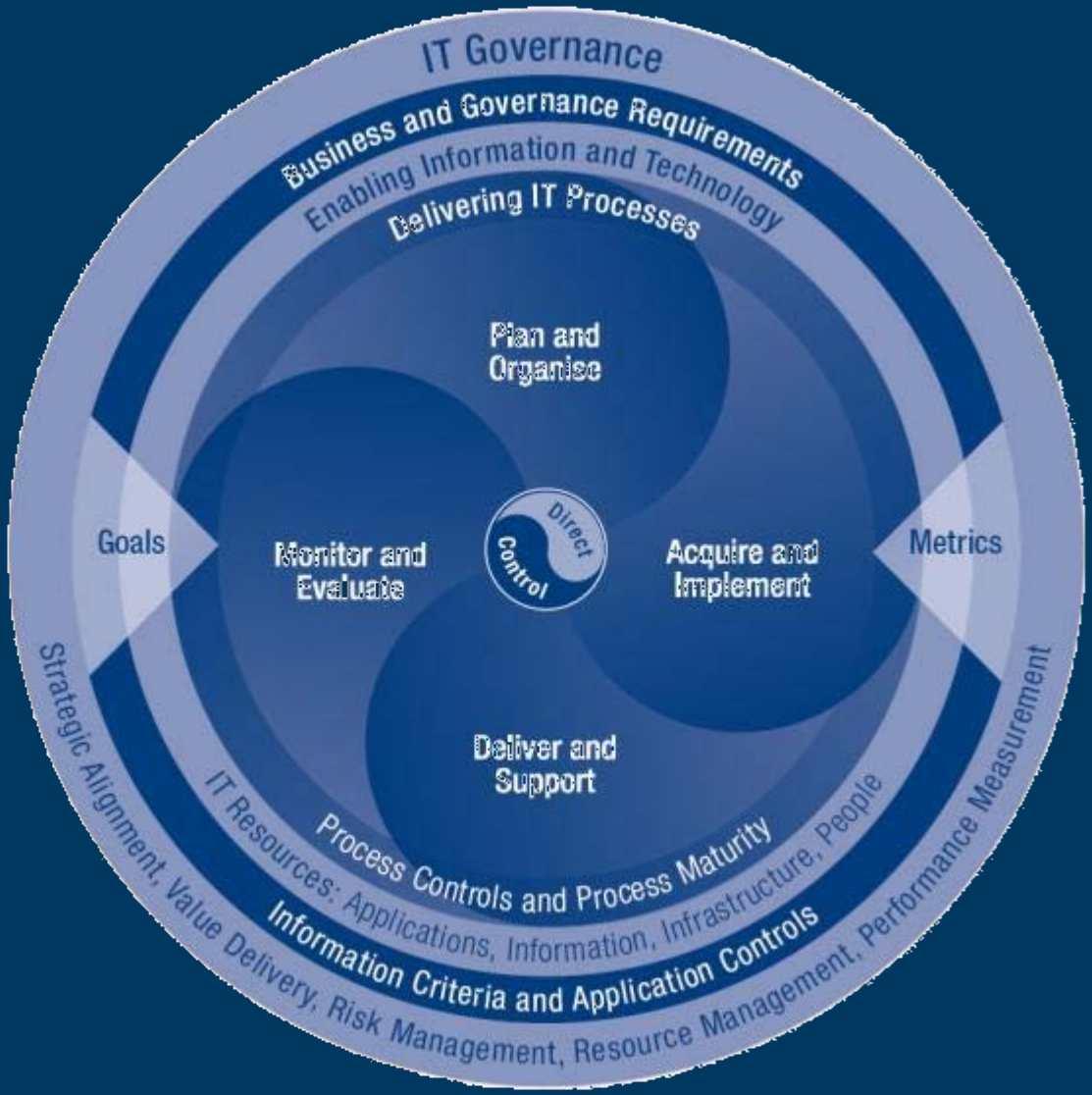
Adopt and Implement an Information Security Framework

- Select 1 framework (or 2 at most) based on relevance to your industry, customers, and/or key stakeholders
- Conduct a gap assessment
- Develop an gap remediation or implementation plan
  - Harden your systems and networks, improving secutiry
- Conduct annual audits and/or compliance reviews
- Achieve compliance or certification
  - Provide assurance to customers and stakeholders that your systems are secure
  - Meet regulatory requirements (HIPAA, GLBA, PCI, etc.)
  - Avoid breaches, fines, lost business/reputation, etc.
  - Marketing tool – strong compliance can be a differentiator

Example Frameworks

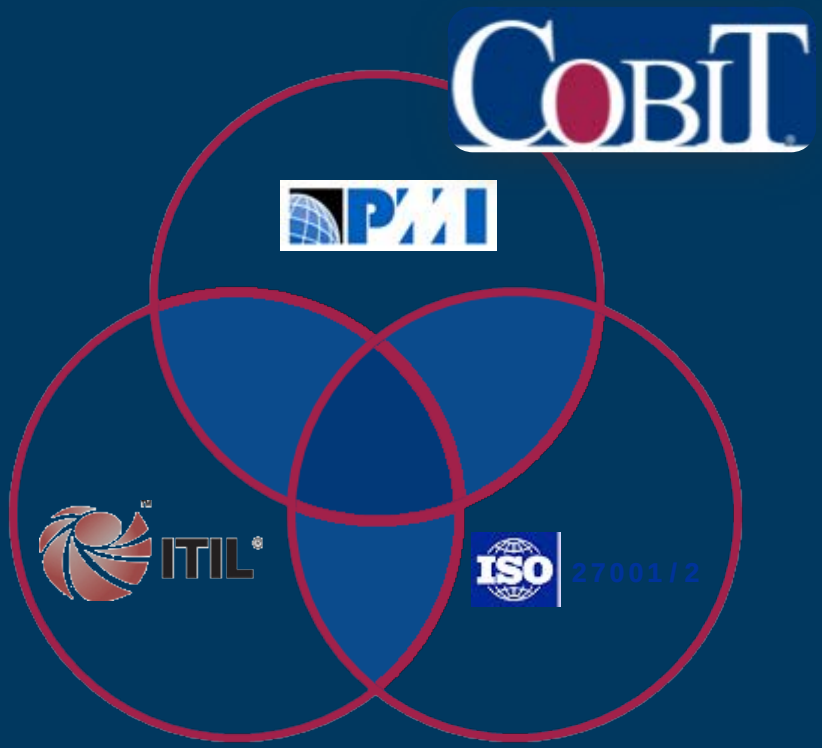
- PCI Data Security Standard 3.1 – credit card security
- Service Organization Controls (SOC) 1, 2 or 3 Reports
  - AICPA standards, widely accepted for internal control assurance
  - SOC 2 Trust Service Principles – Security, Confidentiality, Privacy, Availability, Processing Integrity
- ISO27000
- COBIT 5.0
- ITIL
- NIST Cybersecurity Framework
- HIPAA HITECH – Helathcare, PHI
- HITRUST Common Security Framework V7 – ISO, NIST, PCI, HIPAA, and COBIT

The COBIT Framework

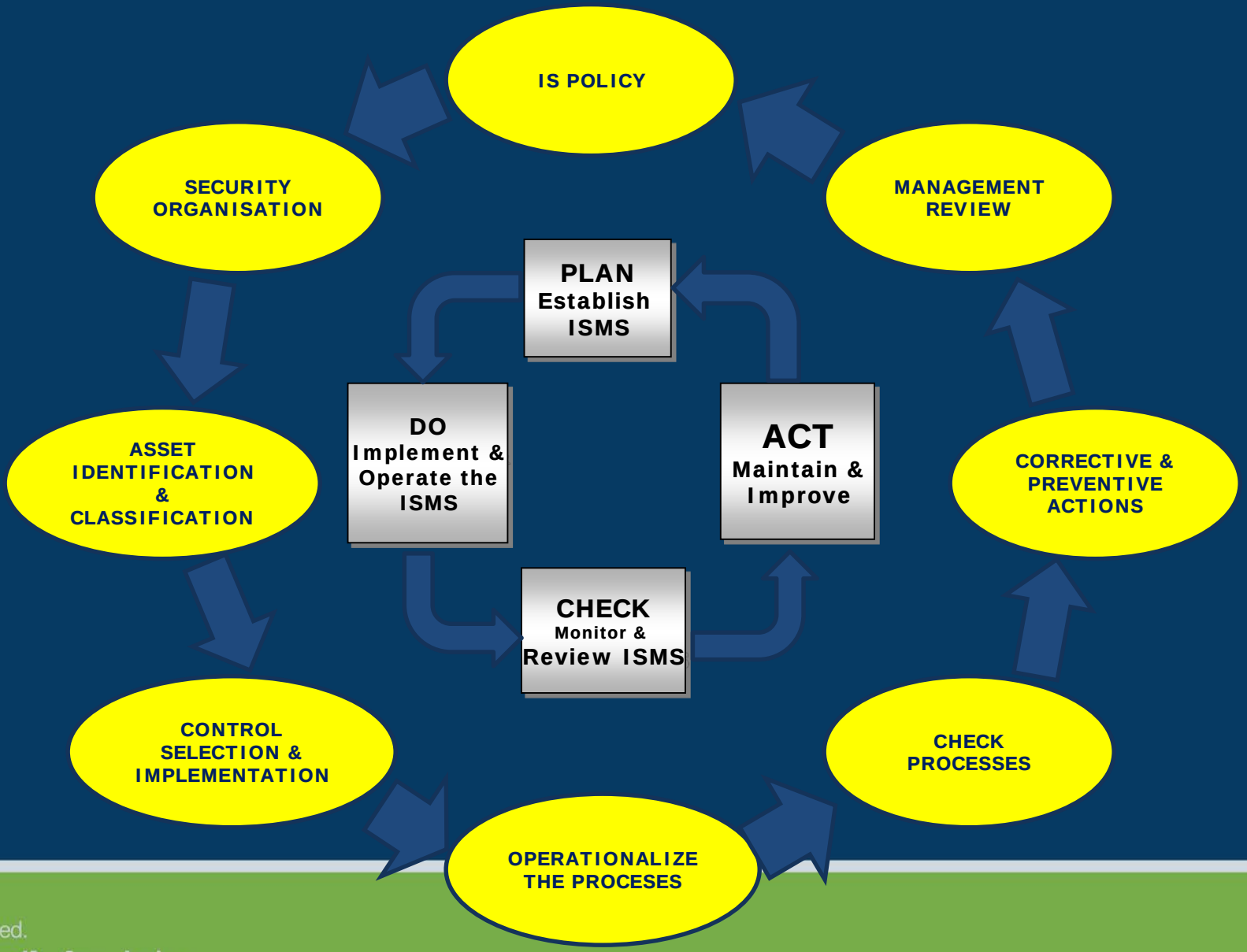


COBIT® Harmonises Other Standards

- COBIT is often used at the highest level of IT governance
- It harmonises practices and standards such as ITIL, ISO 27001 and 27002, and PMBOK
  - Improves their alignment to business needs
  - Covers full spectrum of IT-related activities



IMPLEMENTATION PROCESS CYCLE



ISO 27001 security

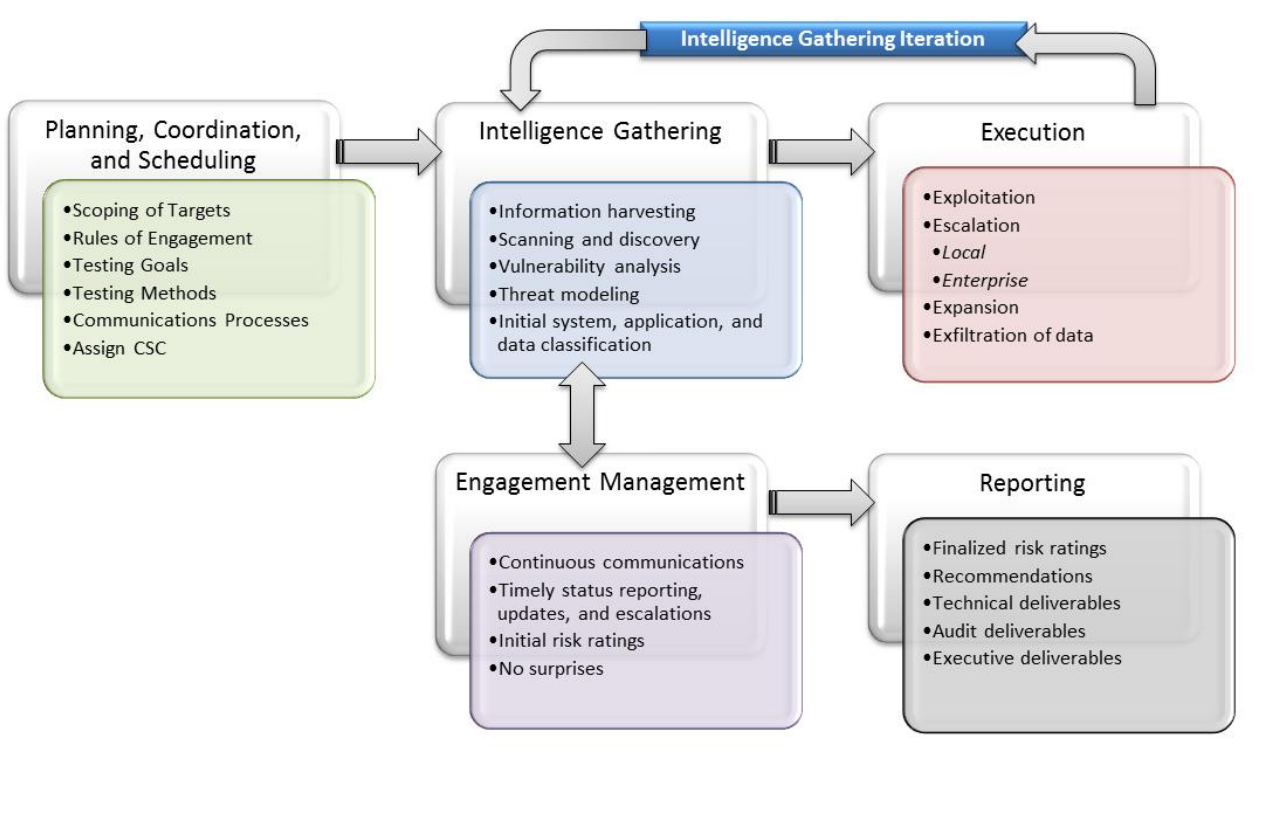
ust earned.
reedMaxick™

11

Establish an Effective Vulnerability and Penetration Testing Program

- Answer questions for management:
  - “Is our network secure?”
  - “How do we know that our network is secure?”
  - “Were we able to compromise any systems to gain unauthorized access?”
  - “Where are the weakest points in our network and do we have a plan to remediate those weaknesses?”
- Provide a baseline to help improve security
- Find configuration mistakes or missing security updates
- Determine whether an attack would be detected

Establish an Effective Vulnerability and Penetration Testing Program

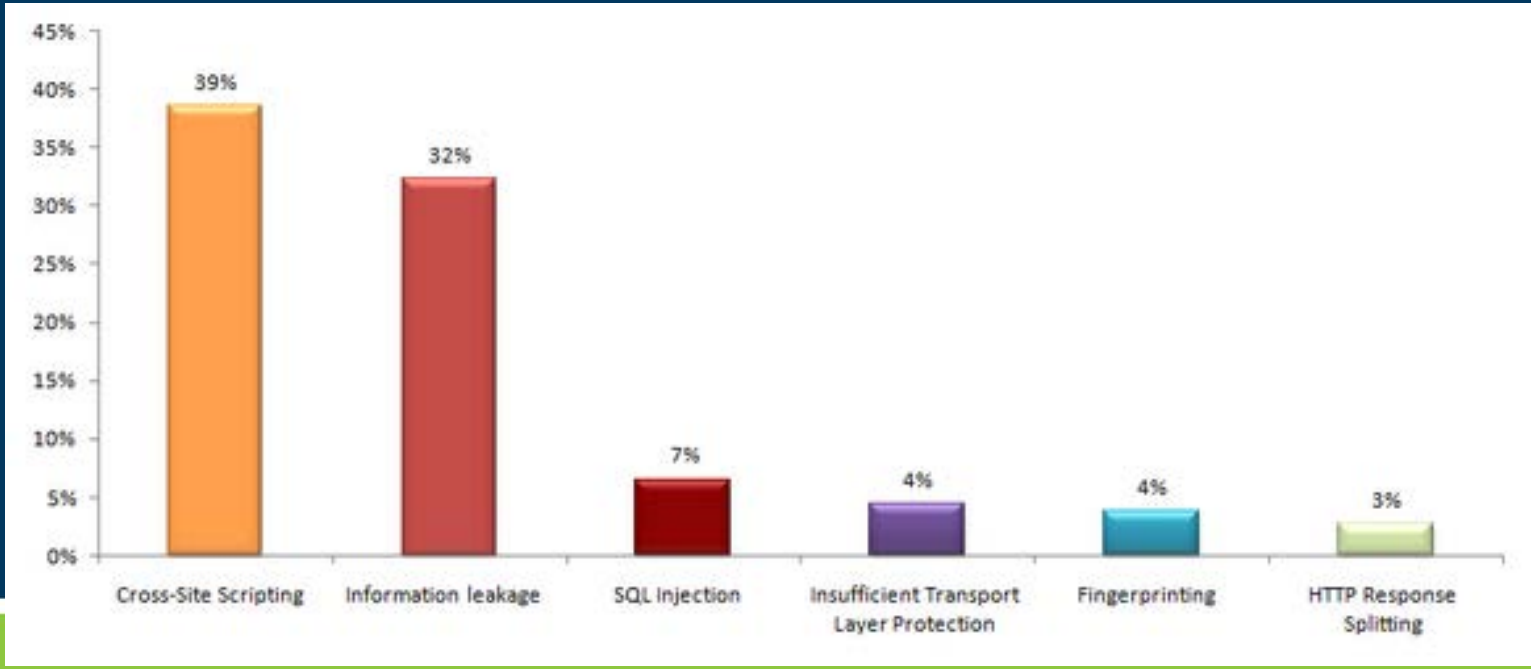


Best Practices:

- Methodology
- Proper Scoping
- Use variety of tools
- External V&P
- Internal V&P
- Web Applications

Web Application Security Review

- The most widespread vulnerabilities: Cross-Site Scripting, Information Leakage, SQL Injection, Insufficient Transport Layer Protection, Fingerprinting and HTTP Response Splitting.
- As a rule, Cross-Site Scripting, SQL Injection and HTTP Response Splitting vulnerabilities are caused by design errors, while Information Leakage, Insufficient Transport Layer Protection and Fingerprinting are often caused by insufficient administration (e.g., access control).



Mobile Device Risks

1. Most smartphone and tablet users don't even have a basic passcode set up on their device
2. Some web apps store user ID and password information for faster authentication, which can be obtained if phone is lost or stolen
3. Device's physical security can sometimes be easily by-passed
4. Service provider authentication is unencrypted or uses weak encryption
6. Average smartphone or tablet user has installed no security software - only a fraction of the security of a laptop or desktop
7. Detected malware developed for the Android platform alone has increased by 400% in the past year
8. Most app stores (e.g., Android Marketplace) don't review apps for security, it is very easy for criminals to post malicious apps that steal information from your mobile device
9. Technology that keeps apps separate on your smartphone or tablet doesn't separate that data – accessible by other apps
10. The temptation to use free WiFi hotspots at cafes, airports and hotels lures people into banking over insecure networks.

Mobile Device Risk Mitigation Strategies

- Communicate your authorized, official “apps”
- Provide best practice guidance to customers
  - Don’t use public Wi-Fi to conduct mobile banking – use a secure access point
  - Never send personal information via text or email
- Require use of secure PIN codes
- Allow downloading mobile apps only from institution websites or proven safe sources
- Separate credentials for Internet and mobile apps

Third Party Service Provider Management

- Frequently one of the highest risk “attack vectors” – Target HVAC!
- Much higher focus in updated PCI DSS 3.1 and in Banking Industry FFIEC regulatory requirements for Vendor Management
- What you need to do about 3rd party security:
  - Contractually require SP’s to provide documented security certification – e.g. SOC report(s), PCI AOC
  - Lock down their access to your network and systems
    - Consider using only temporary FireFighter UIDs rather than allowing them continuous access
  - Monitor, monitor, monitor their access
    - IDS, centralized sys logging, include them in annual or quarterly user access reviews
  - Consider including in V&P testing and/or auditing scope