Using Your Teaching Techniques for Your Career Success

Soft Skills

Litchko & Associates, Inc.

Secure Business-based Solutions™

Al Payne, CISSP
Theta Solutions, LLC.
703-409-4039
Alpayne@verizon.net

Jim Litchko, CISSP, CAS
Litchko & Associates, Inc.
301-661-3984
jim@litchko.com

Techniques & Applications

Wait time ►

Lesson Plans ►

Encouragement ►

Tell – Teach – Tell ►

Thought Provoking ? ►

Think-Pair-Share ►

Visual Learning ►

Differentiation ►

Timing ►

- Leading

- Managing

- Mentoring

- Facilitating

- Presenting

- Selling

Their Frames of Reference

Management	Operations	IT Systems	Security
Money	**Task delivery**	**Technical**	**Minimize risk**

Business Costs
 	
Increase:
    business, revenue,
    profits, productivity,
    market share
Decrease:
    costs, resources,
    deliverables
    resources
	Business Delivery
	
	Faster delivery,
	Less manpower to do
	Lower cost to do
	Make me the hero
		Infrastructure Development
		
		Technological silver bullet
		Most elegant solution
		Open, flexible operations
		Not from overhead budget
			Restrict Services
			
			Little or no risk
			Meet regulations
			Keep me out of trouble

This Is My Approach

NIST C&A Process With System Lifecycle Considerations

C&A

C&A and **System Lifecycle** Processes

The level of effort and detail applied should be commensurate with **FIPS 199** security category of the IS

Pre-Initiation Phase

<u>System Owner's Responsibility</u>

Provide previous C&A documentation, or perform the following functions:

Initial **SSP**
System Identification and Description
Security Assessment (Categorization)
NIST SP 800-18, 53A; FIPS 199

SSP

Define System Boundary
System Inventory,
Network/System Diagram

System Boundary Network Diagram

Risk Assessment
NIST SP 800-30

RA Report

No

SSP & **RA** completed and consistent?

Yes

Initiation Phase

Preparation

Confirm & Validate Documentation:
IS Description (SSP); Security Categorization; Threat Identification; Vulnerability Identification; Security Control Identification; Initial Risk Determination
NIST SP 800-18, 30, 53, 59, 60; OMB A-130 Apx III; FISMA; FIPS 199

Notification and Resource Identification

Notification; Planning and Resources
OMB A-130

C&A Plan w/Milestones

SSP Analysis, Update and Acceptance

Security Categorization Review
NIST SP 800-60; FIPS 199

SSP Analysis; SSP Update
NIST SP 800-18

Updated **SSP** (**CP** part of SSP)

No

SSP Accepted?

Yes

Security Certification Phase

Security Control Assessment

Documentation and Supporting Materials
NIST SP 800-53A; ISO/IEC 15408; FIPS 140-2

Methods and Procedures
(ST&E)
NIST SP 800-53, 53A

ST&E Plan

Security Assessment
(Test Security Controls)

Management	Operational	Technical

Identification and Validation
NIST SP 800-53A

Security Assessment Report
NIST SP 800-53A

Update **SSP** ST&E Report

Entry Point 1

Security Certification Documentation

Findings and Recommendations
NIST SP 800-30

Risk Mitigation

Regression Testing

RRR

Mitigated Risk	Accepted Risk

Residual Risk

Yes:
Examine only
KNOWN
Risks/Findings

Continue Risk Reduction?

No

RA Report RR Report

SSP update
NIST SP 800-18

Update **SSP**

POA&M
OMB memo 02-01

POA&M

Accreditation Package Assembly
OMB A-130, Apx III

Security Accreditation Phase

Security Accreditation Decision

Final Risk Determination
NIST SP 800-30

Risk Acceptability
OMB A-130 Apx III

Risk Acceptable?

No

Yes

Accredit System

Grant IATO?

No

Entry Point 1

Yes

Detailed **POA&M**

POA&M

IATO Accredited

IATO Terms

Security Accreditation Documentation

Security Accreditation Package Transmission
OMB A-130 Apx III
SSP Update
NIST SP 800-18

Update **SSP**

Continuous Monitoring Phase

Techniques & Applications

Wait time ▶

Lesson Plans ▶

Encouragement ▶

Tell – Teach – Tell ▶

Thought Provoking ? ▶

Think-Pair-Share ▶

Visual Learning ▶

Differentiation ▶

Timing ▶

- Leading

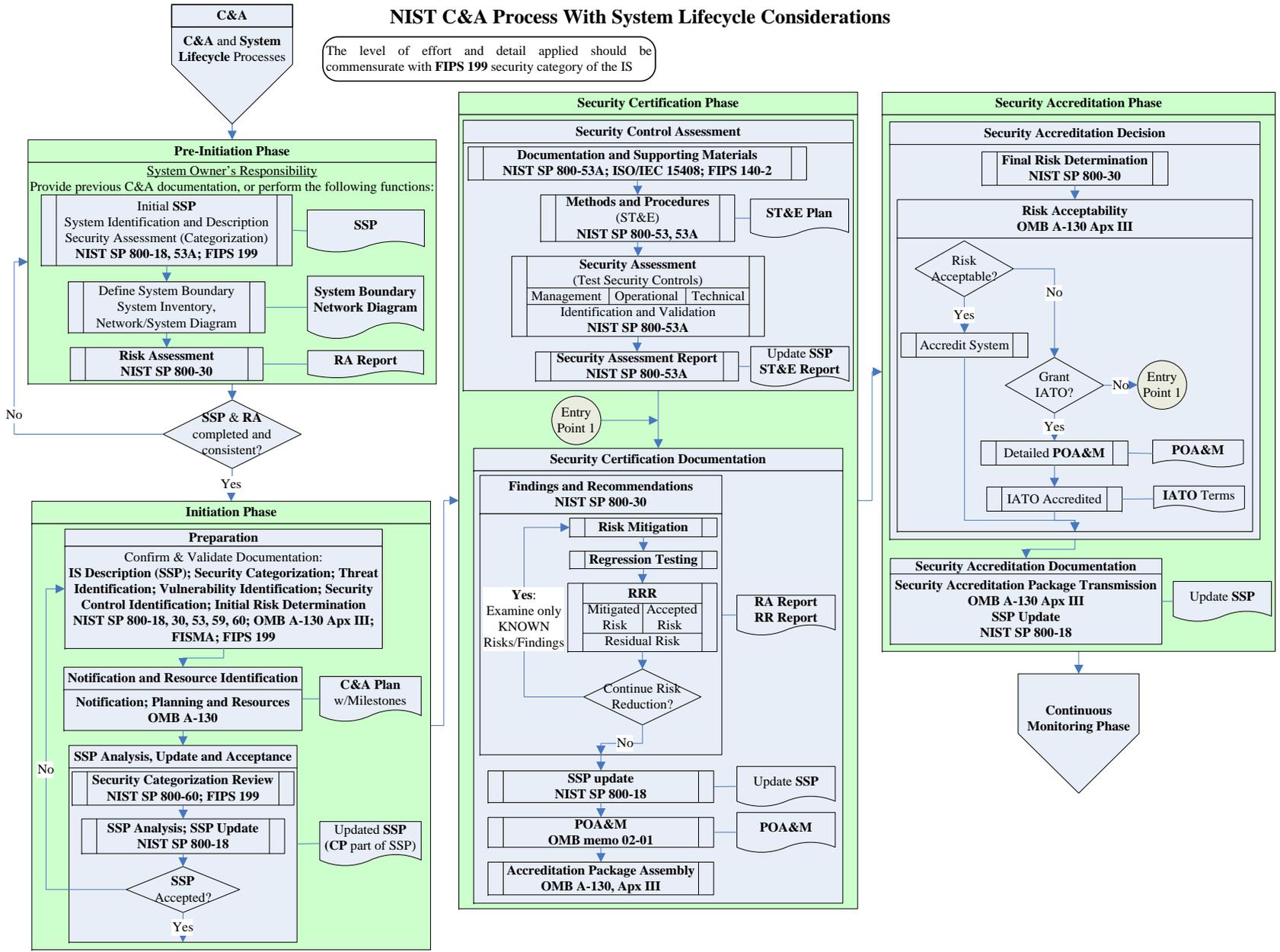- Managing

- Mentoring

- Facilitating

- Presenting

- Selling

Al Payne, CISSP
Jim Litchko, CAS

Combined 60 years experience in managing IT systems and IT security.

Practitioners, integrators, consultants, executives, program managers, budgeters, educators, motivators and facilitators.

Worked in government, military, commercial and academic positions. From NSA to Johns Hopkins University.

Have assessed over 150 IT systems from the White House to an Internet gambling casino.

Authors of four books and speak on security topics at over 30 events a year.

Former Navy and Marine Corp officers.

Cyber Threat Levels Response Handbook

HOMELAND SECURITY ADVISORY SYSTEM
SEVERE
HIGH
ELEVATED
GUARDED
LOW

James P. Litchko
Ron Lander, CPP, CAS
Lew Wagner, CISSP, CP

The handbook of the IT system security actions taken at each Homeland Security Threat Cond

KNOW Your Life

KNOW IT Security
SECURE IT SYSTEMS CASINO STYLE
Securing computers and networks for non-technical managers: a practical case study
James P. Litchko

KNOW Cyber Risk
BY MANAGING YOUR IT SECURITY!
Learn successful strategies so you can manage IT security assessments, sell security to your boss and even improve your career
James P. Litchko
Al Payne, CISSP