Information Security Management

Chapter 6
Security Management Models & Practices

Webster University
Scott Granneman

“Security can only be achieved
through constant change,
through discarding old ideas
that have outlived their usefulness
& adapting others to current facts.”

-- William O. Douglas,
US Supreme Court Justice (1898–1980)

Upon completion of this chapter, you should be able to:

Select from
the dominant infosec management models,
including US government sanctioned models,
& customize them for your organization’s needs

Implement the fundamental elements
of key infosec management practices

Follow emerging trends in the certification
& accreditation of US Federal IT systems

To create or maintain
a secure environment:

✓ Design working security plan

✓ Implement management model
to execute & maintain the plan

↓

May begin
with creation or validation
of security framework,
followed by an infosec blueprint
describing existing controls
& identifying other
necessary security controls

Framework: outline
of the more thorough blueprint,
which is the basis for
the design, selection, & implementation
of all subsequent security controls

Most organizations
draw from established
security models & practices
to develop a blueprint or methodology

One of the most widely referenced
& often discussed security models
is “Information Technology –
Code of Practice for InfoSec Management”,
which was originally published
as British Standard (BS) 7799

The purpose of ISO/IEC 17799
is to give recommendations
for infosec management
for use by those who are responsible
for initiating, implementing, or maintaining
security in their organization

ISO/IEC 17799 was intended
to provide a common basis
for developing
organizational security standards
& effective security management practice
& to provide confidence
in inter-organizational dealings

Volume 2 provides information
on how to implement Volume 1 (17799)
& how to set up
an InfoSec Management Structure (ISMS)

Drawbacks

The global infosec community has not defined any justification for a code of practice as identified in ISO/IEC 17799

Other problems with ISO/IEC 17799

✓ Lacks “the necessary measurement precision of a technical standard”

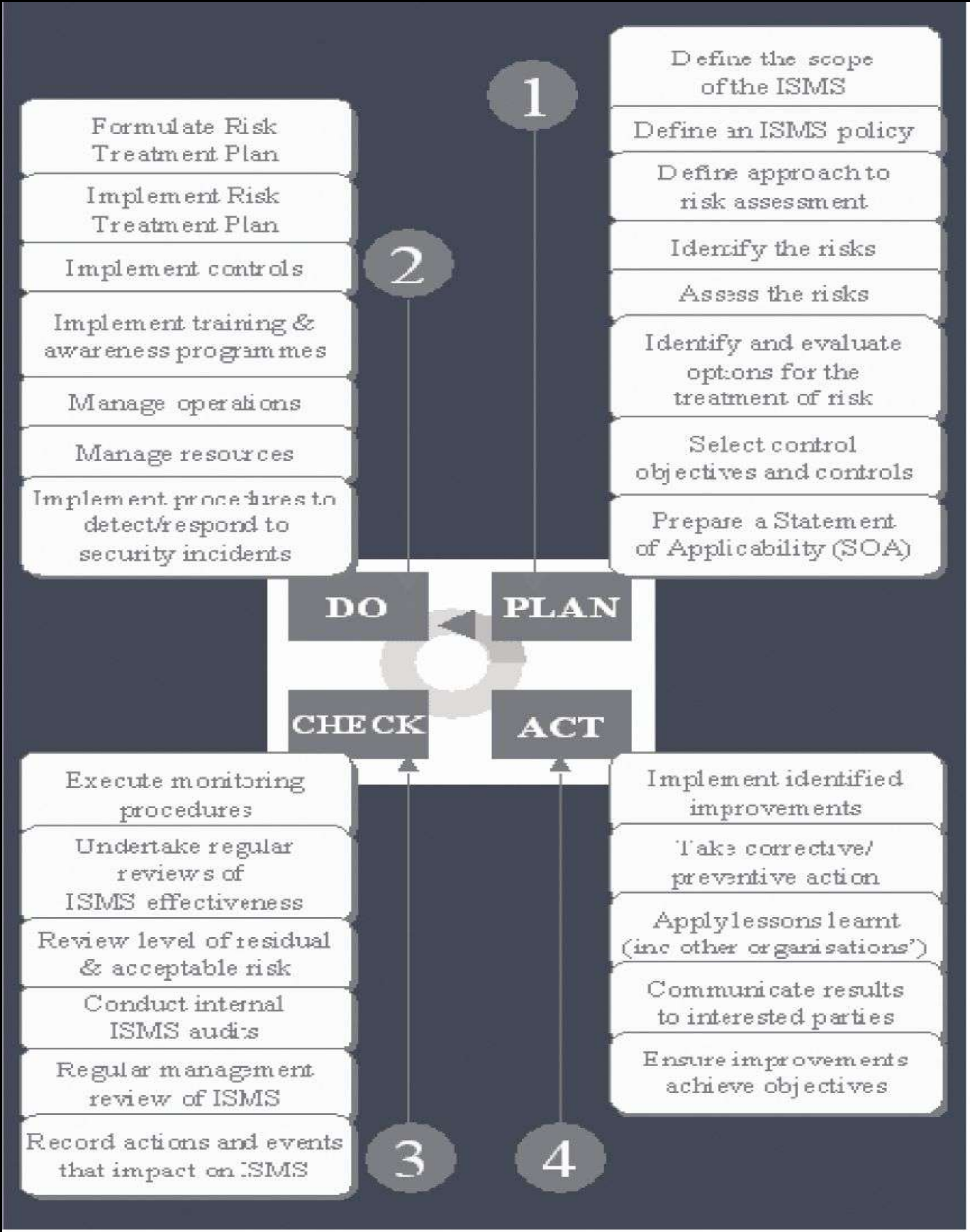
✓ No reason to believe that ISO/IEC 17799 is more useful than any other approach

✓ Not as complete as other frameworks

✓ Perceived to have been hurriedly prepared, given tremendous impact its adoption could have on industry infosec controls

Ten Sections Of ISO/IEC 17799

1. Organizational Security Policy
2. Organizational Security Infrastructure Objectives
3. Asset Classification & Control
4. Personnel Security objectives
5. Physical & Environmental Security Objectives
6. Communications & Operations Management Objectives
7. System Access Control Objectives
8. System Development & Maintenance Objectives
9. Business Continuity Planning
10. Compliance Objectives



1

PLAN

- Define the scope of the ISMS
- Define an ISMS policy
- Define approach to risk assessment
- Identify the risks
- Assess the risks
- Identify and evaluate options for the treatment of risk
- Select control objectives and controls
- Prepare a Statement of Applicability (SOA)

2

DO

- Formulate Risk Treatment Plan
- Implement Risk Treatment Plan
- Implement controls
- Implement training & awareness programmes
- Manage operations
- Manage resources
- Implement procedures to detect/respond to security incidents

3

CHECK

- Execute monitoring procedures
- Undertake regular reviews of ISMS effectiveness
- Review level of residual & acceptable risk
- Conduct internal ISMS audits
- Regular management review of ISMS
- Record actions and events that impact on ISMS

4

ACT

- Implement identified improvements
- Take corrective/ preventive action
- Apply lessons learnt (inc other organisations')
- Communicate results to interested parties
- Ensure improvements achieve objectives

FIGURE 6-2 Plan-Do-Check-Act Cycle from BS 7799:2

To determine how closely an organization is complying with ISO 17799, take Human Firewall Council’s survey, the Security Management Index (SMI)

✓ Asks 35 questions over 10 domains of ISO standard

✓ Gathers metrics on how organizations manage security

✓ Enables infosec officers to benchmark their practices against those of other organizations

Survey has been developed
according to ISO 17799
international security standards
to reflect best practices
from a global perspective

The Security Management Index survey
can help you compare yourself
to other organizations in your industry
& peer group

Human Firewall Council SMI

✓ Familiarize yourself with
the 10 categories of security management

✓ Benchmark your organization’s
security management practices
by taking the survey

✓ Evaluate your results in each category
to identify strengths & weaknesses

✓ Examine the suggestions for improvement
in each category in this report

✓ Use your SMI results
to gain support for improving security

The Security Area Working Group
within the IETF has created RFC 2196,
the Site Security Handbook,
which provides a functional discussion
of important security issues
along with
development & implementation details

Covers security policies,
security technical architecture,
security services,
& security incident handling

Also includes discussion of
the importance of security policies,
& expands into an examination of services,
access controls, & other relevant areas

NIST documents have 2 big advantages:

1. Publicly available at no charge
2. Have been broadly reviewed by government & industry professionals

✓ SP 800-12: Computer Security Handbook

✓ SP 800-14: Generally Accepted Security Principles & Practices

✓ SP 800-18: Guide for Developing Security Plans

✓ SP 800-26: Security Self-Assessment Guide-IT Systems

✓ SP 800-30: Risk Management for Information Technology Systems

NIST SP 800-12
The Computer Security Handbook

✓ Excellent reference & guide
for routine management of infosec

✓ Little provided on design
& implementation
of new security systems

✓ Use as supplement
to gain a deeper understanding
of background & terminology

more … →

Lays out NIST philosophy
on security management
by identifying 17 controls
organized into 3 categories:

1. **Management Controls** section
addresses security topics
characterized as managerial

2. **Operational Controls** section
addresses security controls
focused on controls that are, broadly speaking,
implemented & executed by people
(as opposed to systems)

3. **Technical Controls** section
focuses on security controls
that the computer system executes

NIST Special Publication 800-14
Generally Accepted Principles & Practices
for Securing IT Systems

✓ Describes best practices
useful in the development
of a security blueprint

✓ Describes principles
that should be integrated
into infosec processes

✓ Documents 8 points & 33 Principles

more … →

The more significant points made in NIST SP 800-14 are:

✓ Security supports the mission of the organization
✓ Security is an integral element of sound management
✓ Security should be cost-effective
✓ Systems owners have security responsibilities outside their own organizations
✓ Security responsibilities & accountability should be made explicit
✓ Security requires a comprehensive & integrated approach
✓ Security should be periodically reassessed
✓ Security is constrained by societal factors

Principles of NIST SP 800-14:

✓ Establish sound security policy
as “foundation” for design

✓ Treat security as integral part
of overall system design

✓ Clearly delineate
physical & logical security boundaries
governed by associated security policies

more … →

✓ Reduce risk to acceptable level

✓ Assume that external systems are insecure

✓ Identify potential trade-offs between reducing risk & increased costs & decrease in other aspects of operational effectiveness

✓ Implement layered security (ensure no single point of vulnerability)

more … →

✓ Implement tailored system security measures
to meet organizational security goals

✓ Strive for simplicity

✓ Design & operate an IT system
to limit vulnerability
& to be resilient in response

✓ Minimize system elements to be trusted

✓ Implement security through
a combination of measures
distributed physically & logically

more ... →

✓ Provide assurance that the system is,
& continues to be,
resilient in the face of expected threats

✓ Limit or contain vulnerabilities

✓ Formulate security measures
to address
multiple overlapping information domains

✓ Isolate public access systems
from mission critical resources

more … →

✓ Use boundary mechanisms
to separate computing systems
& network infrastructures

✓ Where possible,
base security on open standards
for portability & interoperability

✓ Use common language
in developing security requirements

✓ Design & implement audit mechanisms
to detect unauthorized use
& to support incident investigations

more … →

✓ Design security to allow for
regular adoption of new technology,
including a secure & logical
technology upgrade process

✓ Authenticate users & processes
to ensure appropriate access control decisions
both within & across domains

✓ Use unique identities to ensure accountability

✓ Implement least privilege

✓ Do not implement
unnecessary security mechanisms

more … →

✓ Protect information while
being processed, in transit, & in storage

✓ Strive for operational ease of use

✓ Develop & exercise
contingency or disaster recovery procedures
to ensure appropriate availability

✓ Consider custom products
to achieve adequate security

more … →

✓ Ensure proper security
in the shutdown or disposal
of a system

✓ Protect against all likely classes of “attacks”

✓ Identify & prevent
common errors & vulnerabilities

✓ Ensure that developers
are trained in how
to develop secure software

NIST Special Publication 800-18
A Guide for Developing Security Plans for Information Technology Systems

✓ Provides detailed methods
for assessing, designing, & implementing
controls & plans
for various sized applications

✓ Serves as a guide for the activities
described in this chapter,
& for the overall infosec planning process

✓ Includes templates
for major application security plans

NIST Special Publication 800-26
17 areas Defining the Core
# of the NIST Security Management Structure

Management Controls

1. Risk Management

2. Review of Security Controls

3. Life Cycle Maintenance

4. Authorization of Processing
(Certification & Accreditation)

5. System Security Plan

Operational Controls

6. Personnel Security

7. Physical Security

8. Production, Input/Output Controls

9. Contingency Planning

10. Hardware & Systems Software

11. Data Integrity

12. Documentation

13. Security Awareness, Training, & Education

14. Incident Response Capability

Technical Controls

15. Identification & Authentication

16. Logical Access Controls

17. Audit Trails

NIST Special Publication 800-30
Risk Management Guide
for Information Technology Systems

Provides a foundation
for the development
of an effective risk management program

Contains both the definitions
& the practical guidance necessary
for assessing & mitigating risks
identified within IT systems

Strives to enable organizations
to better manage IT-related risks

In infosec, 2 categories of benchmarks
for security management practices
are used:

1. Standards of due care/due diligence
2. Best practices

Best practices include
a sub-category of practices
—called the **gold standard**—
that are generally regarded
as “the best of the best”

When organizations adopt
minimum levels of security
for a legal defense,
they may need to show
that they have done
what any prudent organization
would do in similar circumstances –
AKA, a standard of **due care**

Implementing controls
at this minimum standard,
& maintaining them,
demonstrates that an organization
has performed **due diligence**

Due diligence requires
that an organization ensure
that the implemented standards
continue to provide
the required level of protection

Failure to support a standard
of due care or due diligence
can expose an organization to legal liability,
provided it can be shown
that the organization was negligent
in its application or lack of application
of information protection

Security efforts that seek
to provide a superior level of performance
in the protection of information
are referred to as
best business practices
or simply **best practices**

Some organizations
call them **recommended practices**

Security efforts that are among
the best in the industry
are referred to as **best security practices**

Best security practices balance the need
for information access
with the need for adequate protection

Best practices seek to provide
as much security as possible
for information & information systems
while demonstrating fiscal responsibility
& ensuring information access

Companies with best practices
may not be the best in every area

They may only have established
an extremely high quality
or successful security effort in one area

An example of best practices: VISA

VISA has developed 2 important documents
that improve & regulate
its information systems:

1. The “Security Assessment Process” document
contains series of recommendations
for detailed examination of organization’s systems
with the eventual goal
of integration into the VISA systems

2. The “Agreed Upon Procedures” document
outlines the policies & technologies
used to safeguard security systems
that carry the sensitive cardholder information
to & from VISA systems

Best business practices are not sufficient
for organizations that prefer
to set the standard by implementing
the most protective, supportive,
& yet fiscally responsible standards
they can

They strive toward the gold standard,
a model level of performance
that demonstrates industrial leadership,
quality, & concern for the protection of
information

It ain’t easy, though

The implementation
of gold standard security
requires a great deal of support,
both in financial & personnel resources

Choosing which
recommended practices to implement
can pose a challenge for some organizations

In industries
regulated by governmental agencies,
government guidelines
are often requirements

For other organizations,
government guidelines
are excellent sources of information
& can inform their selection of best practices

When considering best practices for your organization, consider the following:

✓ Does your organization resemble
the identified target organization
of the best practice?

✓ Are you in a similar industry as the target?

✓ Do you face similar challenges as the target?

✓ Is your organizational structure
similar to the target?

✓ Are the resources you can expend
similar to those called for by the best practice?

✓ Are you in a similar threat environment
as the one assumed by the best practice?

Microsoft has published a set of best practices in security at its Web site:

✓ Use antivirus software

✓ Use strong passwords

✓ Verify your software security settings

✓ Update product security

✓ Build personal firewalls

✓ Back up early & often

✓ Protect against power surges & loss

Biggest problem with benchmarking in infosec:

✓ Organizations don’t talk to each other
✓ Successful attack is viewed
as organizational failure
& is kept secret, as much as is possible

However, more & more security administrators
are joining professional associations & societies
& sharing their stories & lessons learned

Alternative to this direct dialogue
is the publication of lessons learned

Baseline: “value or profile of a performance metric against which changes in the performance metric can be usefully compared”

Baselining: process of measuring against established standards

In InfoSec, the comparison of security activities & events against the organization’s future performance

Can provide foundation for internal benchmarking, as information gathered for an organization’s first risk assessment becomes the baseline for future comparisons

The Gartner Group offers 12 questions for self assessment of best security practices

People:

1. Do you perform background checks on all employees with access to sensitive data, areas, or access points?

2. Would the average employee recognize a security issue?

3. Would they choose to report it?

4. Would they know how to report it to the right people?

more ... →

Processes:

5. Are enterprise security policies updated
on at least an annual basis,
employees educated on changes,
& consistently enforced?

6. Does your enterprise follow
a patch/update management & evaluation process
to prioritize & mediate
new security vulnerabilities?

7. Are the user accounts of former employees
immediately removed on termination?

8. Are security group representatives involved
in all stages of the project life cycle for new projects?

more ... →

Technology:

9. Is every possible route to the Internet
protected by a properly configured firewall?

10. Is sensitive data
on laptops & remote systems encrypted?

11. Do you regularly scan your systems & networks,
using a vulnerability analysis tool,
for security exposures?

12. Are malicious software scanning tools
deployed on all workstations & servers?

In security management,
accreditation is authorization
of an IT system
to process, store, or transmit information

✓ Issued by management official

✓ Serves as means of assuring
that systems are of adequate quality

✓ Also challenges managers & technical staff
to find best methods to assure security,
given technical constraints, operational constraints,
& mission requirements

Certification: “the comprehensive evaluation
of the technical & non-technical
security controls of an IT system
to support the accreditation process
that establishes the extent to which
a particular design & implementation
meets a set
of specified security requirements”

Organizations pursue
accreditation or certification
to gain a competitive advantage,
or to provide assurance or confidence
to customers

SP 800-37
Guidelines for the Security Certification & Accreditation of Federal IT Systems

✓ Develops standard guidelines & procedures for certifying & accrediting federal IT systems including critical US infrastructure

✓ Defines essential minimum security controls for federal IT systems

more … →

✓ Promotes development
of public & private sector
assessment organizations
& certification of individuals
capable of providing
cost effective, high quality, security certifications
based on standard guidelines & procedures

Specific benefits of security certification & accreditation (C&A) initiative include:

✓ More consistent, comparable, & repeatable certifications of IT systems

✓ More complete & reliable information for authorizing officials —leading to better understanding of complex IT systems & associated risks & vulnerabilities— & therefore, more informed decisions by management officials

✓ Greater availability of competent security evaluation & assessment services

✓ More secure IT systems within the federal government

800-37 focuses on a three-step security controls selection process:

Step 1: Characterize the system

Step 2: Select the appropriate minimum security controls for the system

Step 3: Adjust security controls based on system exposure & risk decision

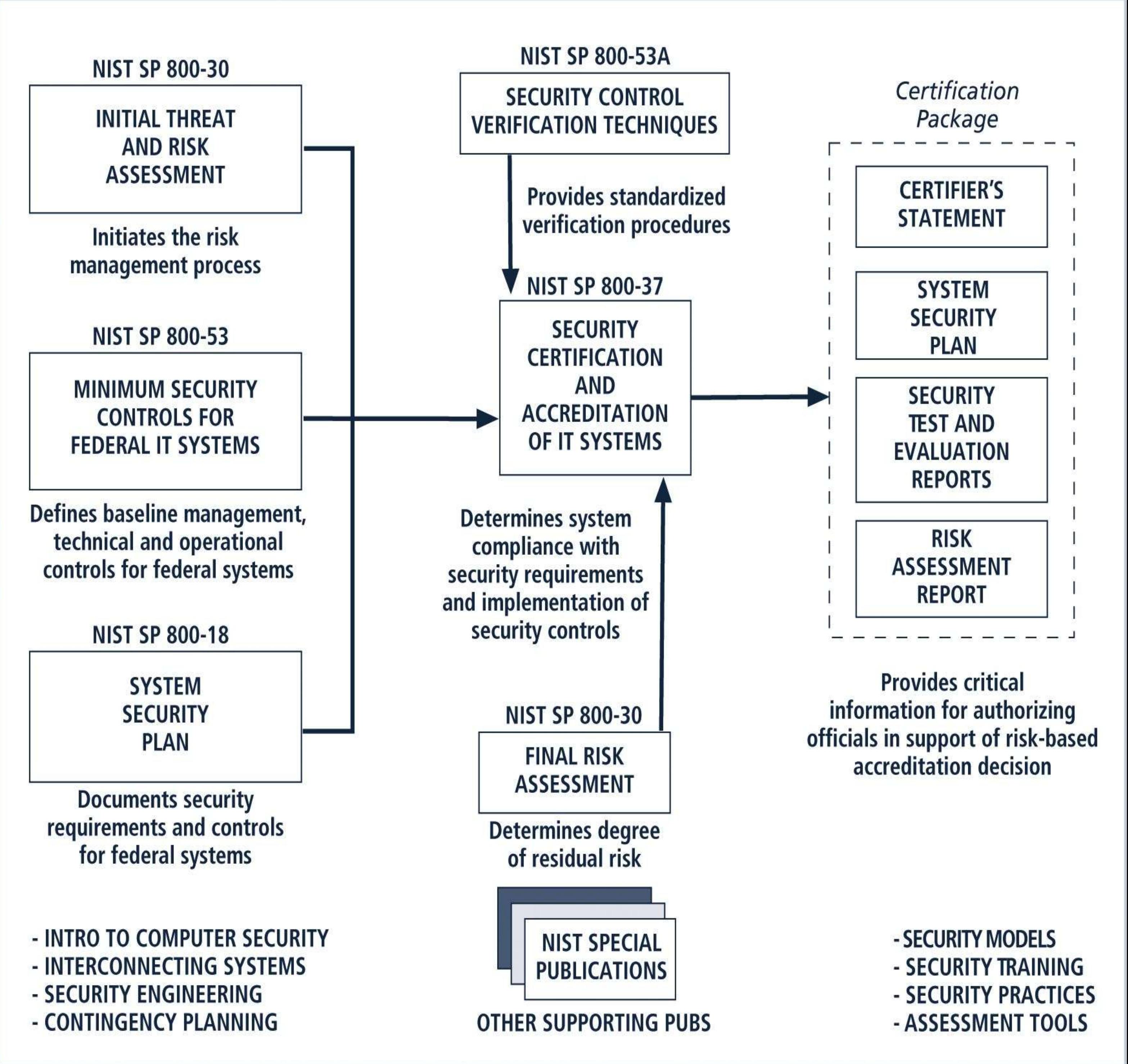

NIST SP 800-30
INITIAL THREAT AND RISK ASSESSMENT
Initiates the risk management process
NIST SP 800-53
MINIMUM SECURITY CONTROLS FOR FEDERAL IT SYSTEMS
Defines baseline management, technical and operational controls for federal systems
NIST SP 800-18
SYSTEM SECURITY PLAN
Documents security requirements and controls for federal systems
NIST SP 800-53A
SECURITY CONTROL VERIFICATION TECHNIQUES
Provides standardized verification procedures
NIST SP 800-37
SECURITY CERTIFICATION AND ACCREDITATION OF IT SYSTEMS
Determines system compliance with security requirements and implementation of security controls
NIST SP 800-30
FINAL RISK ASSESSMENT
Determines degree of residual risk
Certification Package
CERTIFIER'S STATEMENT
SYSTEM SECURITY PLAN
SECURITY TEST AND EVALUATION REPORTS
RISK ASSESSMENT REPORT
Provides critical information for authorizing officials in support of risk-based accreditation decision
- INTRO TO COMPUTER SECURITY
- INTERCONNECTING SYSTEMS
- SECURITY ENGINEERING
- CONTINGENCY PLANNING
NIST SPECIAL PUBLICATIONS
OTHER SUPPORTING PUBS
- SECURITY MODELS
- SECURITY TRAINING
- SECURITY PRACTICES
- ASSESSMENT TOOLS

FIGURE 6-3 Special Publications Supporting SP 800-37

Planned Federal System Certifications

Systems are to be certified to one of 3 levels:

Security Certification Level 1:
Entry-level certification
appropriate for low priority (concern) systems

Security Certification Level 2:
Mid-level certification
appropriate for
moderate priority (concern) systems

Security Certification Level 3:
Top-level certification
appropriate for high priority (concern) systems

SP 800-53
Minimum Security Controls
for Federal IT Systems

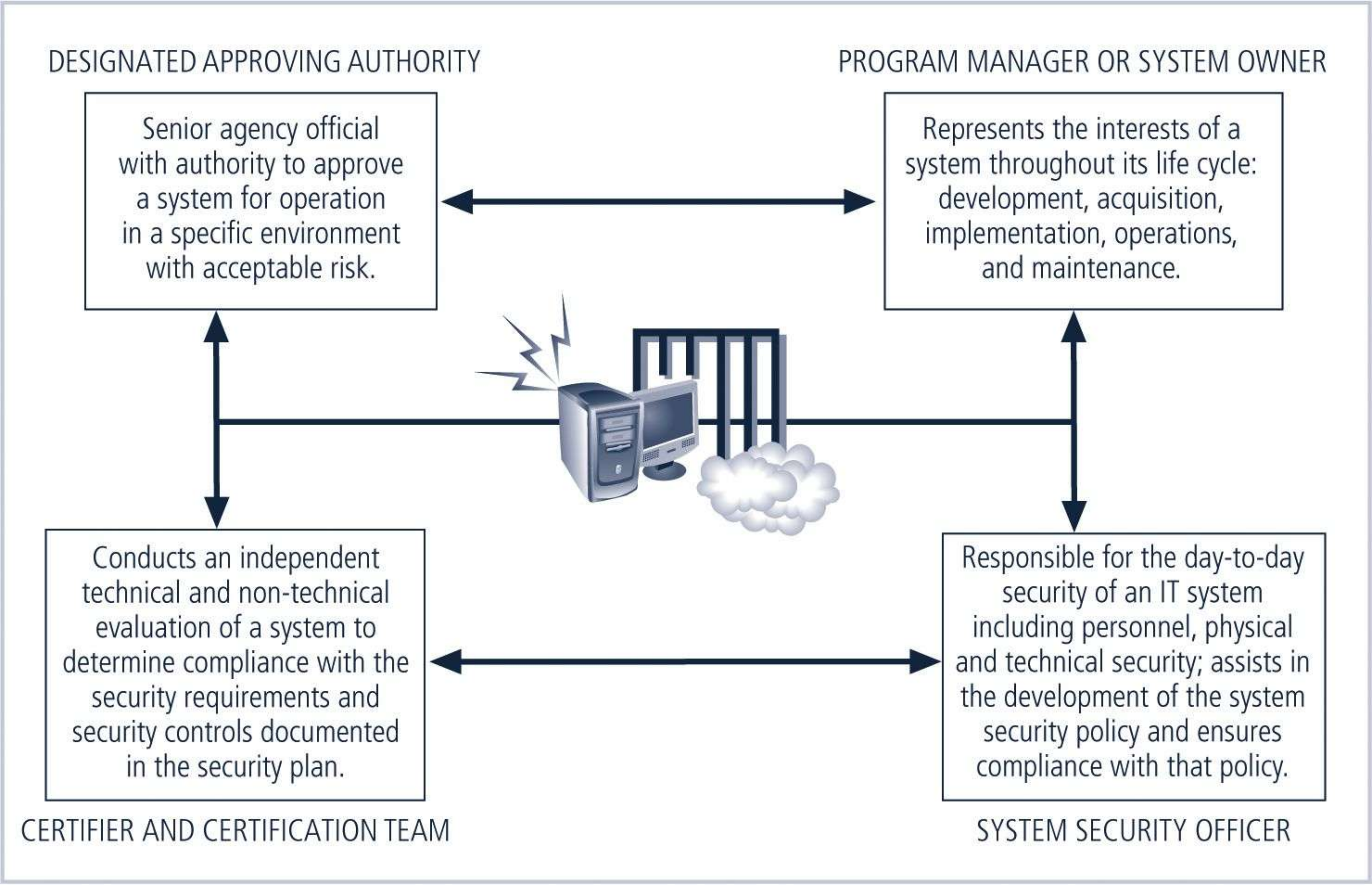
SP 800-53 is part two
of the Certification & Accreditation project

Its purpose is to establish
a set of standardized, minimum security controls
for IT systems
addressing low, moderate, & high levels of concern
for confidentiality, integrity, & availability

Controls are broken into
the 3 familiar general classes of security controls:
management, operational, & technical

Critical elements
represent important security-related
focus areas for the system
with each critical element
addressed by one or more security controls

As technology evolves,
so will the set of security controls,
requiring additional control mechanisms



DESIGNATED APPROVING AUTHORITY

Senior agency official with authority to approve a system for operation in a specific environment with acceptable risk.

PROGRAM MANAGER OR SYSTEM OWNER

Represents the interests of a system throughout its life cycle: development, acquisition, implementation, operations, and maintenance.

CERTIFIER AND CERTIFICATION TEAM

Conducts an independent technical and non-technical evaluation of a system to determine compliance with the security requirements and security controls documented in the security plan.

SYSTEM SECURITY OFFICER

Responsible for the day-to-day security of an IT system including personnel, physical and technical security; assists in the development of the system security policy and ensures compliance with that policy.

FIGURE 6-4 Participants in the Certification and Accreditation Process

Summary

Security Management Models

Security Management Practices

Emerging Trends in Certification & Accreditation

Thank you!

Scott Granneman