Motorola Secure Software Development Model (MSSDM)

Lessons Learned

Francis Mahendran
Larry McCarthy
Margaret Nadworny

August 2007

Biography Information

Director of Security Awareness

- Tools, Processes, and Training for Security

Established Motorola Software Centers

- St. Petersburg, Russia
- Krakow, Poland.
- Both organizations were the first organizations in their respective countries to be assessed at SEI CMM Level 5.

R&D in two of the Motorola Business Units

- Device Simulation
- High Performance Computing

Contact Information: Margaret.Nadworny@motorola.com

Co-Authors and Contributors

Jacob Jacob and Kumar Shiviswamy

both formerly working in the Motorola Software Center in Bangalore, India

Initial work on the capability maturity model

Francis Mahendran

Motorola Software Center in Singapore

Credit for the current model

Members of Motorola Corporate Security Metrics subteam

Review and enhancements

Larry McCarthy

Lead Assessor In Motorola Software Group

Motorola representative to SEI Steering Group

Vision

Make all software delivered by Motorola more secure.

Motorola's Policy Statement

"It is the policy of Motorola to offer security solutions designed to protect the confidentiality, integrity and availability of information and other assets appropriate to their value to Motorola, and to service providers (and their customers) using Motorola products."

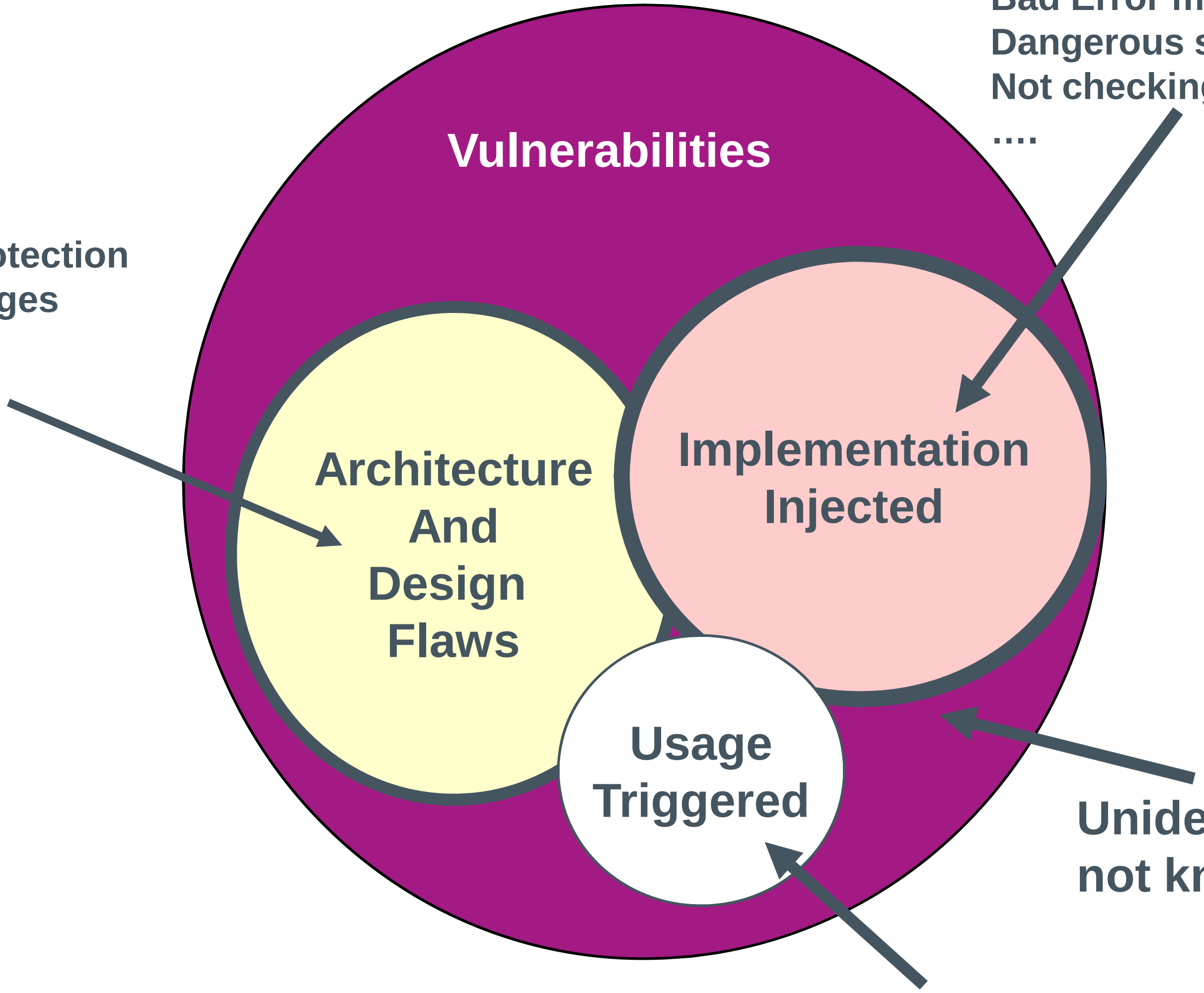
Need for Secure Software

“Time and time again security problems that are encountered come from errors in software.”

-- Terry Stanley, VP Security, Master Card

“Malicious hackers don’t create security holes; they simply exploit them. Security holes and vulnerabilities – the real root cause of the problem – are the result of bad software design and implementation.” -- John Viega & Gary McGraw

Vulnerability Space



Vulnerabilities

Architecture And Design Flaws

Implementation Injected

Usage Triggered

Buffer Overflows
Bad Error messages
Dangerous system calls
Not checking input values
....

No Password protection
Encoding Messages
…

Unidentified List not known

Misuse of privileges

Need for a Secure Software Development Model

Ability to measure maturity of security implementation.

Serves as a reference point to assess current status of an organization and to plan for future process improvements.

Allows the flexibility to choose the area of improvement.

Ability to compliment CMMI and to stand on its own.

Existing Models

ISO 17799©

SSE-CMM©

FAA-iCMM©

IA-CMM©

Current focus is varied, from security controls to identifying and removing security vulnerabilities in the product.

There is a need for a security model focused on software life cycle development. From Security Requirements through Analysis, Design, Implementation and Testing.

Decision to Align with CMMI®

Widely used model in the software industry.

Widely used across Motorola business units.

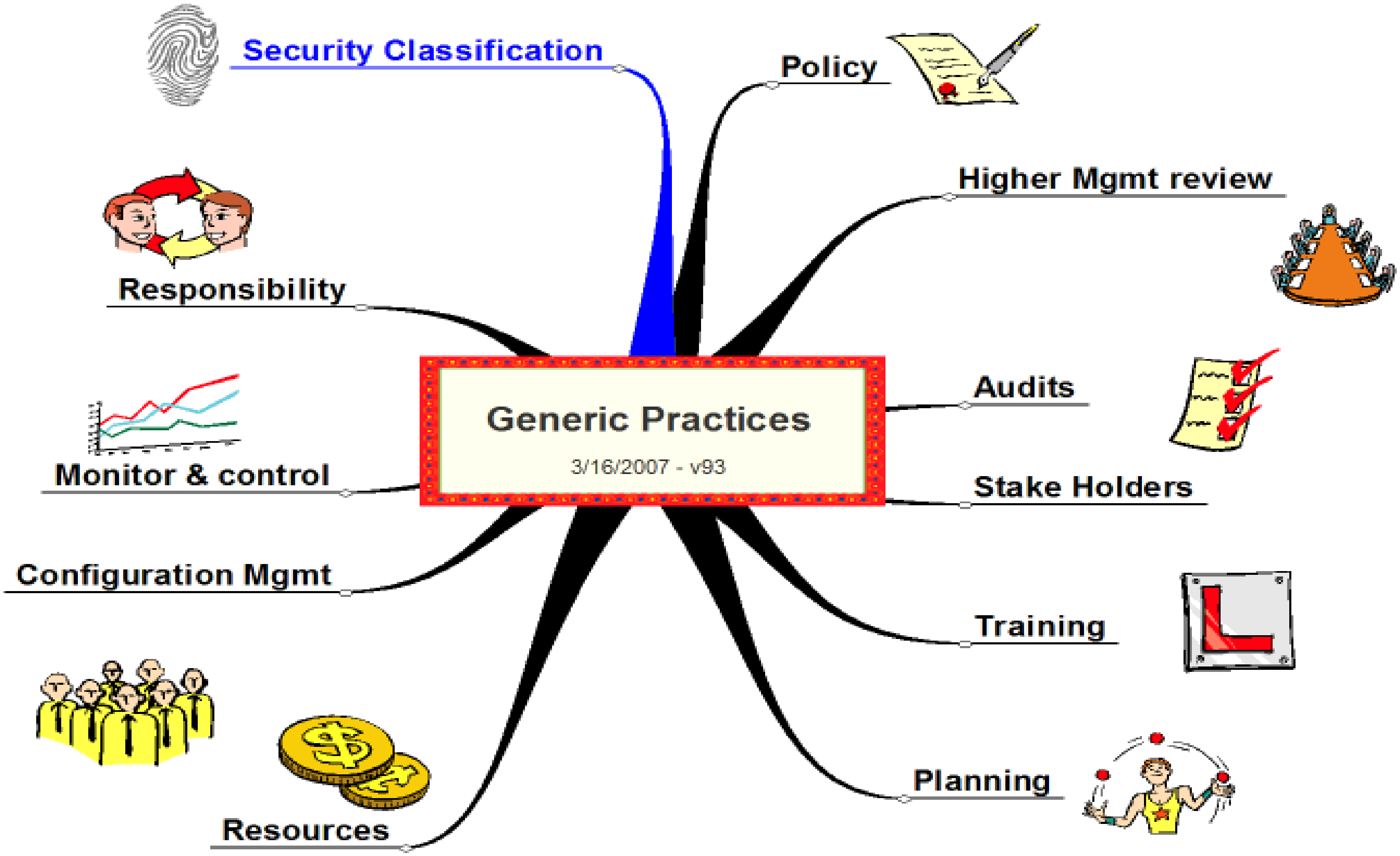
Well understood within Motorola.

Culturally accepted within Motorola Software Group.
- Trying to repeat previous acceptance and adoption.

Motorola Software Group is:
- part of the Corporate Technology Office
- a world wide confederation of software organizations
  - majority assessed at SEI CMM/CMMI L5
- approximately 6500 software developers combined
- a development partner for each of the Motorola Business Units

Motorola Secure Software Development Model – Overview

Generic Practices



Generic Practices

3/16/2007 - v93

Security Classification

Responsibility

Monitor & control

Configuration Mgmt

Resources

Policy

Higher Mgmt review

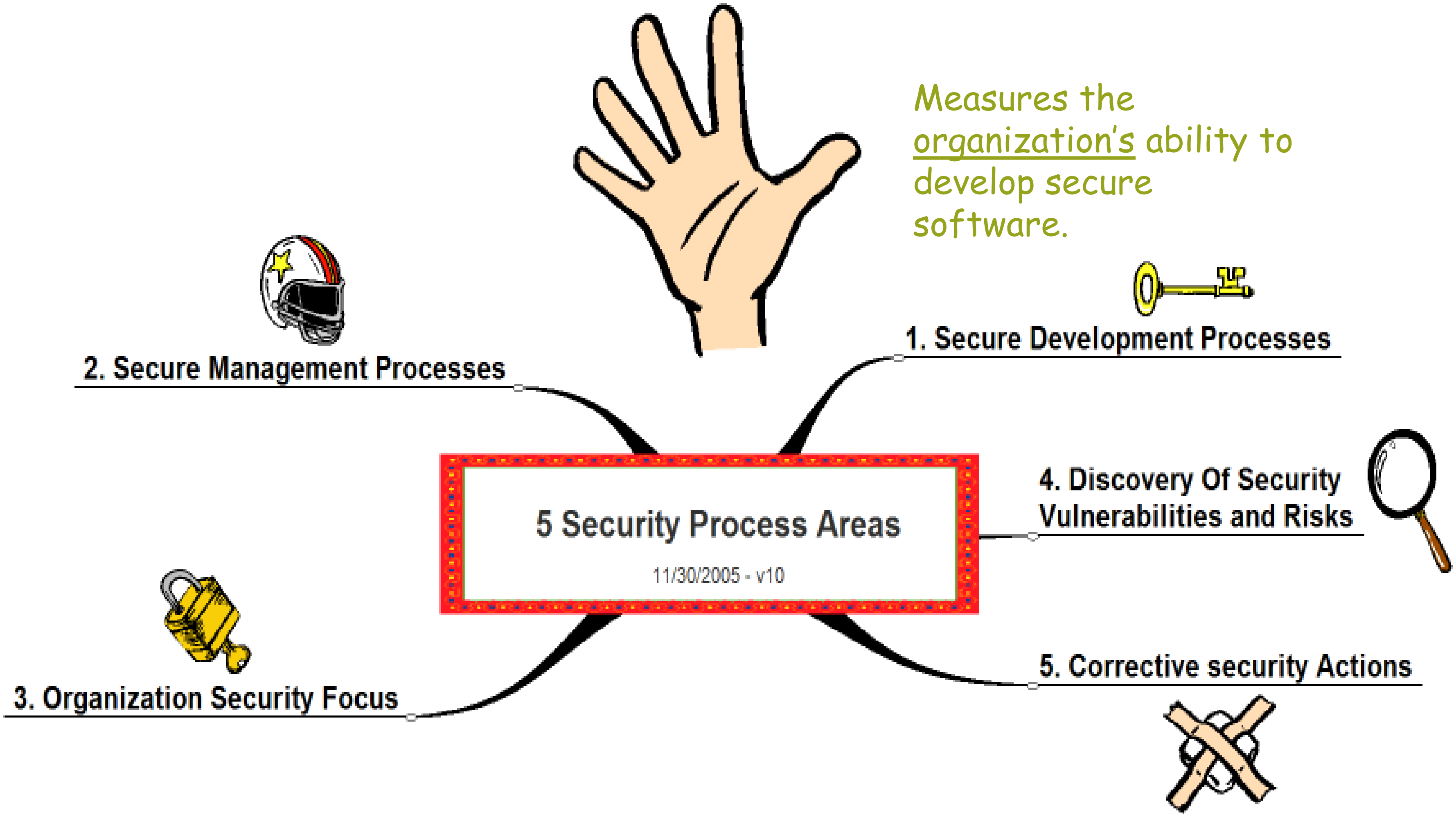
Audits

Stake Holders

Training

Planning

Motorola's Approach – Highlights



Measures the organization's ability to develop secure software.

5 Security Process Areas

11/30/2005 - v10

1. Secure Development Processes

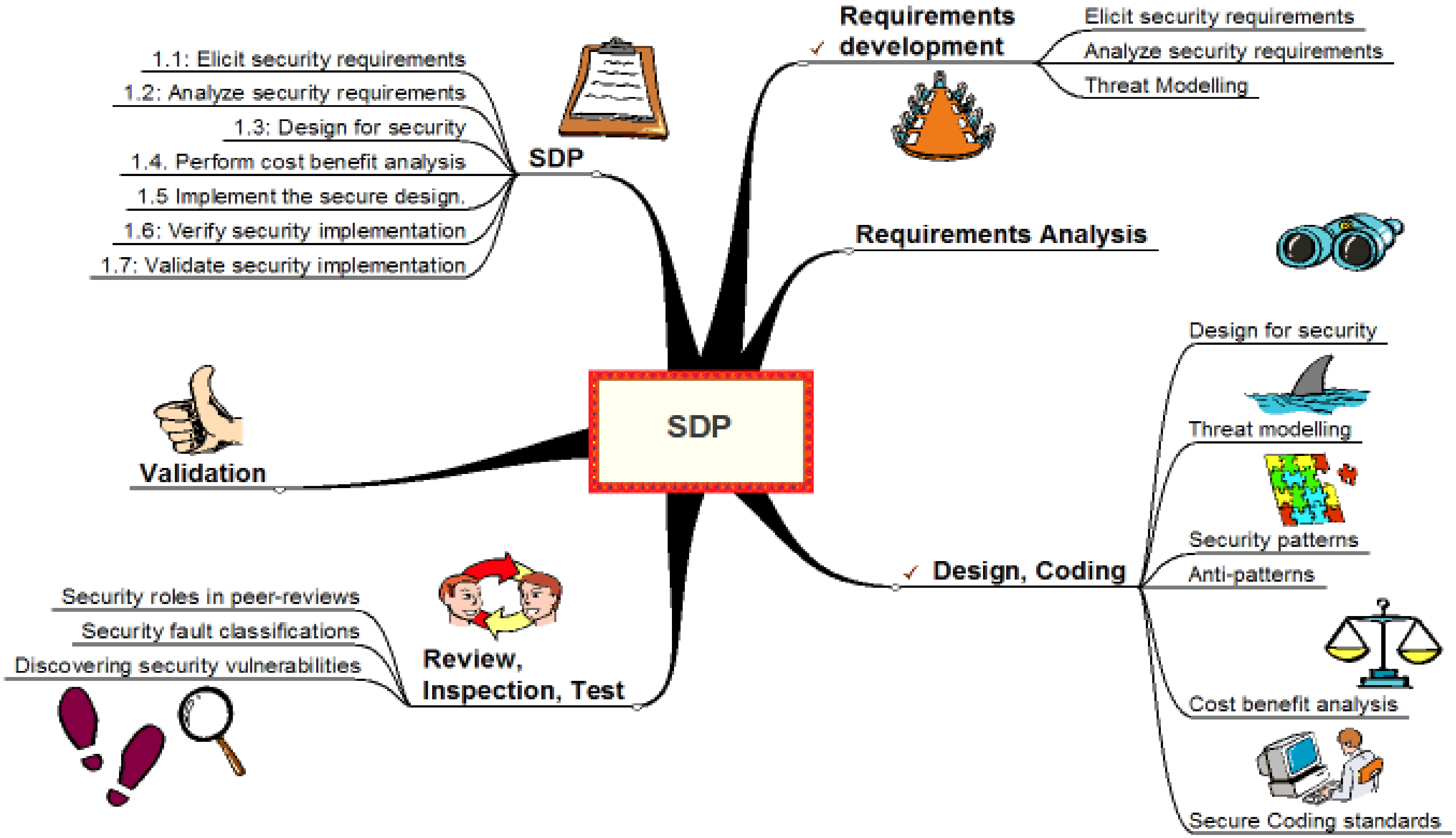
2. Secure Management Processes

3. Organization Security Focus

4. Discovery Of Security Vulnerabilities and Risks

5. Corrective security Actions

PA1: Secure Development Processes (SDP)



SDP

SDP
- 1.1: Elicit security requirements
- 1.2: Analyze security requirements
- 1.3: Design for security
- 1.4. Perform cost benefit analysis
- 1.5 Implement the secure design.
- 1.6: Verify security implementation
- 1.7: Validate security implementation

✓ Requirements development
- Elicit security requirements
- Analyze security requirements
- Threat Modelling

Requirements Analysis

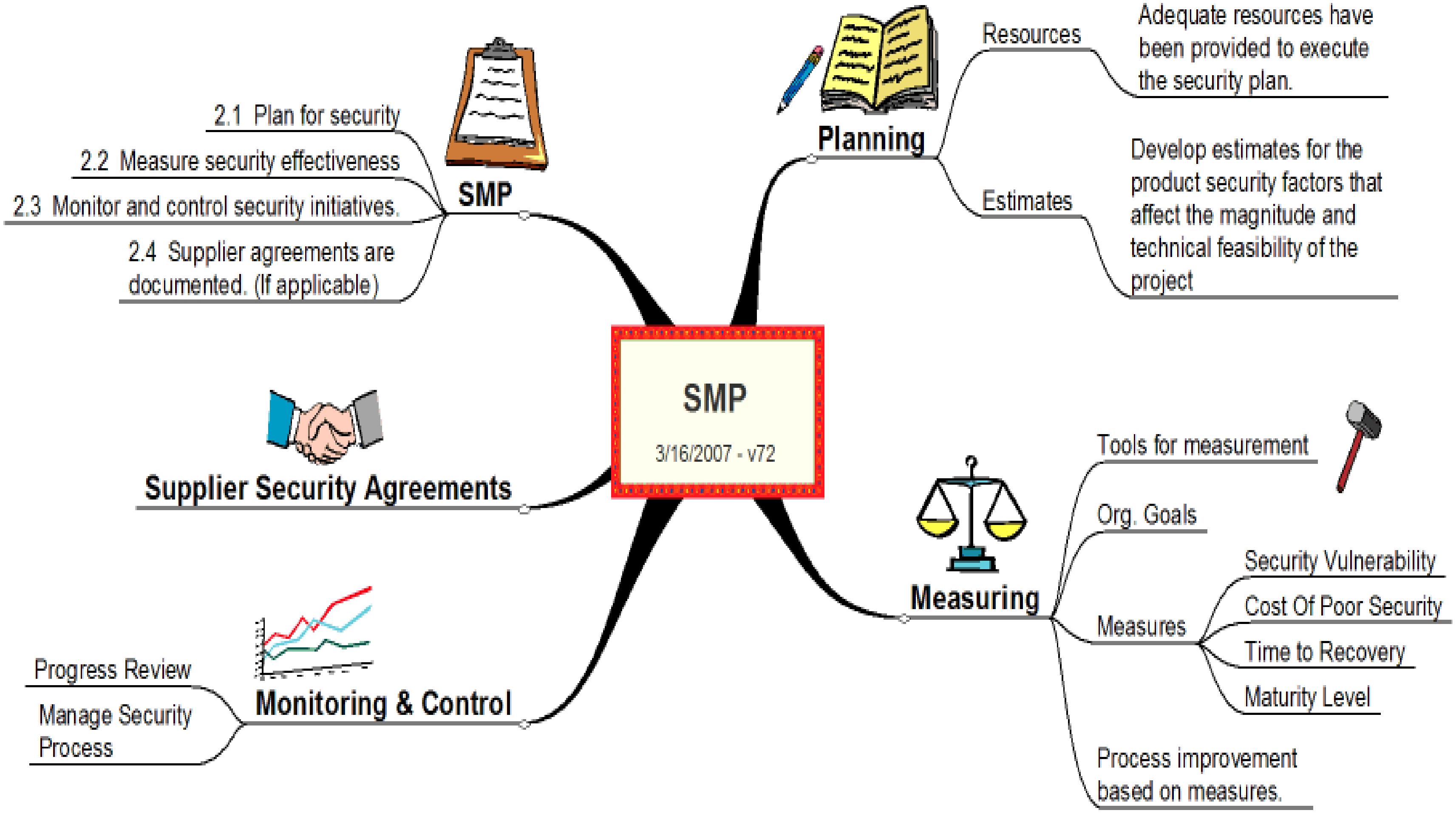
✓ Design, Coding
- Design for security
- Threat modelling
- Security patterns
- Anti-patterns
- Cost benefit analysis
- Secure Coding standards

Validation

Review, Inspection, Test
- Security roles in peer-reviews
- Security fault classifications
- Discovering security vulnerabilities

Motorola Secure Software Development Model   7 August 2007

PA2: Secure Management Processes (SMP)



SMP

3/16/2007 - v72

SMP
- 2.1 Plan for security
- 2.2 Measure security effectiveness
- 2.3 Monitor and control security initiatives.
- 2.4 Supplier agreements are documented. (If applicable)

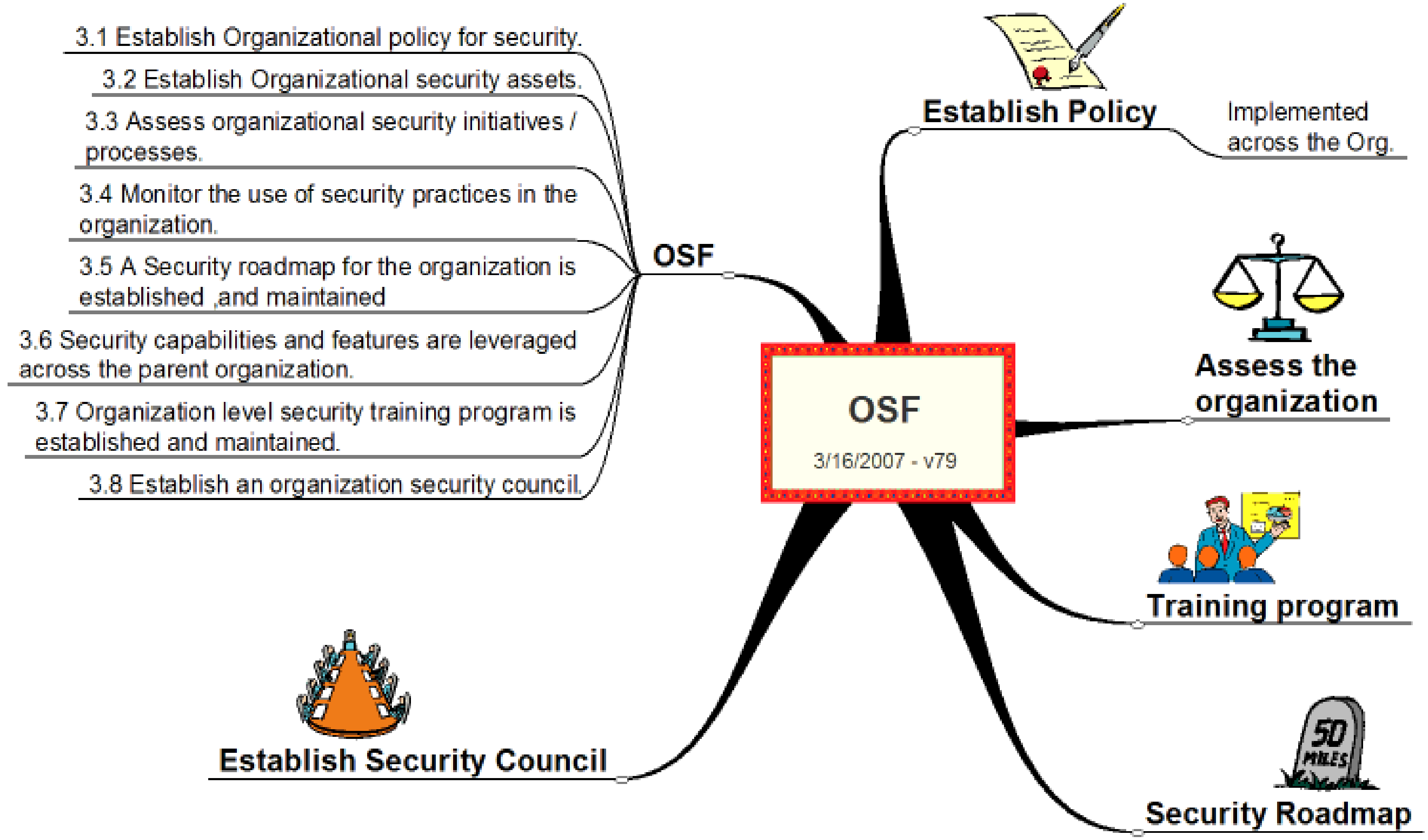
Supplier Security Agreements

Monitoring & Control
- Progress Review
- Manage Security Process

Planning
- Resources
  - Adequate resources have been provided to execute the security plan.
- Estimates
  - Develop estimates for the product security factors that affect the magnitude and technical feasibility of the project

Measuring
- Tools for measurement
- Org. Goals
- Measures
  - Security Vulnerability
  - Cost Of Poor Security
  - Time to Recovery
  - Maturity Level
- Process improvement based on measures.

PA3: Organization Security Focus (OSF)



OSF

3/16/2007 - v79

Establish Policy

Implemented across the Org.

Assess the organization

Training program

Security Roadmap

Establish Security Council

OSF

3.1 Establish Organizational policy for security.

3.2 Establish Organizational security assets.

3.3 Assess organizational security initiatives / processes.

3.4 Monitor the use of security practices in the organization.

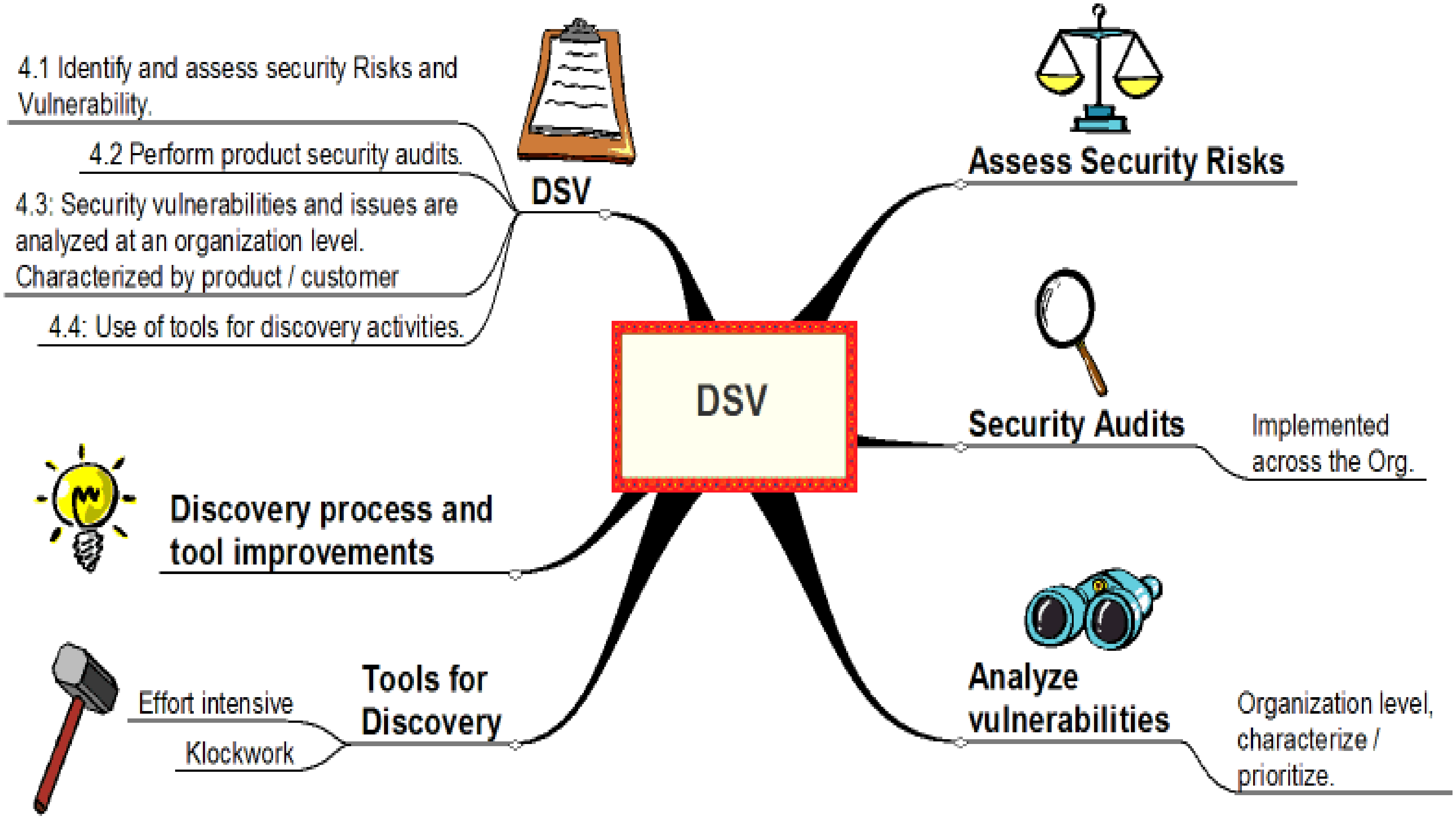
3.5 A Security roadmap for the organization is established ,and maintained

3.6 Security capabilities and features are leveraged across the parent organization.

3.7 Organization level security training program is established and maintained.

3.8 Establish an organization security council.

PA4: Discovery of Security Vulnerability & Risks (DSV)



DSV

DSV

4.1 Identify and assess security Risks and Vulnerability.

4.2 Perform product security audits.

4.3: Security vulnerabilities and issues are analyzed at an organization level. Characterized by product / customer

4.4: Use of tools for discovery activities.

Assess Security Risks

Security Audits

Implemented across the Org.

Analyze vulnerabilities

Organization level, characterize / prioritize.

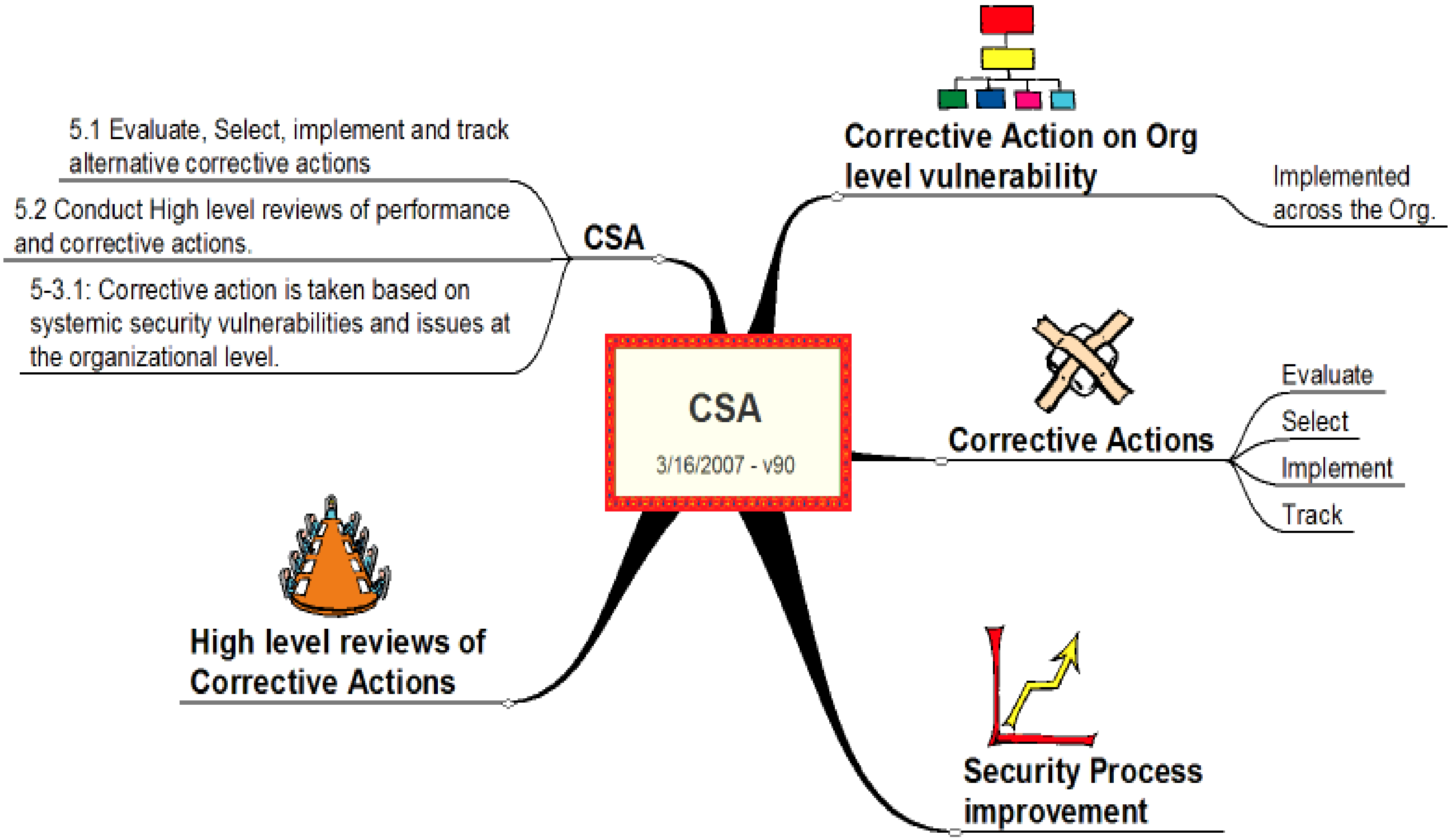
Discovery process and tool improvements

Tools for Discovery

Effort intensive

Klockwork

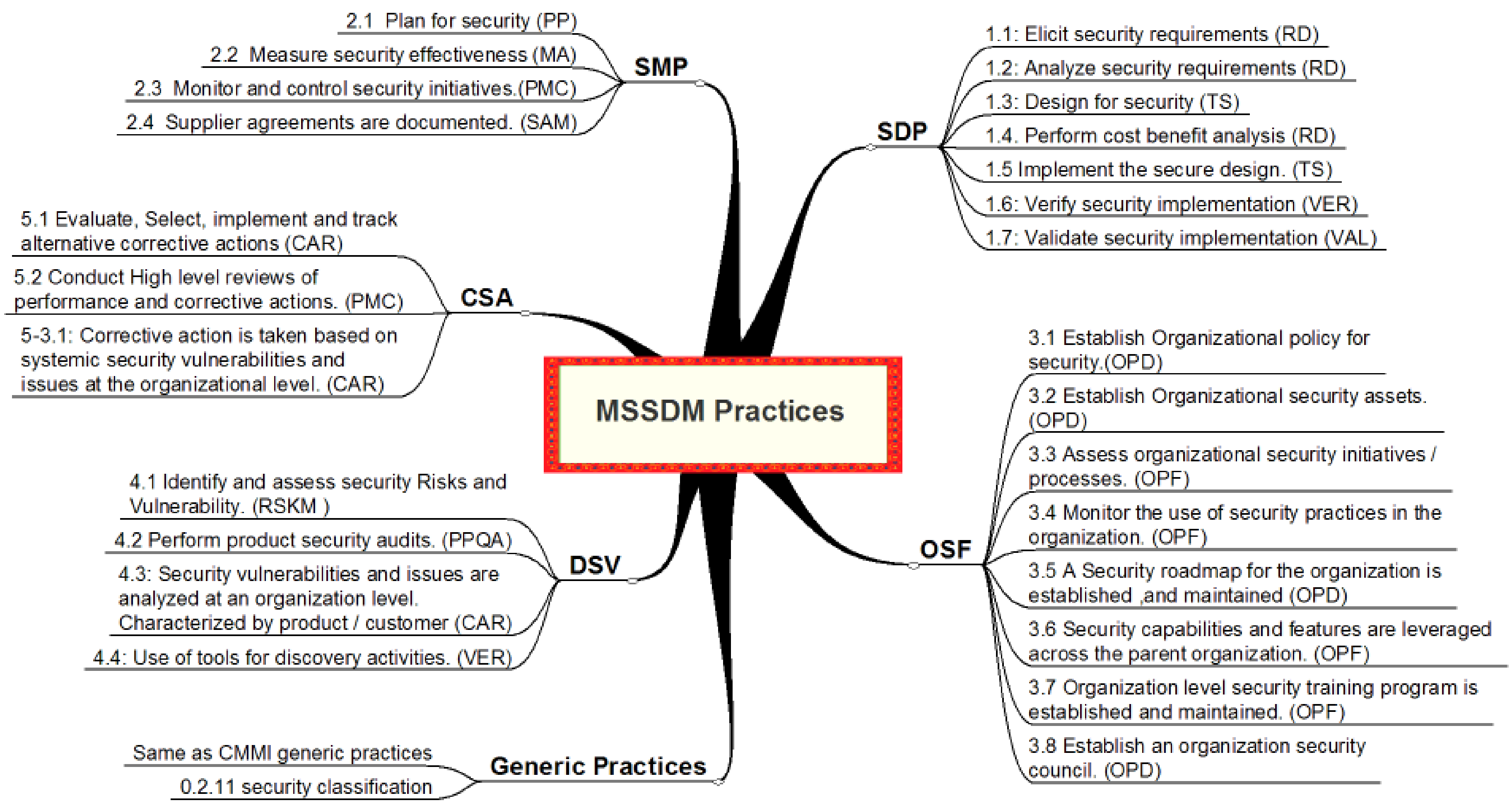
PA5: Corrective Security Actions (CSA)


5.1 Evaluate, Select, implement and track alternative corrective actions
5.2 Conduct High level reviews of performance and corrective actions.
5-3.1: Corrective action is taken based on systemic security vulnerabilities and issues at the organizational level.
CSA
CSA
3/16/2007 - v90
Corrective Action on Org level vulnerability
Implemented across the Org.
Corrective Actions
Evaluate
Select
Implement
Track
High level reviews of Corrective Actions
Security Process improvement

Integrated Appraisal Pilot

MSSDM practices can be aligned with CMMI PA's in a SCAMPI appraisal

Motorola Secure Software Development Model (MSSDM)



MSSDM Practices

SMP

- 2.1 Plan for security (PP)
- 2.2 Measure security effectiveness (MA)
- 2.3 Monitor and control security initiatives.(PMC)
- 2.4 Supplier agreements are documented. (SAM)

SDP

- 1.1: Elicit security requirements (RD)
- 1.2: Analyze security requirements (RD)
- 1.3: Design for security (TS)
- 1.4. Perform cost benefit analysis (RD)
- 1.5 Implement the secure design. (TS)
- 1.6: Verify security implementation (VER)
- 1.7: Validate security implementation (VAL)

CSA

- 5.1 Evaluate, Select, implement and track alternative corrective actions (CAR)
- 5.2 Conduct High level reviews of performance and corrective actions. (PMC)
- 5-3.1: Corrective action is taken based on systemic security vulnerabilities and issues at the organizational level. (CAR)

OSF

- 3.1 Establish Organizational policy for security.(OPD)
- 3.2 Establish Organizational security assets. (OPD)
- 3.3 Assess organizational security initiatives / processes. (OPF)
- 3.4 Monitor the use of security practices in the organization. (OPF)
- 3.5 A Security roadmap for the organization is established ,and maintained (OPD)
- 3.6 Security capabilities and features are leveraged across the parent organization. (OPF)
- 3.7 Organization level security training program is established and maintained. (OPF)
- 3.8 Establish an organization security council. (OPD)

DSV

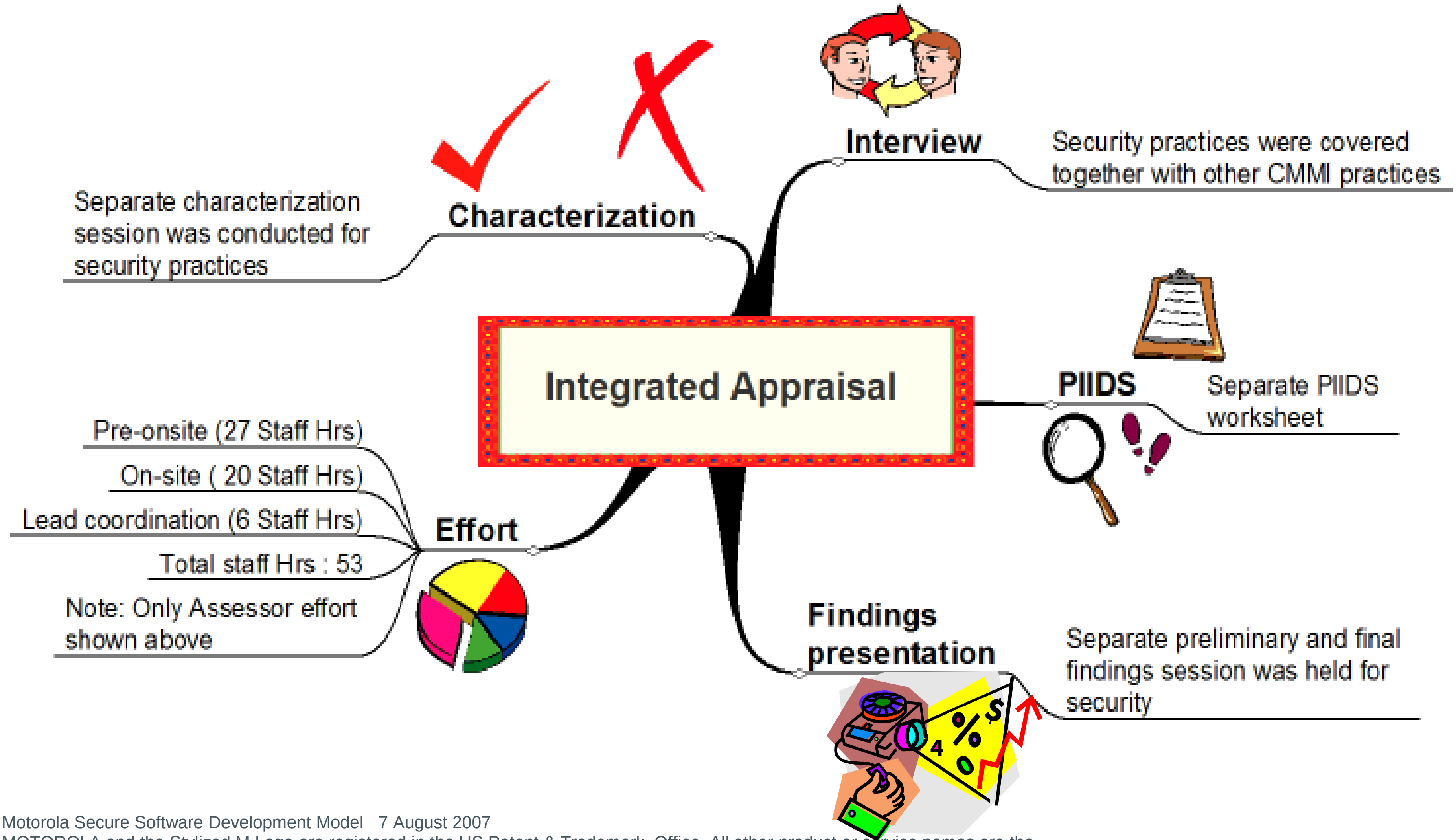
- 4.1 Identify and assess security Risks and Vulnerability. (RSKM)
- 4.2 Perform product security audits. (PPQA)
- 4.3: Security vulnerabilities and issues are analyzed at an organization level. Characterized by product / customer (CAR)
- 4.4: Use of tools for discovery activities. (VER)

Generic Practices

- Same as CMMI generic practices
- 0.2.11 security classification

Integrated Appraisal Pilot

Piloted the integrated appraisal (together with a SCAMPI B) at one of Motorola Software facilities.


Integrated Appraisal
Interview
Security practices were covered together with other CMMI practices
Characterization
Separate characterization session was conducted for security practices
PIIDS
Separate PIIDS worksheet
Effort
Pre-onsite (27 Staff Hrs)
On-site (20 Staff Hrs)
Lead coordination (6 Staff Hrs)
Total staff Hrs : 53
Note: Only Assessor effort shown above
Findings presentation
Separate preliminary and final findings session was held for security
$
%
4
0

Lessons Learned

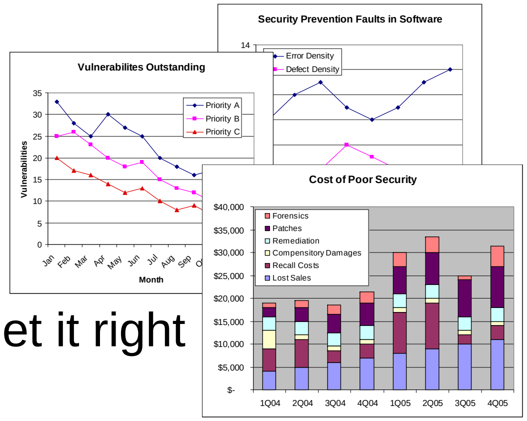
Tools

New and different

e.g. static analysis

Metrics

Relearn – get it right



Coding Standards

More Substantial

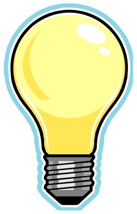
Increasing Demand

Process

All assets are impacted.

More Lessons Learned

Awareness



Practitioners receptive

Training

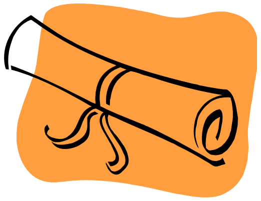
Assessment

Integrate w/CMMI

Optimize Effort/Cost

Policy

Commitment required at all levels



Time for Questions?