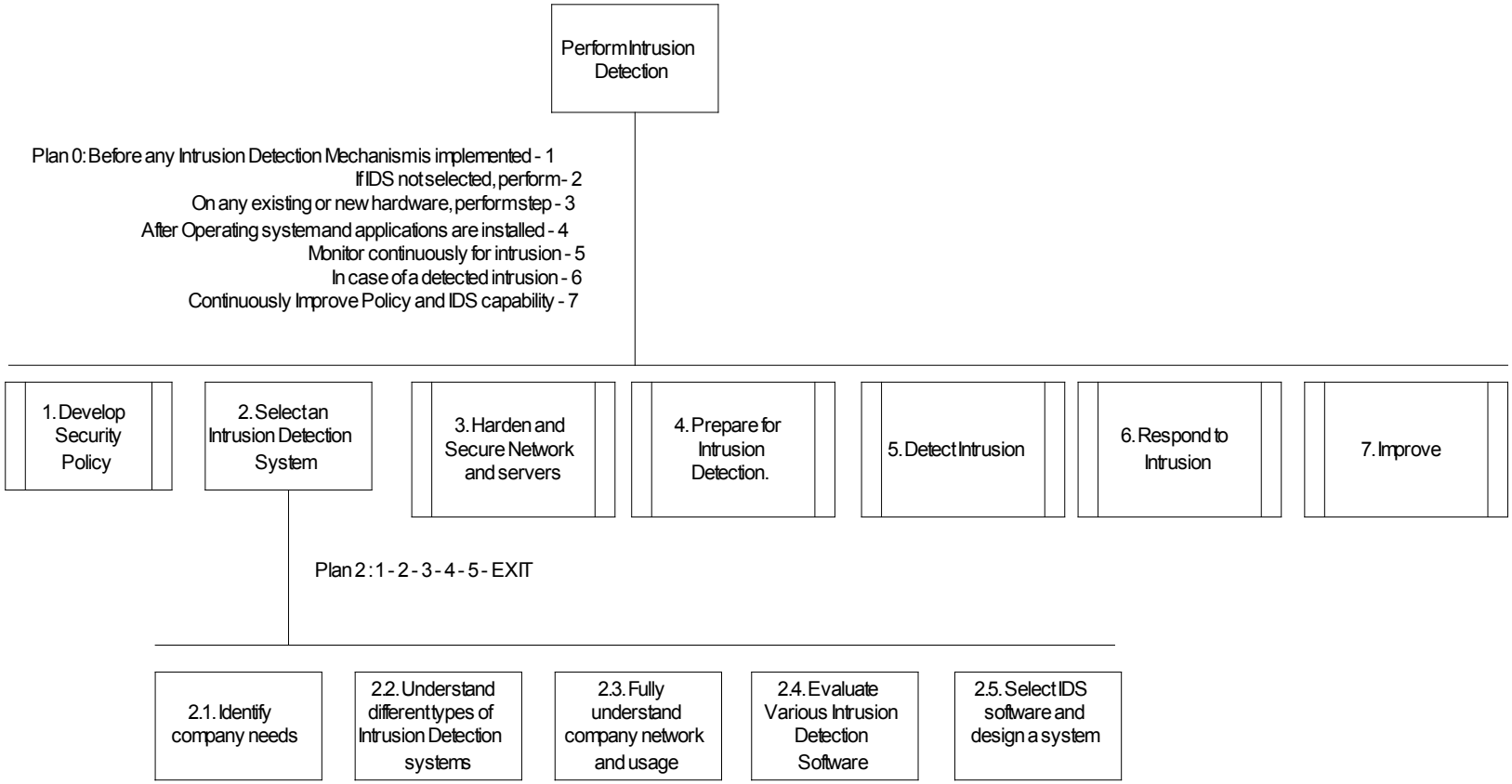
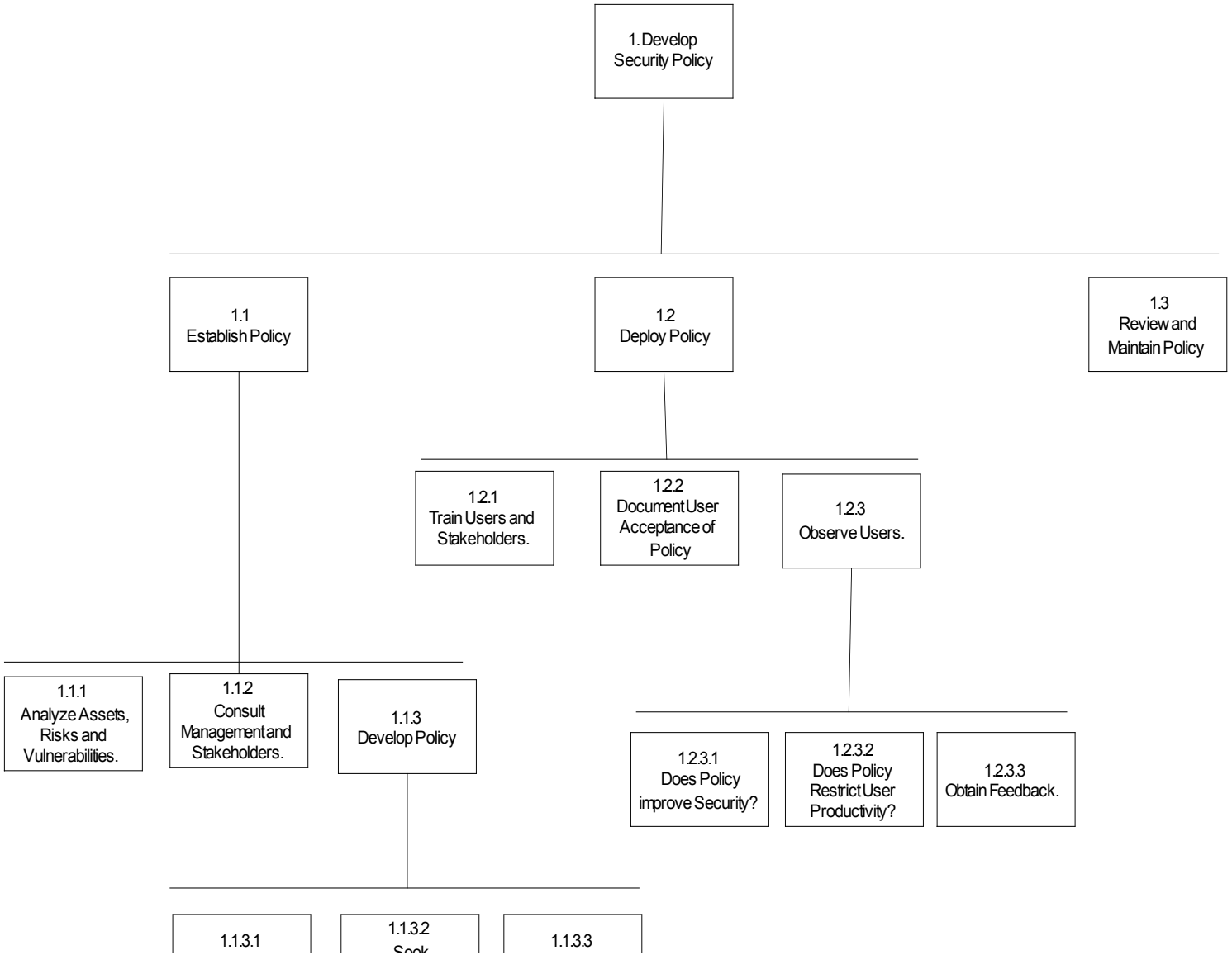
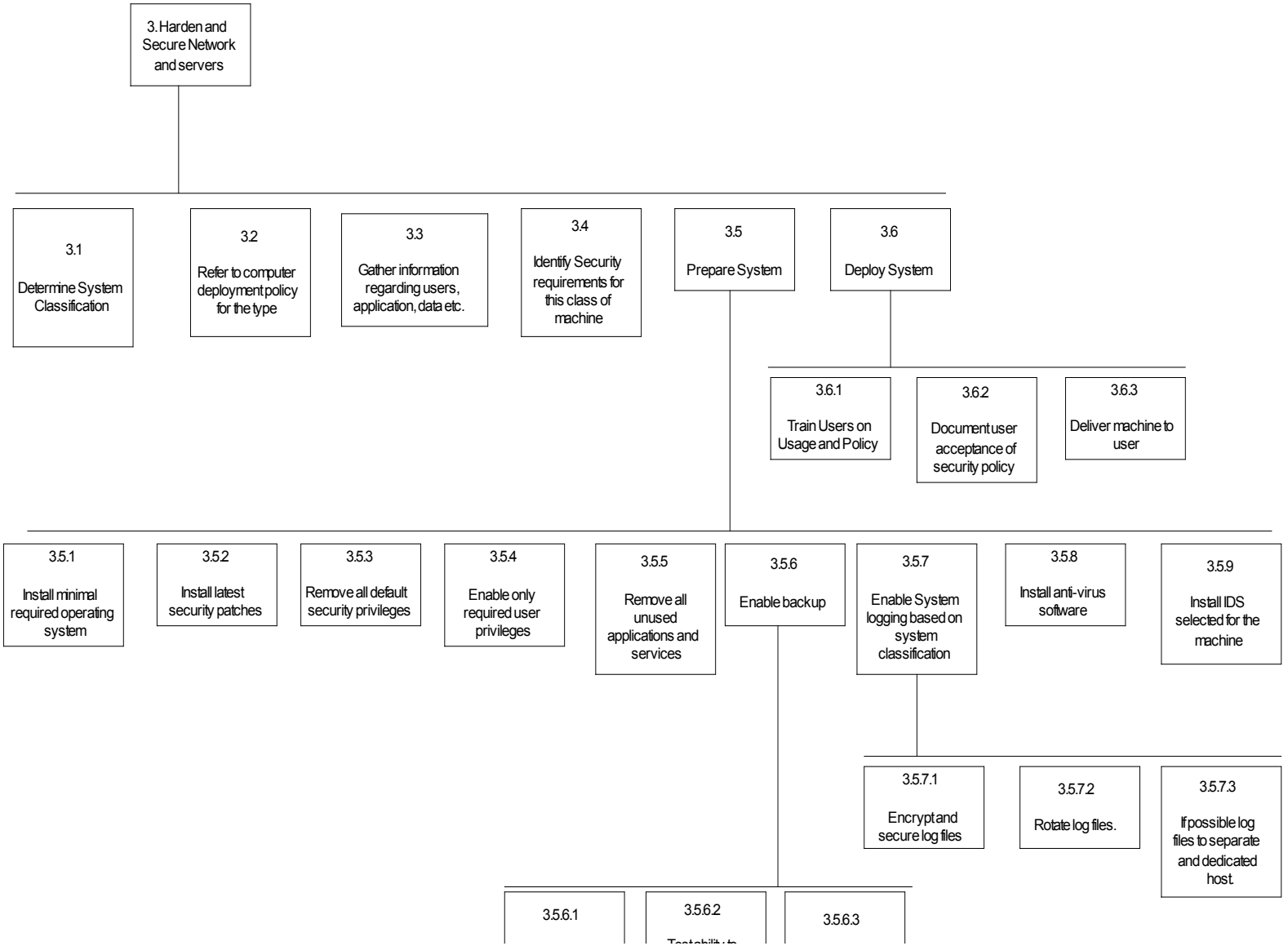
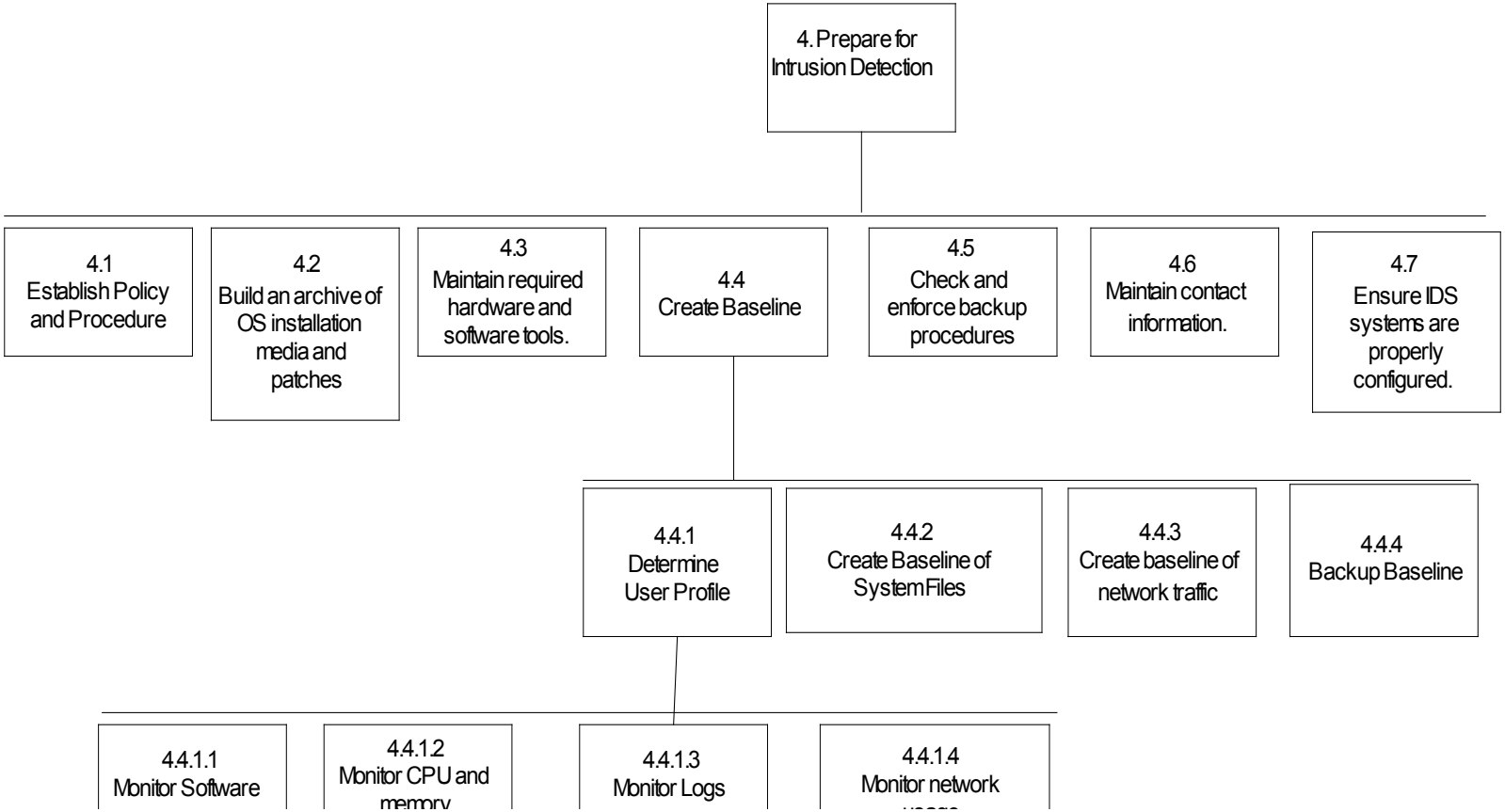
4. DIAGRAMS

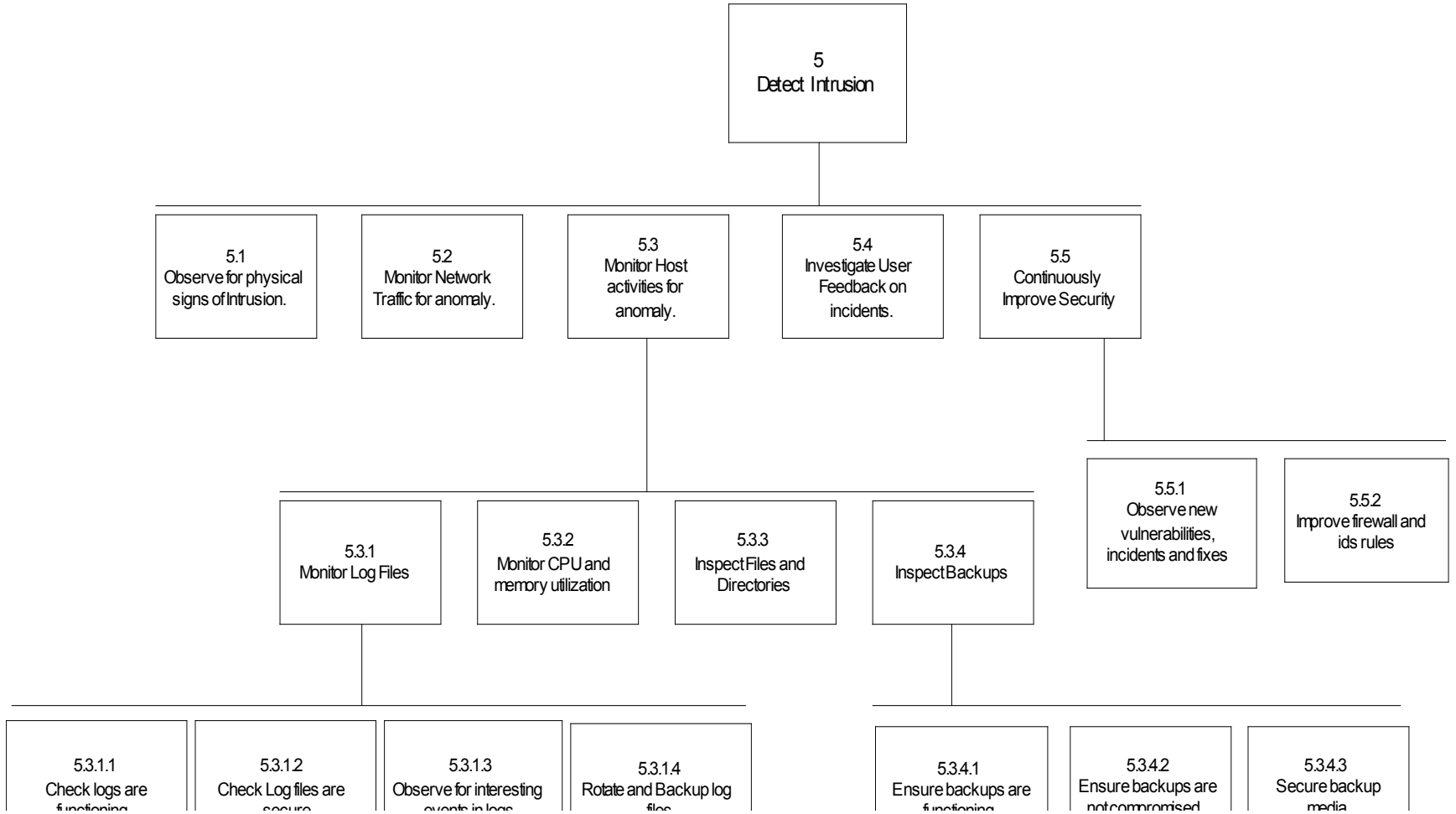

Perform Intrusion Detection
Plan 0: Before any Intrusion Detection Mechanism is implemented - 1
If IDS not selected, perform - 2
On any existing or new hardware, perform step - 3
After Operating system and applications are installed - 4
Monitor continuously for intrusion - 5
In case of a detected intrusion - 6
Continuously Improve Policy and IDS capability - 7
1. Develop Security Policy
2. Select an Intrusion Detection System
3. Harden and Secure Network and servers
4. Prepare for Intrusion Detection.
5. Detect Intrusion
6. Respond to Intrusion
7. Improve
Plan 2 : 1 - 2 - 3 - 4 - 5 - EXIT
2.1. Identify company needs
2.2. Understand different types of Intrusion Detection systems
2.3. Fully understand company network and usage
2.4. Evaluate Various Intrusion Detection Software
2.5. Select IDS software and design a system

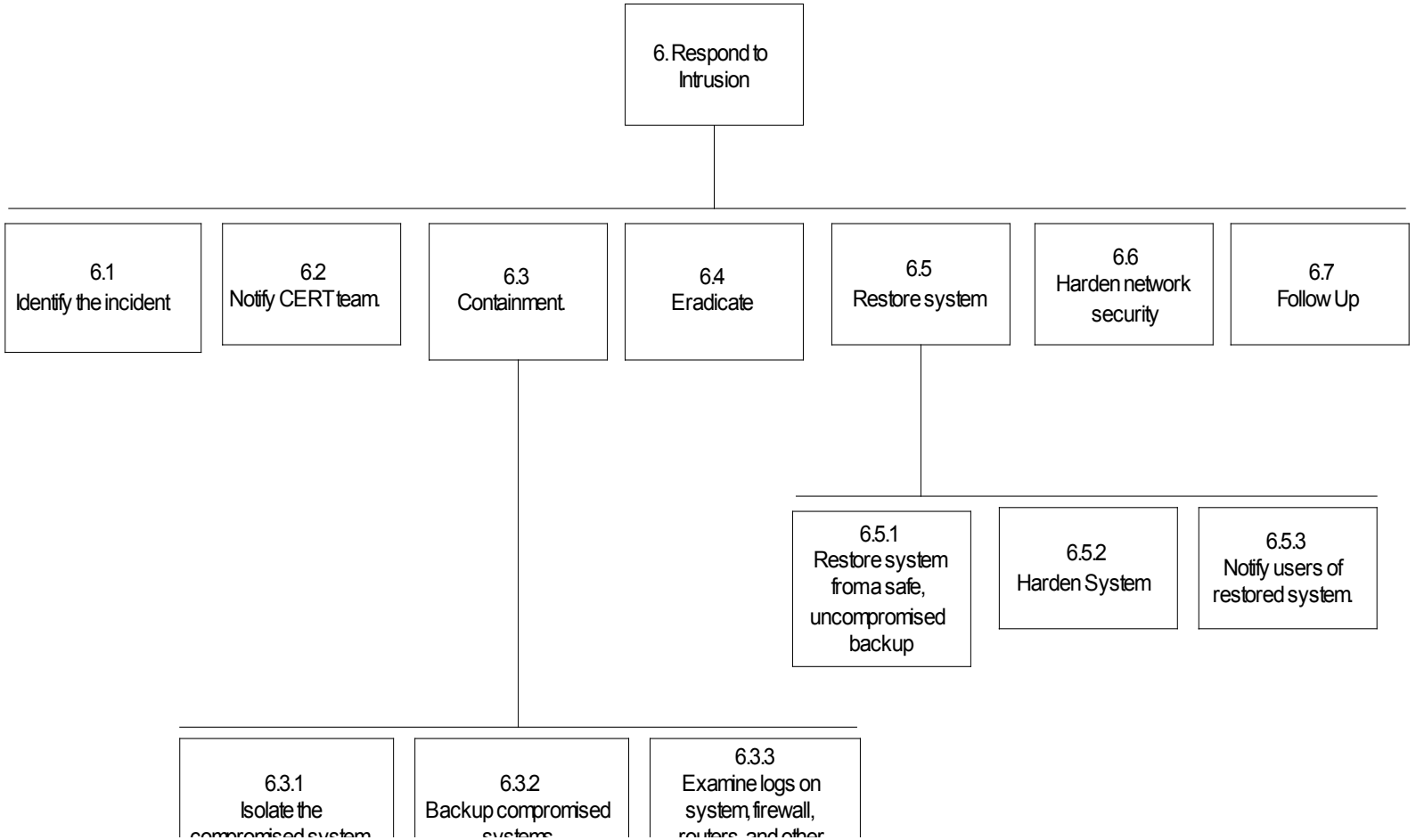
Legend

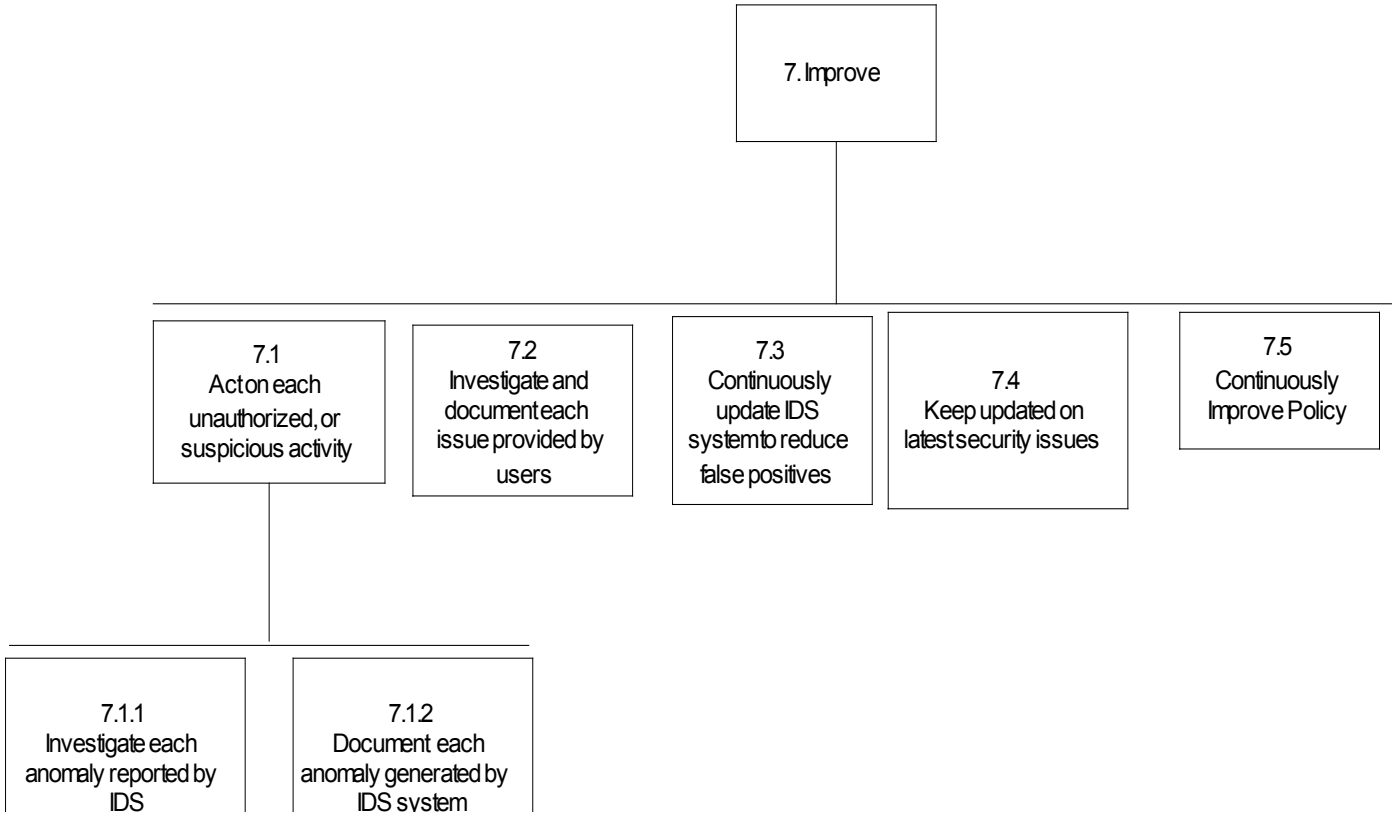

1. Develop Security Policy
1.1 Establish Policy
1.2 Deploy Policy
1.3 Review and Maintain Policy
1.2.1 Train Users and Stakeholders.
1.2.2 Document User Acceptance of Policy
1.2.3 Observe Users.
1.1.1 Analyze Assets, Risks and Vulnerabilities.
1.1.2 Consult Management and Stakeholders.
1.1.3 Develop Policy
1.2.3.1 Does Policy improve Security?
1.2.3.2 Does Policy Restrict User Productivity?
1.2.3.3 Obtain Feedback.
1.1.3.1
1.1.3.2
1.1.3.3


3. Harden and Secure Network and servers
3.1 Determine System Classification
3.2 Refer to computer deployment policy for the type
3.3 Gather information regarding users, application, data etc.
3.4 Identify Security requirements for this class of machine
3.5 Prepare System
3.6 Deploy System
3.6.1 Train Users on Usage and Policy
3.6.2 Document user acceptance of security policy
3.6.3 Deliver machine to user
3.5.1 Install minimal required operating system
3.5.2 Install latest security patches
3.5.3 Remove all default security privileges
3.5.4 Enable only required user privileges
3.5.5 Remove all unused applications and services
3.5.6 Enable backup
3.5.7 Enable System logging based on system classification
3.5.8 Install anti-virus software
3.5.9 Install IDS selected for the machine
3.5.7.1 Encrypt and secure log files
3.5.7.2 Rotate log files.
3.5.7.3 If possible log files to separate and dedicated host.
3.5.6.1
3.5.6.2
3.5.6.3


4. Prepare for Intrusion Detection
4.1 Establish Policy and Procedure
4.2 Build an archive of OS installation media and patches
4.3 Maintain required hardware and software tools.
4.4 Create Baseline
4.5 Check and enforce backup procedures
4.6 Maintain contact information.
4.7 Ensure IDS systems are properly configured.
4.4.1 Determine User Profile
4.4.2 Create Baseline of System Files
4.4.3 Create baseline of network traffic
4.4.4 Backup Baseline
4.4.1.1 Monitor Software
4.4.1.2 Monitor CPU and
4.4.1.3 Monitor Logs
4.4.1.4 Monitor network


5
Detect Intrusion
5.1
Observe for physical signs of Intrusion.
5.2
Monitor Network Traffic for anomaly.
5.3
Monitor Host activities for anomaly.
5.4
Investigate User Feedback on incidents.
5.5
Continuously Improve Security
5.5.1
Observe new vulnerabilities, incidents and fixes
5.5.2
Improve firewall and ids rules
5.3.1
Monitor Log Files
5.3.2
Monitor CPU and memory utilization
5.3.3
Inspect Files and Directories
5.3.4
Inspect Backups
5.3.1.1
Check logs are
5.3.1.2
Check Log files are
5.3.1.3
Observe for interesting
5.3.1.4
Rotate and Backup log
5.3.4.1
Ensure backups are
5.3.4.2
Ensure backups are not compromised
5.3.4.3
Secure backup media


6. Respond to Intrusion
6.1 Identify the incident
6.2 Notify CERT team.
6.3 Containment.
6.4 Eradicate
6.5 Restore system
6.6 Harden network security
6.7 Follow Up
6.5.1 Restore system from a safe, uncompromised backup
6.5.2 Harden System
6.5.3 Notify users of restored system.
6.3.1 Isolate the
6.3.2 Backup compromised
6.3.3 Examine logs on system, firewall,


7. Improve
7.1
Act on each unauthorized, or suspicious activity
7.2
Investigate and document each issue provided by users
7.3
Continuously update IDS system to reduce false positives
7.4
Keep updated on latest security issues
7.5
Continuously Improve Policy
7.1.1
Investigate each anomaly reported by IDS
7.1.2
Document each anomaly generated by IDS system