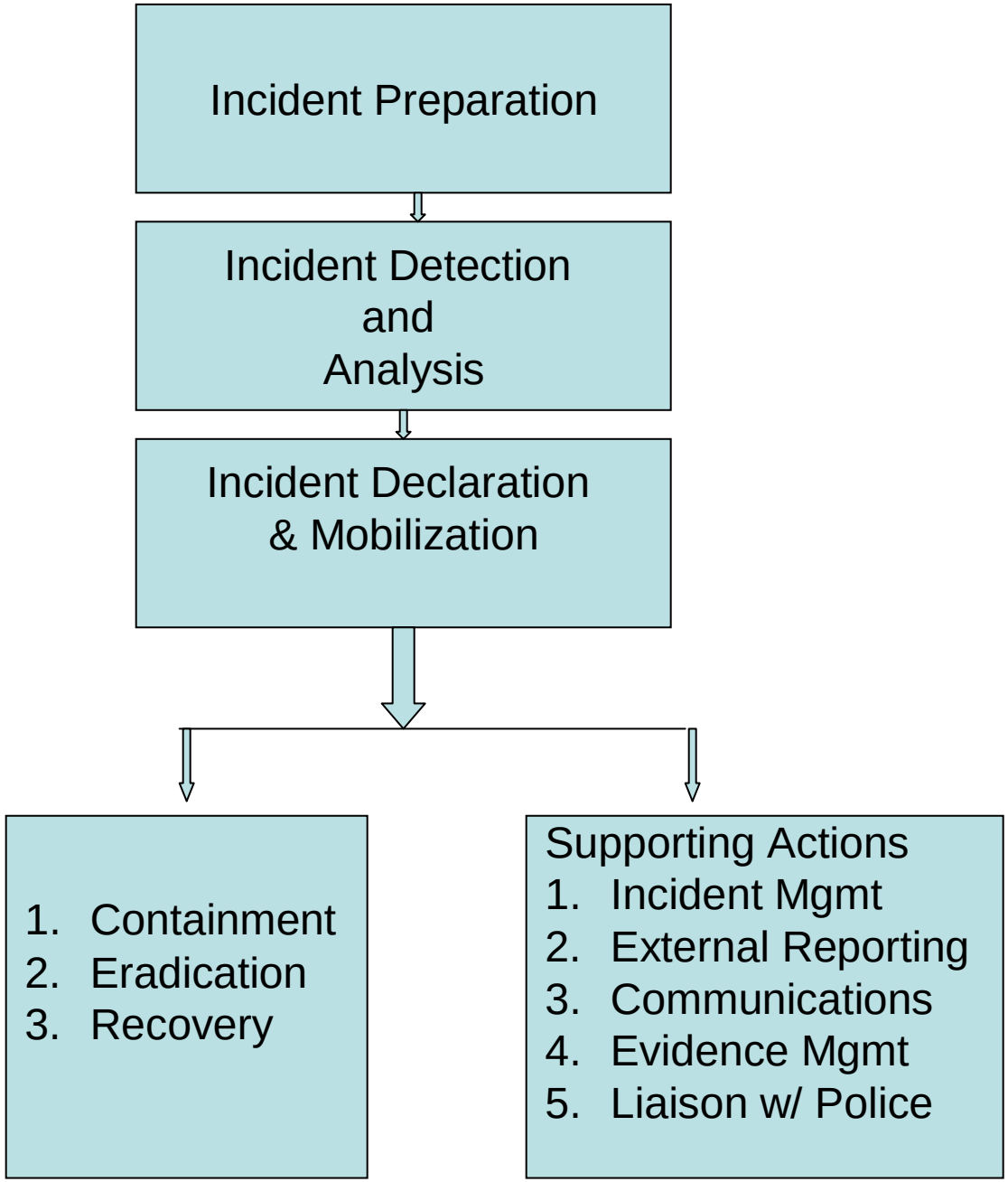
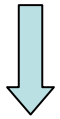

Incident Preparation
Incident Detection and Analysis
Incident Declaration & Mobilization
1. Containment
2. Eradication
3. Recovery
Supporting Actions
1. Incident Mgmt
2. External Reporting
3. Communications
4. Evidence Mgmt
5. Liaison w/ Police

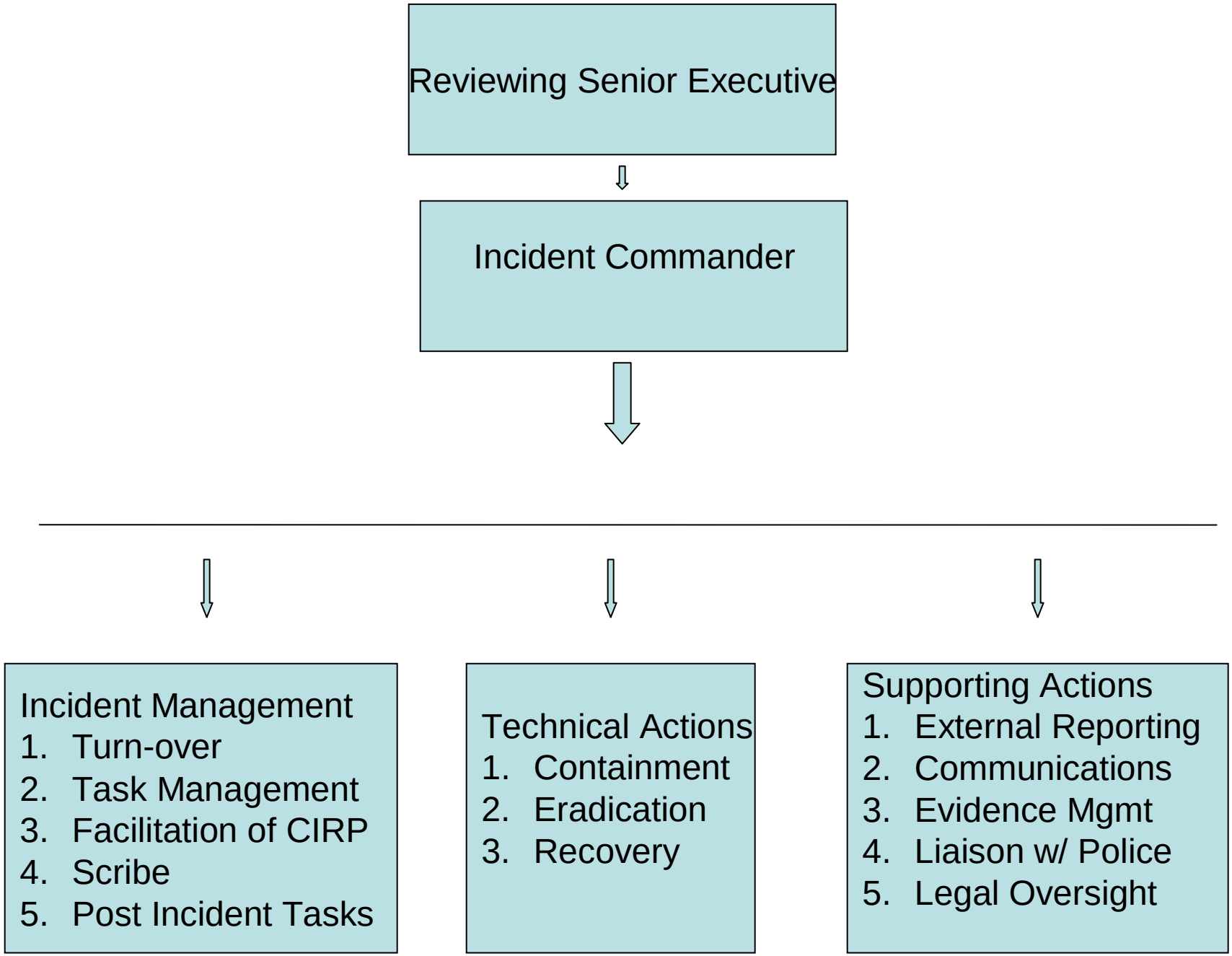


Post Incident

1. Termination
2. Statistics
3. Evidence Retention
4. Lessons Learned

Plan Maintenance

1. Quarterly Updates
2. Annual Testing


Reviewing Senior Executive
Incident Commander
Incident Management
1. Turn-over
2. Task Management
3. Facilitation of CIRP
4. Scribe
5. Post Incident Tasks
Technical Actions
1. Containment
2. Eradication
3. Recovery
Supporting Actions
1. External Reporting
2. Communications
3. Evidence Mgmt
4. Liaison w/ Police
5. Legal Oversight

Hygienic Checklist

- Technology Agnostic
- Confirms scope of breach
  - Affected & non-affected confirmation
- Requirement prior to senior management notification (CEO / BOD)
- May be customized by individuals
  - Add criteria but don’t delete
  - Maintain personal / group copy

Computer Incident Response Plan (CIRP)
Hygienic Checklist

Purpose: The purpose of this checklist is to provide an initial technology-agnostic assessment of a potential system compromise. Completion of this document is required prior to briefing senior management during an incident response.

1. Unusual activity in the access or system logs
2. Recent changes to the system (including processes)
3. New user or Super User ID's created
4. Deleted log files
5. Deleted or altered system files
6. Recent Super User activity
7. Past escalation of privileges
8. Recent off-hour activity
9. Recent file transfers from the system