Incident Scene
Assign ID to the scene • Incident environment protection • ID and possible sources of evidence • Collect evidence • Avoid or minimize evidence contamination
Locard's Exchange Principle
In a crime the suspected person leaves something and takes something. The leftovers can be used to identify the suspect.

Live Evidence
Primary Evidence
- Most reliable and used by trial
- Original document - Eg: Legal contracts
- No copies or duplicates
Secondary Evidence
- Less powerful and reliable than primary evidence
- Eg. Copies of originals, witness oral evidence
- If primary evidence is available secondary of the same context is not valid.
Direct Evidence
Can prove without a backup support • Eg. witness testimony by his/her own 5 senses.
Conclusive Evidence
- Cannot contradict, conditional evidence, no other supportive evidence requires
- Cannot be used to directly prove a fact
Corroborative Evidence
- Used as substitute for other evidence
Hearsay Evidence
- Something heard by the witness where another person told

Asset Management
Preserve Availability • Authorization and Integrity • Redundancy and Fault Tolerance • Network-based IDS
Direct Evidence Can prove without a backup support.

Other recovery
- Prevention
- Intrusion Detection System (IDS) • Preparing to fail
- Firewalls
- IDS (Intrusion Detection System) Automated inspection of logs and real-time system events to detect intrusion attempts and system failures. KPIs are an effective method of detecting many DoS and DDoS attacks.
- IPS (Intrusion Prevention System) A IDS with additional capabilities to stop intrusions.

Firewalls
Monitor and analyze the intrinsics of a computing system, including its network connections points. Eg. Mainframe computer.

HIDS (Host-based IDS)
Monitor and analyze network activity specifically scanning for malicious activities and policy violations.

NIDS (Network-based IDS) Hardware based device or software applications used to monitor and analyze network activity, specifically scanning for malicious activities and policy violations.

Hierarchical Recovery Types of System Failure

Types of System Failure
1. Critical
2. Essential
3. Critical

Intrusion Detection and Prevention Systems (IDS & IPS)
IDS (Intrusion Detection System)
Automated inspection of logs and real-time system events to detect intrusion attempts and system failures. KPIs are an effective method of detecting many DoS and DDoS attacks.

IPS (Intrusion Prevention System) A IDS with additional capabilities to stop intrusions.

Direct Evidence
- Evidence collected by evidence retention method

Characteristics of Evidence
- Validity: Can be accepted.
- Relevance: Reasonable facts, with proof of crimes, acts and methods used, event documentation
- Permissibility: Evidence obtained lawfully

Interviewing and Interrogation
Interviewing
Collects facts to determine matters of the incident.
Interrogation
- The Process: Prepare questions and topics, summarize information
- Opinion Rule: Witnesses test only the facts of the case, not used as evidence.

Governing Laws
- Common Law - USA, UK, Australia, Canada
- Civil Law - Europe, South America
- Islamic and other Religious laws - Middle East, Africa, Indonesia, USA

Lawful law: Statutory law - Make the laws
- Executive: Administrative law - Enforce the laws
- Judicial: Interpret the laws

Categorization of Evidence
- Criminal law: Laws in force in the USA or another country which result in a damage or loss, result in financial penalities.
- Administrative: Regulatory law - how the industries, organizations and officers should act. Punishments can be imprisonment or financial penalities

Uniform Computer Information
Common framework for the conduct of computer related business transactions. A federal law. Use of software licensing

Computer Crime Laws
- Unauthorized intrusion
- Unauthorized alteration or destruction
- Malicious code

Admissible Evidence
- Relevant, sufficient, reliable, does not have to be tangible

Evidence Evaluation
- The legal system: To prove facts.

Evidence Lifecycle
1. Discovery
2. Protection
3. Relevant
4. Probative
5. Reasonable
6. Permissible
7. Evidence obtained lawfully

Digital Evidence
Six principles to guide digital evidence technicians
- All general forensic and procedural principles apply.
- Upon seizure, all actions should not change the data
- All people accessing the data should be trained
- All actions performed on the data should be fully documented and accessible
- Anyone that possesses evidence is responsible for all actions taken with it while in their possession.
- Any agency that possesses evidence is in responsible for compliance with these principles.

Digital Forensics
Five rules of evidence
- Be authentic • Be accurate • Be complete
- Be convincing • Admissible

Security Incident and Event Management (SIEM)
Log review automating real-time analysis of events occurring on systems

Record Event Data 
Transaction Redundancy Implementations
Electronic Vaulting • Remote Journaling • Database shadowing

System Hardening
- Unsuccessful unauthorized actions • Disable unnecessary services
- Deny unneeded ports • External storage device restrictions
- Monitoring and Reporting • Vulnerability Management System
- KPI/IP: Attack signature engine should be updated regularly

Disaster Recovery Methods
Cold Site
An alternative workspace with power and HVAC setup, but no hardware. All recovery efforts will be technician heavy

RAID, SAN, & NAS
RAID Redundant Array of Independent / Inexpensive Disks
- RAID 0: Parallel data access across multiple devices where as data is written twice, doubles up on storage requirements
- RAID 1: Mirror data across devices simultaneously provides high data integrity
- RAID 5: Block data striping across multiple drives and parity information
- RAID 6: Expensive
- RAID 10 (RAID 5 + RAID 0)
- RAID 1 (RAID 0 + RAID 1) Stripes data across multiple drives and mirrors to a separate set of disks

Streets data across available drives and mirrors to a separate set of disks

Business Continuity Planning
MTTF: Mean Time To Failure
MTTR: Mean Time To Repair
MTBF: Mean Time Between Failures
Transaction Redundancy Implementations
Electronic Vaulting • Remote Journaling • Database shadowing

Disaster Recovery Methodology
Shadowing (CI)
Review of as many components, assemblies, and systems as possible to identify potential failure modes.

Root Cause Analysis (RCA)
Fault tree analysis (FTA)
Fault mode and effects analysis (FMEA)

Pareto Analysis
- The 80/20 rule
- The 20% of the cause is 80% of the problem

Causation
- Connects individual cause-and-effect relationships to insights into the system of causes within an issue

Disaster Recovery Terminology & Concepts
Business Continuity Plan (BCP)
Concerns the preservation and recovery of business in the event of natural disasters or forces beyond normal business operations.

Disaster Recovery Plan (DRP)
A framework of steps and actions that need to be taken to achieve business continuity and disaster recovery goals.
- End Goal – Return to normal operations and development or management is complete.
- Plan approval and implementation - management approval

Costs
Benefits
Risk
A framework of steps and actions that need to be taken to achieve business continuity and disaster recovery goals.

Business Continuity Steps
1. Scope and plan initiation
2. BA: assess impact of disruptive processes
3. Business Continuity Plan development - Use BIA to develop BCP

Cybersecurity
- System Recovery
- After a failure of operating system or application, the system should be restored
- All enough to have the system secure

Trusted Recovery
- Breach Confirmation
- Confirm secure breach not happen during system failure
- Failure Prevention
- Backup critical information to enable recovery
- System Recovery
- After a failure of operating system or application, the system should be restored
- All enough to have the system secure

BSCP Plan Development
1. Scope and plan initiation
2. BA: assess impact of disruptive processes
3. Business Continuity Plan development - Use BIA to develop BCP

Testing
- Plan approval and implementation - management approval

Business Continuity Plan (BCP)
Concerns the preservation and recovery of business in the event of natural disasters or forces beyond normal business operations.

Disaster Recovery Plan (DRP)
A framework of steps and actions that need to be taken to achieve business continuity and disaster recovery goals.
- End Goal – Return to normal operations and development or management is complete.
- Plan approval and implementation - management approval

Trusted Recovery
- Breach Confirmation
- Confirm secure breach not happen during system failure
- Failure Prevention
- Backup critical information to enable recovery
- System Recovery
- After a failure of operating system or application, the system should be restored
- All enough to have the system secure

BSCP Plan Development
1. Scope and plan initiation
2. BA: assess impact of disruptive processes
3. Business Continuity Plan development - Use BIA to develop BCP

Testing
- Plan approval and implementation - management approval

Business Continuity Planning
Version: state of the CI, Configuration - collection of component that makes another CI Building Asset Management with component 0's build list

Antifacts
Recorvery procedures. Eg. system reset. Should be accessed by unauthorized users from authorized terminals.