Root of Trust (Trust Source)

A trusted third party or component that ensures a new connection or system is secure and real.

Examples:

- **HSM (Hardware Security Module):** A physical device that safely stores encryption keys, certificates, and passwords.
- **TPM (Trusted Platform Module):** A built-in security chip that protects against brute force attacks. It can work with full disk encryption (FDE).
- **Secure Enclave (iOS):** A special part of the processor that keeps user data safe, even if the main system is hacked. It also creates random numbers and stores cryptographic keys.
- **CA (Certificate Authority):** Issues SSL/TLS certificates to verify website identity.

Access Control Types:

- **RBAC (Role-Based Access Control):** Different roles have different access rights (e.g., IT vs. Management).
- **Discretionary Access Control:** The file owner decides who can access it.
- **Mandatory Access Control:** Different files and users have security levels (Public, Private, Secret).
- **Rule-Based Access Control:** Access is allowed only under certain conditions (e.g., specific time or browser).

Email Anti-Spoofing:

- **DMARC:** Uses SPF and DKIM to disposition if an email goes to spam.

- **SPF:** Checks if the email comes from an approved server.
- **DKIM:** Ensures the email was not changed. It digitally signs emails so recipients can verify authenticity.

Network Access Control (NAC):

A security system that checks if a device meets security requirements before allowing internet access (e.g., firewall settings or OS updates).

Disaster Recovery Terms:

- **RPO (Recovery Point Objective):** Defines how much data loss is acceptable.
- **RTO (Recovery Time Objective):** Defines how long it takes to restore service.

Security Tools:

- **SIEM (Security Information and Event Management):** Collects and analyzes security logs.
- **IPSec:** Used for VPN security.
- **Escalation Scripting:** Automates incident response.

Security Documents:

- **Statement of Work:** Defines tasks in a project.
- **SLA (Service Level Agreement):** Defines minimum service guarantees (e.g., 99% uptime).
- **Data Retention Policy:** Defines how long data must be stored.
- **Due Care:** Ensuring proper security measures are in place (e.g., penetration testing).

Risk Management:

- **Accept:** The business decides to live with the risk.
- **Transfer:** The risk is moved to another entity (e.g., insurance).
- **Avoid:** Disconnect from the internet to remove risk.
- **Tolerate:** Acceptable level of risk.
- **Mitigate:** Reduce risk (e.g., offline backups for ransomware).

Other Security Terms:

- **Shadow IT:** Using personal cloud services (e.g., Google Drive) for company data.
- **Quarantine (Antivirus):** Isolating infected files.
- **IPS (Intrusion Prevention System):** Blocks known threats.
- **Fail Open:** If IPS fails, network traffic still flows.
- **Sideloading:** Installing apps manually outside official stores.
- **Vendor Monitoring:** Regularly checking supplier security.
- **Regulatory Compliance:** Following laws and industry rules.
- **Attestation:** Formal proof of compliance.

Self-Assessment & Auditing:

- **Self-Assessment:** A company checks its own security.
- **Gap Analysis:** Identifies differences between the current state and desired security level.
- **Policy Administrator:** Issues access tokens or credentials.
- **Snapshot:** A backup copy of a virtual machine.
- **SCAP (Security Content Automation Protocol):** Automates vulnerability checks.
- **RAID:** Combines multiple hard drives for reliability (not a backup solution).
- **Right to Audit:** Allows audits in contracts with third parties.

Data Protection & Loss Prevention:

- **Something You Have:** Physical security tokens (e.g., RFID card, token generator).
- **DLP (Data Loss Prevention):** Prevents sensitive data from being sent out (e.g., via email).
- **Data Sovereignty:** Data must stay in its original country.
- **Geographical Dispersion:** Data centers in different locations for safety.

Security Best Practices:

- **Blocking Keyloggers:** Block unknown outgoing network traffic.
- **Chain of Custody:** Tracks who handled digital evidence.
- **E-Discovery:** Collecting digital evidence (e.g., emails).
- **Legal Hold:** Prevents deletion of data due to legal requests.
- **Non-Repudiation:** Ensures an action happened and proves who did it.

Network & Infrastructure Security:

- **WAF (Web Application Firewall):** Protects web applications.
- **VPN Concentrator:** Manages multiple remote VPN connections.
- **UTM (Unified Threat Management):** A multi-function firewall.
- **XDR (Extended Detection and Response):** Identifies malware and cyberattacks.
- **SASE (Secure Access Service Edge):** Cloud-based security (like VPN).
- **HIPS (Host-Based IPS):** Protects individual computers.
- **SNMP (Simple Network Management Protocol):** Sends alerts about network issues.
- **End of Life (EOL):** A product is no longer supported.
- **Embedded System:** A device with fixed software that cannot be updated (e.g., a time clock).
- **ICS (Industrial Control System):** Security for industrial operations.
- **Enumeration:** Gathering information about a system.

- **Access Point:** Allows wireless devices to connect to a network.
- **NetFlow Logs:** Summarizes network traffic.

Encryption & Key Exchange:

- **In-Band Key Exchange:** Sending keys through the same communication channel.
- **Out-of-Band Key Exchange:** Sending keys separately (e.g., via SMS).
- **Diffie-Hellman:** A method for securely exchanging encryption keys over an untrusted network.

Data Handling Roles:

- **Data Controller:** Decides how to process data (e.g., HR department).
- **Data Owner:** Manages data (e.g., HR manager).
- **Data Subject:** The person whose data is processed (e.g., shipping address).
- **Processor:** A third-party company that processes data but doesn't control it.
- **Data Custodian:** Manages access permissions.

IT Management & Operations:

- **Access Control List (ACL):** Restricts network access (e.g., who can enter a data center).
- **Stakeholder Management:** Balancing interests of different groups in a project.
- **Retention Policies:** Define how long backups are kept.
- **Change Management:** Planning and tracking changes in IT systems.
- **Bloatware:** Pre-installed apps that users may not need. (Compass on iOS)
- **Regulatory Pentesting:** Security testing required by law (e.g., for financial or healthcare companies).

Financial Risk Terms:

- **SLE (Single Loss Expectancy):** The cost of one incident. 1phone=100 Euro (tip: E like Euros).
- **ARE (Annual Rate of Occurrence):** How often incidents happen in a year. 7dead phones per year.
- **ALE (Annual Loss Expectancy):** Total cost of all incidents in a year. (tip: E like Euros).

Cybersecurity Techniques:

- **Key Stretching:** Strengthening passwords by hashing them multiple times.
- **SD-WAN (Software-Defined WAN):** Direct cloud access from all company locations.
- **802.1X:** Uses corporate credentials for network access. (+Kebreros or Radius)
- **VPN:** Securely connects employees working from cafes or hotels.
- **Replay Attack:** Capturing and resending network data to fool a system.

High Availability (HA) for Web Applications:

1. **Redundancy:** Running the app on multiple servers.
2. **Load Balancing:** Spreading user traffic across servers.
3. **Failover:** Automatically switching to a backup server if one fails.
4. **Monitoring & Auto-Recovery:** Detecting problems and fixing them automatically.