Q.1 Organizations have a duty to protect sensitive data within applications. To that end, you must encrypt critical data while it's at rest & in transit. This includes financial transactions, web data, browser data, & information residing in mobile apps. Regulations like the EU General Data protection Regulation make data protection a serious compliance issue.
What are the security policies & compliance rule required in above organisation & Explain in brief.

→ (a) Acceptable Use policy - It outlines the acceptable use of computer equipment. It is used for business purposes in serving the interests of the company, clients, & customers in the course of normal operation.

(b) Security Awareness & Training Policy - It should be administered to all workforce members, so they can properly carry out their functions while appropriately safeguarding company information.

(c) Change management Policy - An organization's change management policy ensures that changes to an information system are managed, approved and tracked.

(d) Incident Response Policy - It is part of an organization's Business continuity Plan. It outlines an organizations response to an information security incident.

(e) Remote Access Policy - Remote access involves connecting to the company's network from any host. It is designed to minimize potential exposure from damages that may result from unauthorized use of resources.

(f) Password creation & Management Policy - It provides guidance on developing, implementing & reviewing a documented process for appropriately creating, changing & safeguarding strong & secure passwords used to verify user identities & obtain access for company systems or information.

(g) Network Security Policy - It ensures the confidentiality integrity & availability of data on company's systems by following a specific procedure for conducting information system & network activity review on a periodic basis.

Q.2 Explain intrusion Detection & Prevention Mechanism

→ I. An intrusion detection & prevention system monitors a network for possible threats to alert the administrator, thereby preventing potential attacks.

II. Functions of IDPS

(a) Guards technology infrastructure & sensitive data: Data is constantly flowing through the network, so the easiest way to attack or gain access to a system is to hide within the actual data. The IDS part of the system is reactive alerting security experts of such possible incidents.

(b) Reviews existing user & security policies - Every security driven organization has its own set of user policies & access related policies for its applications & systems.

(c) Gather information about n/w resources - An IDS-IPS also gives the security team a birds eye view of the traffic flowing through its n/w. This helps them keep track of n/w resources, allowing them to modify a system in case of traffic overload or under-usage of servers.

IV. An IDPS works by scanning processes for harmful patterns, comparing system files & monitoring users behavior & system patterns. IPS uses web application firewalls & traffic filtering solutions to achieve incident prevention

Types of IDPS -

(a) Network based intrusion prevention system -
Monitor the entire networks or network segment for malicious traffic. This is usually done by analyzing protocol activity.

(b) Wireless intrusion Prevention system -
monitor wireless networks by analyzing wireless networking specific protocol. WIPS are deployed within the wireless network & in areas that are susceptible to unauthorized wireless networking.

(c) Network behavior Analysis -
While HIPS analyze deviation in protocol activity, network behavior analysis systems identify threats by checking for unusual traffic patterns.

(d) Host based intrusion prevention system -
It differ from the rest in that they're deployed in a single host monitors the traffic flowing in & out of that particular host by monitoring running processes, network activity, system logs, application activity.

Q3 Explain web application security frameworks.

→ I. Web application security refers to a variety of processes, technologies or methods for protecting web servers, web applications & web services such as APIs from attack by internet-based threats.

II. Web application security is crucial to protecting data, customers & organizations from data theft, interruptions in business continuity or other harmful results of cybercrime.

III. The world today runs on apps, from online banking & remote work apps to personal entertainment delivery & e-commerce. It is no wonder that applications are a primary target for attackers, who exploit vulnerabilities such as weaknesses in APIs, open source code

IV. Common attacks against web application- Brute force, sql injection, cross-site scripting cookie poisoning, session hijacking

V. The application framework provides a holistic approach to information security & risk management by providing organizations with the breadth & depth of verifying / validating security controls that are necessary to strengthen information systems & the associated environments.