Problem 1

With “bring your own device”, there are several security threats: lack of physical security controls, use of untrusted mobile devices, use of untrusted networks, use of untrusted contents, use of applications created by unknown parties, interaction with other systems, use of location services. The device should be inspected, and guidelines should be enlisted with regards to the operating system and applications.

The following security controls should also be implemented on the device:

- Enable auto lock
- Enabling a pin/password to unlock the device and using it to log into other applications
- Avoid using auto-complete features that remember usernames or passwords.
- Ensure that SSL protection is enabled, if available.
- Make sure that software, including operating systems and applications, is up to date.
- Install antivirus software as it becomes available.
- Either sensitive data should be prohibited from storage on the mobile device or it should be encrypted.
- IT staff should also have the ability to remotely access devices, wipe the device of all data, and then disable the device in the event of loss or theft.

Also, all traffic should be encrypted with either SSL, IPv6, or through a VPN. And a firewall should be used to limit the scope of data and application access.

Problem 2

With a wireless LAN, the transmission medium provides possible security vulnerable points. The key factors that contribute to the higher risk are the wireless channels, device mobility, limited hardware resources, and increases accessibility. Some of the threats include accidental association, malicious association, ad hoc networks, identity theft, man-in-the-middle attacks, and denial of service. To combat some of wireless transmission threats, encryption and signal hiding will be used (turn of SSID, reduce signal strength). To prevent unauthorized access to the network, the IEEE 802.11i (RSN) standard will be used.

Here are some other techniques that will be used to secure the wireless LAN.

- Use antivirus and antispyware software, and a firewall. These facilities should be enabled on all wireless network endpoints.
- Turn off identifier broadcasting. Wireless routers are typically configured to broadcast an identifying signal so that any device within range can learn of the router’s existence.
- Change the identifier on your router from the default.
- Change your router’s pre-set password for administration.
- Allow only specific computers to access your wireless network. A router can be configured to only communicate with approved MAC addresses.

Problem 3

The standard internet mail architecture will be used with IMAP for MS → MUA. IMAP uses a TCP connection and provides more features and stronger authentication when compared with POP3. Additionally, MIME will be used so that we are not limited by SMTP. Some of the email security threats include:

- Phishing/Spear phishing
- Email modified in transit
- Disclosure of sensitive information via monitoring and capturing of email traffic
- Unsolicited bulk email
- DoS/DDoS attacks against servers

To mitigate some of these threats, domain-based authentication techniques, digital signatures, TLS to encrypt email transfer, end-end encryption, filtering techniques, and multiple servers (cloud-based) will be used. The following counter threat protocols may also be used as an extension: STARTTLS, S/MIME, DNSSEC, and DANE.

Problem 4

In order to implement a secure virtual private network, IPSec tunnel mode will be used. Tunnel mode provides protection to the IP packets. Encryption and authentication algorithms/protocols will be used in the VPN. The architecture of the VPN will be explained using a top-down approach. The user system with IPSec is connected to the private network via a secure IP traffic link. In the private network many virtual tunnels protected by IPSec connect the boarder of one end to the other. The private network is then connected to a networking device running IPSec via a secure IP traffic connection. The network device is connected to an ethernet switch via an unprotected IP traffic link. The ethernet switch is connected to the end user/server via an unprotected IP traffic connection.

For IPSec an automated key exchange will be used, specifically ISAKMP/Oakley.

Problem 5

Both host IDS and network IDS will be used, and both will be utilizing misuse and anomaly detection. The three components of an IDS are the sensors, analyzers, and user interface. The sensor collects the data the analyser determines if an intrusion occurred, and the UI enables the user to view the results. The NIDS will look at the packets on the network as they pass by some sensor. The packets are of interest if they match a signature. The three primary types of signatures are string, port and header. String looks for a text string that indicates a possible attack. Port watches for connection attempts to well known, frequently attacked ports. Header watches for dangerous or illogical combinations in packet headers.

Problem 6

The aim of the firewall will be to protect ABC's network from internet-based attacks and to provide a single choke point where security and auditing can be imposed. It can also be used to segregate portions of the network. The firewall will provide a location for monitoring security related events, provide a platform for several internet functions that are not security related, and provide a platform for the VPN.

Four techniques the firewall will use to control access and enforce ABC's security policy:

- Service control – Determines type of internet service that can be accessed, inbound/outbound.
- Direction control – Determines direction in which particular service requests may be initiated and allowed to flow through.
- User control – Controls access to a service according to which user is attempting to access it.
- Behavioural control – Controls how particular services are used

ABC will implement firewalls in all aspects of the business. Thus, it will have a packet filtering firewall, stateful inspection firewall, application proxy firewall, and a circuit-level proxy firewall.

Problem 7

DOS/DDOS will prevent legitimate users from a service from using that service. Single host/node attacks is referred to as DOS. Distributed compromised hosts/nodes attack is referred as DDOS. Typically, a flood of useless packets will be sent to the server so that the service it provides becomes unavailable. At ABC, we will try to prevent DOS/DDOS attacks by implementing the following counter measures:

- Attack prevention and preemption (before the attack):
    - Enable victim to ensure attack attempts without denying service
    - Techniques: enforcing policies for resource consumption and providing backup resources available on demand.
    - Prevention mechanisms to modify systems and protocols on the Internet to reduce the possibility of DDoS attacks.
- Attack detection and filtering (during the attack):
    - Mechanisms that attempt to detect the attack as it begins and respond immediately.
    - Detection involves looking for suspicious patterns of behavior
    - Response involves filtering out packets likely to be part of the attack
- Attack source traceback and identification (during and after the attack):
    - Attempt to identify the source of the attack as a first step in preventing future attacks (may not yield results fast enough, if at all, to mitigate an ongoing attack)

Problem 8

ABC will deploy both public and private cloud models since it is a bank. Also, ABC will utilize SaaS and IaaS since it needs an internal system and an interface for its clients. The top security threats to a bank would be data breaches, system/application vulnerabilities, account hijacking, and loss of data.

To ensure a data breach does not occur, the data must be secured while at rest, in transit, and in use, and access to the data must be controlled. To do this, the client can employ encryption to protect data in transit, and/or enforce access control techniques (however the CSP is involved to some extent depending on the service model used). In addition, for data at rest, the ideal security measure is for the client to encrypt the database and only store encrypted data in the cloud, with the CSP having no access to the encryption key.

To counter system/application vulnerabilities, consistent technical and management process must be used. Risk analysis and management, regular vulnerability detection, patch management, and IT staff training would all be involved.

To fight account hijacking counter measures would include:

- Prohibit the sharing of account credentials between users and services
- Leverage strong two-factor authentication techniques where possible
- Employ proactive monitoring to detect unauthorized activity
- Understand CSP security policies and SLAs

To prevent data loss, the CSC should be assured that the CSP has a thorough redundancy scheme with regular backups, including geographic redundancy (may be supplemented by a cloud-to-premise backup so that a recent copy is available at the customer site).