Network Security Solutions and Risk Analysis

1. VLAN Segmentation

Solution:

- Create separate VLANs for each department (Civil, Mechanical, EEE, CSE, EC, AI/ML, AI/DS, Library, Exam Centre, Administration).
- Configure inter-VLAN routing on the MAN router with ACLs restricting unnecessary cross-department communication.

Technologies:

- IEEE 802.1Q VLAN tagging
- Layer 3 routing on ISR4331 MAN router
- Access Control Lists (ACLs)

Risks if not implemented:

- Lateral movement of malware between departments.
- Data exposure between unrelated departments.

Advantages:

- Reduces broadcast domains.
- Limits attack surface.
- Easier traffic monitoring and policy enforcement.

---

2. Wireless Network Security

Solution:

- Use WPA3-Enterprise with RADIUS authentication for all departmental wireless routers and access points.
- Disable SSID broadcast for non-public networks.
- Implement MAC address filtering for critical wireless devices.

Technologies:

- WPA3-Enterprise encryption
- RADIUS server authentication
- MAC filtering on access points

Risks if not implemented:

- Unauthorized wireless access.
- Eavesdropping on sensitive communications.

Advantages:

- Strong encryption and authentication.
- Reduces risk of rogue access.
- Centralized wireless credential management.

---

3. Redundancy and High Availability

Solution:

- Deploy a secondary MAN router and link aggregation between critical switches.
- Configure Rapid Spanning Tree Protocol (RSTP) for fast failover.

Technologies:

- Link Aggregation Control Protocol (LACP)
- RSTP (IEEE 802.1w)
- Dual-homing distribution switches

Risks if not implemented:

- Single point of failure causing complete network downtime.

Advantages:

- Continuous network availability.
- Faster recovery during hardware or link failure.

---

4. Printer and Peripheral Security

Solution:

- Change default admin credentials on all printers.
- Disable unused protocols such as FTP, Telnet, and SNMPv1.
- Restrict printer network access to departmental VLAN only.

Technologies:

- Printer access control via IP ACL
- Secure management protocols (SNMPv3, HTTPS)

Risks if not implemented:

- Printers exploited as entry points for attackers.
- Data leakage from print jobs.

Advantages:

- Reduced risk of compromise via peripherals.
- Protection of confidential documents.

---

5. Server Hardening

Solution:

- Isolate servers in a dedicated VLAN with firewall policies.
- Apply regular OS and application security patches.
- Enable logging and intrusion detection on server VLAN.

Technologies:

- VLAN isolation
- Host-based firewalls
- IDS/IPS integration

Risks if not implemented:

- Direct exposure of servers to internal threats.
- Increased likelihood of data breaches.

Advantages:

- Improved server security posture.
- Easier monitoring of critical assets.

---

6. Centralized Monitoring and Logging

Solution:

- Deploy a Security Information and Event Management (SIEM) system to collect logs from routers, switches, servers, and wireless devices.
- Configure alerting for abnormal activity.

Technologies:

- SIEM platform (e.g., Splunk, Wazuh)
- Syslog and SNMP traps

Risks if not implemented:

- Delayed detection of security incidents.

Advantages:

- Faster threat detection.
- Centralized incident response.