**List 3 specific exploits or damaging actions you could perform using the employees access.**

1. Modifying or altering payroll data.
2. Sending phishing emails to all employees.
3. Steal sensitive employee personal information

**Now take on the role of the security analyst and for each action you listed, explain why it was possible based on flawed access control decision.**

1. Violation of least privilige : HR employee had admin rights instead of read-only access.
2. Lack of seperation of duties: Payroll modification didn’t require Finance approval.
3. Ability to send phising email to all staff emails list without approval.

**For each action, recommend one realistic and proportionate mitigation, using principles such as least privilege, access revocation or access control models.**

1. Enforce least priviliges : Restrict HR database access to read only unless explicitly needed.
2. Implement seperation of duties : Require finance approval for payroll changes.
3. Apply approval workflow: Restrict distribution list edits to IT and mandate multi-person review.

### ****CIA Triad****

**Advantages**

* Simple and easy to understand.
* Widely adopted and recognized.
* Covers core security needs (C, I, A).

**Disadvantages**

* Too broad and high-level.
* Doesn’t address human factors or usability.
* Lacks depth for modern security issues.

### ****Parkerian Hexad****

**Advantages**

* More comprehensive than CIA.
* Includes authenticity, possession, and utility.
* Better for analyzing real-world trade-offs.

**Disadvantages**

* More complex, harder to explain.
* Some overlap between elements.
* Less commonly used than CIA.