Alpha Bank part 2

AlphaBank is a mid-sized regional bank with 25 branches and over 500 employees. The bank has recently undergone rapid expansion, acquiring two smaller competitors and integrating their systems into its core banking platform.

AlphaBank's IT department is responsible for maintaining the core banking system, customer online banking portal, and internal HR and payroll systems. The IT team is small, with 1 IT manager, 2 system administrators, 2 developers, and 1 helpdesk technician.

The most critical systems are hosted on-premises in the data center at headquarters, with daily backups sent to a third-party cloud storage service.

Recently, internal audit reviewed AlphaBank's IT environment and found several areas of concern.

Audit Findings

1. **User Access Management**
    - User accounts for employees who resigned more than 6 months ago were still active.
    - Some employees shared admin passwords to "get things done faster."
    - No periodic review of access rights to sensitive systems.
2. **Change Management**
    - Developers directly deploy code changes into production without formal approval.
    - No record is kept of what changes were made or who authorized them.
    - Sometimes, code changes have caused unexpected downtime in the online banking portal.
3. **Backup and Recovery**
    - Backups are taken daily, but no tests have been performed to verify if they can be restored.
    - The backup schedule and retention policy are not documented.
4. **Incident Management**
    - There is no formal procedure to handle security incidents.
    - In a recent phishing attack, employees were unsure who to report it to, and the incident went unreported for two weeks.
5. **Physical Security**
    - The data center at headquarters is locked, but keys are kept in an unlocked drawer at reception.
    - Visitors are not required to sign in before accessing IT areas.

Questions

1. Identify at least **two risks** associated with each of the findings (user access, change management, backup, incident management, physical security).
2. For each finding, recommend **specific IT general controls (ITGC)** that Alpha Bank should implement to mitigate the risks.
3. For one of the findings, suggest how management can **monitor and test the effectiveness** of the implemented controls.
4. What principle(s) of information security (e.g., confidentiality, integrity, availability) are at risk in this case study? Explain.