IS Audit Findings:

1. **Risk 1:** The company's server room should be secured with additional security method rather than a single factor authentication method such as facial recognition.
   Risk Outcome:
   The attacker could be sniffing on the network capturing information from the swipe card reader.

   COBIT Practices - DSS05.05 Manage physical access to I&T assets.
   Activities – 4. Restrict and monitor access to sensitive IT sites by establishing perimeter restrictions, such as security devices on interior and exterior doors.

2. **Risk 1:** A security policy must be tailored for each company according to its specific situation.
   Risk 2: HR should not assume that all employees are aware of this policy.
   Risk Outcome:
   Risk 1: Some employees might not know what steps to take when they are faced with security related issues.

   COBIT Practices - APO13.01 Establish and maintain an information security management system (ISMS).
   Activities – 1. Define the scope and boundaries of the information security management system (ISMS).

3. **Risk 1:** IT strategic plan should be reviewed by the IT team since they have knowledge in this area.
   Risk Outcome:
   Risk 1: The steering committee may not have enough knowledge to review and evaluate the IT strategic plan.

4. **Risk 1:** Users should include complexity in their passwords including special characters.
   Risk Outcome:
   Risk 1: Intruders will find it easier to retrieve the password using a brute force attack and gain access to a user's account.

   COBIT Practices - DSS05.02 Manage network and connectivity security.
   Activities – 6. Based on risk assessments and business requirements, establish and maintain a policy for security of connectivity.

5. **Risk 1:** Different vendors have different hardware and software configurations which may not be compatible with the companies IT infrastructure.
   Risk Outcome:
   Risk 1: Users would experience more disruptions when undertaking daily tasks on the computer.

   COBIT Practices - BAI02.02 Perform a feasibility study and formulate alternative solutions.
   Activities – 1. Identify required actions for solution acquisition or development based on the enterprise architecture. Take into account scope and/or time and/or budget limitations.

6. **Risk 1:** A background process may be interrupted when the computer times out.
   Risk Outcome:
   Risk 1: Interrupting a background process such as a scheduled data backup can cause data loss.

   COBIT Practices - DSS05.03 Manage endpoint security.
   Activities – 1. Configure operating systems in a secure manner.

7. **Risk 1:** Company and employee account information can be compromised.
   Risk Outcome:
   Risk 1: Retired employees can expose or take advantage of company personal information since they are legally not bound by the company contract.

   COBIT Practices - DSS05.04 Manage user identity and logical access.
   Activities – 3. Segregate, reduce to the minimum number necessary and actively manage privileged user accounts. Ensure monitoring on all activity on these accounts.

8. **Risk 1:** These personal devices do not follow the companies IT requirements.
   Risk Outcome:
   Risk 1: Employee personal devices may not have an antivirus or have a weak antivirus installed.
   Risk 2: If these personal devices were already infected with a virus, they can spread it over the corporate network.

   COBIT Practices - DSS05.01 Protect against malicious software.
   Activities - 1. Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that 2 are updated as required (automatically or semi-automatically).

9. **Risk 1:** Sharing an account can cause issues when the company needs to investigate issues relating to processing purchase information.
   Risk Outcome:
   Risk 1: File's may accidentally be deleted, or modified without permission and the company may not know who made these actions.

   COBIT Practices - DSS05.04 Manage user identity and logical access.
   Activities - 6. Ensure that all users (internal, external and temporary) and their activity on IT systems are uniquely identifiable.

10. **Risk 1:** Employees may have access to parts of the IT system they should not have access to.
    Risk Outcome:
    Risk 1: Damage to the IT system can happen if an unqualified employee has access to more advanced areas of the system.

    COBIT Practices - DSS05.04 Manage user identity and logical access.
    Activities – 8. Perform regular management review of all accounts and related privileges.

11. **Risk 1:** Employees testing these systems must be proven to be experienced and educated.
    Risk Outcome:
    Risk 1: If the employees are not experienced enough, there may be loop holes in the IDS that go unnoticed.

    COBIT Practices - APO13.02 Define and manage an information security and privacy risk treatment plan.
    Activities - 5. Implement information security and privacy training and awareness programs.

12. **Risk 1:** Mr. Jacobs might process a change request that Ms Brown later considers not acceptable.
    Risk Outcome:
    Risk 1: The company occurring more software issues in the future.

    COBIT Practices - BAI06.02 Manage emergency changes.
    Activities – 2. Ensure that a documented procedure exists to declare, assess, approve preliminarily, authorize after the change and record an emergency change.

13. **Risk 1:** Mr. Bill may assign the wrong user rights to employees.
    Risk Outcome:
    Risk 1: Mr. Bill's employees may be either hindered in their productivity when accessing the system or be given too much permissions.

    COBIT Practices - DSS05.04 Manage user identity and logical access.
    Activities - 7. Maintain an audit trail of access to information depending upon its sensitivity and regulatory requirements.

14. **Risk 1:** Employee have privileges and access to more files than they need.
    Risk Outcome:
    Risk 1: Employees can cause harm to the system.

    COBIT Practices - DSS05.02 Manage network and connectivity security.
    Activities – 1. Allow only authorized devices to have access to corporate information and the enterprise network.

15. **Risk 1:** If Ms Brown decides to manage the project internally, she may face difficulties due to the lack of experience and the time available to dedicate to this project.
    Risk Outcome:
    Risk 1: The project may exceed the given budget or completion date due to the lack of time and project management experience.

    COBIT Practices - APO02.01 Understand enterprise context and direction.
    Activities - 1. Develop and maintain an understanding of the external environment of the enterprise.