**Analyze the Audit Scope, Goals, and Risk Assessment**

* **Significant Risks:** The most significant risks to XYZ Financial Services include potential data breaches, unauthorized access to financial records, disruption of financial services, and non-compliance with financial regulations.
* **Priority Controls:** Controls such as data encryption, access controls, intrusion detection systems, regular data backups, and employee training on cybersecurity best practices should be prioritized for immediate implementation.
* **Compliance Regulations:** XYZ Financial Services must adhere to financial regulations such as the Gramm-Leach-Bliley Act (GLBA) and Payment Card Industry Data Security Standard (PCI DSS). Compliance is crucial to protect customer financial data, maintain regulatory trust, and ensure business continuity.

**Controls Assessment**

* **Administrative Controls:**
  + **Asset Category: Customer Financial Data**
    - **Access Controls:** [X] High
      * Implement strong access controls to limit who can access and modify customer financial records.
    - **Employee Training:** [X] Medium
      * Conduct cybersecurity training for employees to reduce the risk of human errors in data handling.
  + **Asset Category: Employee Devices**
    - **Access Controls:** [X] High
      * Implement access controls to restrict unauthorized access to employee devices (computers, phones).
    - **Employee Training:** [X] Medium
      * Train employees on cybersecurity best practices to minimize security risks associated with devices.
* **Technical Controls:**
  + **Asset Category: Customer Financial Data**
    - **Data Encryption:** [X] High
      * Implement data encryption to protect customer financial data in transit and at rest.
    - **Intrusion Detection Systems:** [X] High
      * Implement IDS to quickly identify and respond to potential security incidents related to customer data.
    - **Regular Data Backups:** [X] Medium
      * Regularly backup customer financial data to ensure business continuity and data recovery capabilities.
  + **Asset Category: Employee Devices**
    - **Endpoint Security Software:** [X] High
      * Deploy endpoint security software on employee devices to protect against malware, unauthorized access, and data breaches.
    - **Mobile Device Management:** [X] Medium
      * Implement MDM solutions to enforce security policies, remotely wipe data, and track employee mobile devices for security and compliance.
    - **Full Disc Encryption:** [X] High
      * Apply full disk encryption on laptops to protect sensitive data in case of device loss or theft.
* **Physical Controls:**
  + **Asset Category: Server Room Access**
    - **Access Control System:** [X] High
      * Implement a biometric access control system to restrict entry to the server room based on authorized personnel only.
    - **Video Surveillance:** [X] High
      * Install video surveillance cameras to monitor and record activities in and around the server room for security and audit purposes.
    - **Environmental Controls (HVAC):** [X] Medium
      * Implement environmental controls to monitor and maintain optimal temperature and humidity levels in the server room to prevent hardware damage.

**Step 4: Conduct the Audit: Compliance Checklist**

* **Asset Category: Customer Financial Data**
  + **General Data Protection Regulation (GDPR):** [X] XYZ Financial Services operates internationally, making GDPR compliance essential for protecting EU citizens' data and privacy.
  + **Payment Card Industry Data Security Standard (PCI DSS):** [X] As a financial services provider, PCI DSS compliance is mandatory to secure cardholder data.
  + **HIPAA:** [ ] Not applicable as XYZ Financial Services is not in the healthcare sector.
  + **SOC type 1, SOC type 2:** [X] SOC compliance ensures transparency and trust with clients and partners.
  + **FERC-NERC:** [ ] Not applicable to XYZ Financial Services' operations.
* **Asset Category: Employee Devices**
  + **General Data Protection Regulation (GDPR):** [X] GDPR compliance is necessary to protect EU citizens' data privacy, even when handled on employee devices.
  + **Payment Card Industry Data Security Standard (PCI DSS):** [ ] Not directly applicable unless used for payment processing.
  + **HIPAA:** [ ] Not relevant to employee devices in a financial services organization.
  + **SOC type 1, SOC type 2:** [X] SOC compliance ensures secure user access policies and data safety.
  + **FERC-NERC:** [ ] Not applicable to employee devices.
* **Asset Category: Server Infrastructure**
  + **General Data Protection Regulation (GDPR):** [X] GDPR compliance is vital to protect sensitive data stored on servers.
  + **Payment Card Industry Data Security Standard (PCI DSS):** [X] PCI DSS compliance is essential for servers processing credit card transactions.
  + **HIPAA:** [ ] Not necessary unless healthcare data is involved.
  + **SOC type 1, SOC type 2:** [X] SOC compliance ensures secure data handling.
  + **FERC-NERC:** [ ] Not directly applicable to server infrastructure.
* **Asset Category: Network Infrastructure**
  + **General Data Protection Regulation (GDPR):** [X] GDPR compliance is necessary for protecting data transmitted over the network.
  + **Payment Card Industry Data Security Standard (PCI DSS):** [X] PCI DSS compliance is vital for network security when processing credit card transactions.
  + **HIPAA:** [ ] Not necessary unless healthcare data is transmitted.
  + **SOC type 1, SOC type 2:** [X] SOC compliance ensures secure data transmission.
  + **FERC-NERC:** [ ] Not directly applicable to network infrastructure.

**Step 5: Assess Your Activity**

* Reviewed the audit scope, considered risks, and ensured controls address these risks.
* Selected controls based on relevance and rated their priority for implementation.
* Selected compliance regulations and provided explanations for their necessity.