INFO 7374 - Cybersecurity Audit and Compliance
Week 13 - Assignment 12

Krisha Lakhani – 002334794

1. Identify and discuss 5 HITRUST CSF v11.4 control categories that are most critical to INFO-7374 Health LLC's current context. Justify your selection.

a. Risk Management

This category is foundational due to the absence of a formalized risk register. HITRUST requires entities to identify, assess, and document risks, specifically for HIPAA-regulated entities that handle PHI.

b. Access Control

Sensitive PHI will require strict access limitations. With cloud and third-party systems leveraged, the assurance of appropriate access controls is imperative to ensure the confidentiality and integrity of the PHI.

c. Vendor Management

INFO-7374 relies on third parties for its cloud infrastructure as well as claims processing. Managing those vendor relationships safely is essential to minimizing supply chain risk.

d. Logging & Monitoring

The organization engages in limited logging practices. Logging is important for identifying unauthorized access and providing audit trails, which is important for both HIPAA and SOC 2 standards.

e. Information Security Governance

The absence of any formally documented policies indicates a weak governance structure. These categories are fundamental in establishing governance that aligns with HITRUST, HIPAA, SOC 2, among other best practices.

INFO 7374 - Cybersecurity Audit and Compliance
Week 13 - Assignment 12

Krisha Lakhani – 002334794

2. For each selected category, list two key implementation controls to verify during the audit. Explain how you'd assess them (what evidence you would request).

Category	Implementation Control	Evidence to Assess
Risk Management	(i) Formal risk assessment annually (ii) Documented risk register	- Risk assessment report - Risk register with mitigation actions
Access Control	(i) Role-based access controls (RBAC) (ii) User access reviews quarterly	- Access control policies - Logs of access reviews with sign-offs
Vendor Management	(i) Vendor due diligence checklist (ii) Third-party risk assessments	- Signed contracts and SLAs - Vendor risk assessment reports
Logging & Monitoring	(i) Security event logging enabled (ii) Review of logs for anomalies	- Screenshots/logs from SIEM tools - Log review procedures
Information Security Governance	(i) Established security policies and roles (ii) Formal information security training	- Information security policy document - Employee training logs and sign-in sheets

3. Recommend 3 immediate remediation priorities to prepare for the HITRUST Validated Assessment.

- **Develop a Formal Risk Register**
  Conduct a comprehensive risk assessment and maintain a living risk register with mitigation plans.
- **Implement Centralized Logging & Monitoring**
  Set up a centralized logging system (e.g., SIEM) and document regular review procedures.
- **Establish Governance Framework**
  Formalize information security policies, define roles/responsibilities, and initiate a company-wide training program.

INFO 7374 - Cybersecurity Audit and Compliance
Week 13 - Assignment 12

Krisha Lakhani – 002334794

4. Describe how the HITRUST maturity model (PRISMA) would impact scoring during the Validated Assessment. Provide examples for at least two categories.

The PRISMA model assesses each control across five maturity levels: Policy, Procedure, Implemented, Measured, and Managed. A control must be fully "Implemented" to be scored above 62.5%.

- **Example 1 – Access Control**
  If INFO-7374 only documents access policies (Policy + Procedure) but hasn't enforced or audited them (Implemented), the maturity score remains low. Evidence of actual access enforcement will push the control to a compliant level.
- **Example 2 – Logging & Monitoring**
  Limited logging without documented reviews will cap scoring. If logs are regularly analyzed and improvements are tracked (Measured + Managed), the control scores higher, aiding certification.

5. Explain how INFO-7374 Health LLC can use MyCSF to streamline their HITRUST certification journey.

- **Central Repository:**
  MyCSF acts as a single platform to upload, manage, and track evidence and policies aligned with each control.
- **Readiness Assessments:**
  Organizations can perform internal readiness assessments, get score projections, and identify gaps before formal validation.
- **Cross-Framework Mapping:**
  MyCSF maps HITRUST controls to HIPAA, SOC 2, and GDPR, ensuring INFO-7374 can demonstrate compliance across multiple frameworks simultaneously.
- **Automation & Collaboration:**
  Tasks, comments, and workflows can be assigned, making the certification process collaborative and efficient.