**Assessment Worksheet – 3**

**Defining the Scope and Structure for an IT Risk Management Plan**

**Course Name and Number**: IAA202  
**Student Name**: Vu Hoang  
**Instructor Name**: Ho Hai  
**Lab Due Date**: 02/06/2020

1. Circle the scenario and industry vertical your Instructor assigned to your group:

a. Healthcare provider under HIPPA compliance law:

* Health plans
* Health care clearinghouses
* Health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers.

d. Higher-education institution under FERPA compliance law

* The Family Educational Rights and Privacy Act of 1974 (FERPA): Designed to protect students and their families by ensuring the privacy of student educational records.
* The Health Insurance Portability and Accountability Act of 1996 (HIPAA): Requires covered entities (typically medical and health insurance providers and their associates) to protect the security and privacy of health records.
* The Gramm Leach Bliley Act of 1999 (GLBA): Imposes privacy and information security provisions on financial institutions; designed to protect consumer financial data.
* Federal Policy for the Protection of Human Subjects (“Common Rule”): Published in 1991 and codified in separate regulations by 15 federal departments and agencies, outlines the basic ethical principles (including privacy and confidentiality) in research involving human subjects.
* The Fair and Accurate Credit Transaction Act of 2003 (FACTA, or “Red Flags Rule”): Requires entities engaged in certain kinds of consumer financial transactions (predominantly credit transactions) to be aware of the warning signs of identity theft and to take steps to respond to suspected incidents of identity theft.
* The Privacy Act of 1974: Specifies the rules that a federal agency must follow to collect, use, transfer, and disclose an individual’s personally identifiable information (PII).

2. Make sure your table of contents addresses your scenario and vertical industry.

3. Make sure your table of contents includes at a minimum, the five major parts of IT risk management:

• Risk planning:

1. Establish the context
2. Identify risks
3. Analyze risks
4. Evaluate risks
5. Treat/ Manage risks

• Risk identification:

* 1. User domain
  2. Workstation domain
  3. Lan-to-wan domain
  4. Wan domain
  5. Remote access domain
  6. Systems/ Application domain

• Risk assessmen:

1. Fire.
2. Noise.
3. Vibration.
4. Manual handling.
5. Hazardous substances.
6. Display screen equipment.

• Risk mitigation:

1. Avoidance
2. Acceptance
3. Reduction
4. Control
5. Transference

• Risk monitoring:

1. Triggers
2. Mitigation plan progress
3. Identify new risks
4. Validate your plans

4. Make sure your table of contents is executive management ready and addresses all the risk topics and issues needed for executive management awareness:

**1. Ask the questions**

**2. Create the right culture**

**3. Clarify responsibilities and rules**

**4. Use suitable reward systems**

**5. Focus on the business objectives**

**6. Recognize the limitations of risk assessments**

**7. Put business managers in the driver’s seat**

**8. Demand integrated management information**

**9. Make sure rules are enforceable**

**10. Align internal audit with the business**