The first component of the summative assessment for this course is the development and creation of a **risk analysis paper**. The assessment will allow students

the opportunity to investigate international and U.S. cyberlaws; state statutes; criminal, civil, private, and public laws; and ethics and then compare them within

the current cyber business model of an organization to identify any implications for information technology. Students will research their chosen organization,

studying the business models, to identify key areas of potential risk due to the business activities and industry.

**Prompt:** Submit a comprehensive risk analysis paper that identifies the cyberlaw foundations that affect the current information technology business model. The

framework for the assessment will include how the business model ensures that their current cyber practices are both legal and ethical.

**Specifically the following critical elements must be addressed:**

1. Define and evaluate the information technology business model of the organization.

2. Analyze the precise cyber-security laws, private and public laws, state statutes, criminal and civil laws, and ethical guidelines that are pertinent to the

organization.

3. Evaluate the current cyberlaws, regulations, and policies within the organization as they relate to the organization’s information systems.

4. Cyberlaw crimes

a) Evaluate how cyber-related crimes should be **investigated and handled** within an organization.

b) Analyze the **impact** that these cyber-crimes can have on an organization’s information technology structure.

c) Evaluate the appropriate **information security measures** that should be in place to safeguard an organization’s information.

5. Cyber-crime and e-commerce

a) Analyze the organization’s current **information systems security measures** in place that allow users to access the organization’s data.

b) Evaluate the current **cyberlaws** to ensure that they protect the organization’s data against outside intrusion.