1. A security awareness program framework, an explanation of why it is needed, and the potential cost in terms of noncompliance. Note: the cost of not complying is not always limited to fines and penalties!

A security awareness program is a structured, ongoing process for educating employees about cybersecurity threats and teaching them how to identify and prevent attacks. It is important to have a framework in place to ensure that the program is effective and meets the needs of the organization.

There are several potential costs of not having a security awareness program or of not complying with an established framework. One cost is the financial impact of a cyberattack. Cyberattacks can result in the theft of sensitive data, disruption of operations, and damage to a company's reputation, all of which can have significant financial consequences.

In addition to these tangible costs, there is also the intangible cost of damage to an organization's reputation. If a company experiences a cybersecurity breach, it can harm the public's trust in the organization and negatively impact its reputation. This can lead to a loss of customers and revenue.

2.Specific items that need to be addressed in the training per HIPAA and/or Texas statutory requirements

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that sets standards for protecting personal health information. It applies to covered entities, which include healthcare providers, health plans, and healthcare clearinghouses, as well as their business associates.

Under HIPAA, covered entities are required to implement a security awareness and training program to ensure that all employees are aware of and understand their responsibilities for protecting personal health information.
There are several specific items that need to be addressed in HIPAA training:

1. The HIPAA Privacy Rule, which establishes standards for the protection of personal health information.

2. The HIPAA Security Rule, which sets standards for the protection of electronic personal health information.

3. The HIPAA Breach Notification Rule, which requires covered entities to notify affected individuals, the Department of Health and Human Services (HHS), and in some cases the media, of a breach of unsecured personal health information.

4. The HIPAA Enforcement Rule, which outlines the process for enforcing HIPAA regulations and the penalties for noncompliance.

In Texas, there are also state laws that regulate the protection of personal health information. For example, the Texas Medical Records Privacy Act establishes standards for the protection of medical records and requires covered entities to implement appropriate safeguards to protect the privacy of personal health information.
It is important for organizations in Texas to be aware of and comply with both HIPAA and state laws in order to avoid fines and penalties and protect the personal health information of their patients.

3. List of internal groups or departments that should be consulted before the awareness training is submitted to management for final approval.

Before submitting a security awareness training program for final approval, it is important to consult with a variety of internal groups or departments to ensure that the

training is comprehensive and meets the needs of the organization. Some of the internal groups or departments that should be consulted include:

1. Human Resources: HR can provide input on the training program, help with the development of materials, and assist with the rollout of the training to employees.

2. Legal: The legal department can review the training materials to ensure that they comply with relevant laws and regulations.

3. Information Technology: IT can provide technical input on the training program, including identifying specific threats and vulnerabilities that should be addressed.

4. Risk Management: Risk management can help assess the potential risks and impacts of a cyberattack and provide guidance on how to mitigate those risks through the training program.

Consulting with these internal groups and departments can help ensure that the security awareness training program is comprehensive, relevant, and effective in protecting the organization from cyber threats.