In the context of ABC Inc., which is a large on-line electronic product company, answer the following questions.

1. **State three regulations and standards that it should comply with.**

ABC Inc. would have to follow the PCI DSS regulation in order to allow card payments on its website. This regulation is designed to ensure that customers' payment card data is handled and protected appropriately.

ABC Inc. would also have to follow the Federal Trade Commission Act. This ensures that the company is acting in a fair manner in regard to commerce. This request that companies don't operate or act in unethical manners to gain an upper hand on competitors.

Lastly, the company would have to follow the California Consumer Privacy Act (CCPA). This is similar to the GDBR designed with the intent for companies to disclose what information they are obtaining about customers. What they are planning to do with said information and if it is going to be shared to others.

2. **List the responsibilities (roles) of the Information Security Officer of ABC Inc.**

ISOs are tasked with ensuring that the area they are working within is maintaining proper security practices.

They might conduct risk assessments to determine what areas of the business need to be improved upon.

Educate those within their team about best practices and ways to ensure a technically secure environment.

Develop or improve standards and policies.

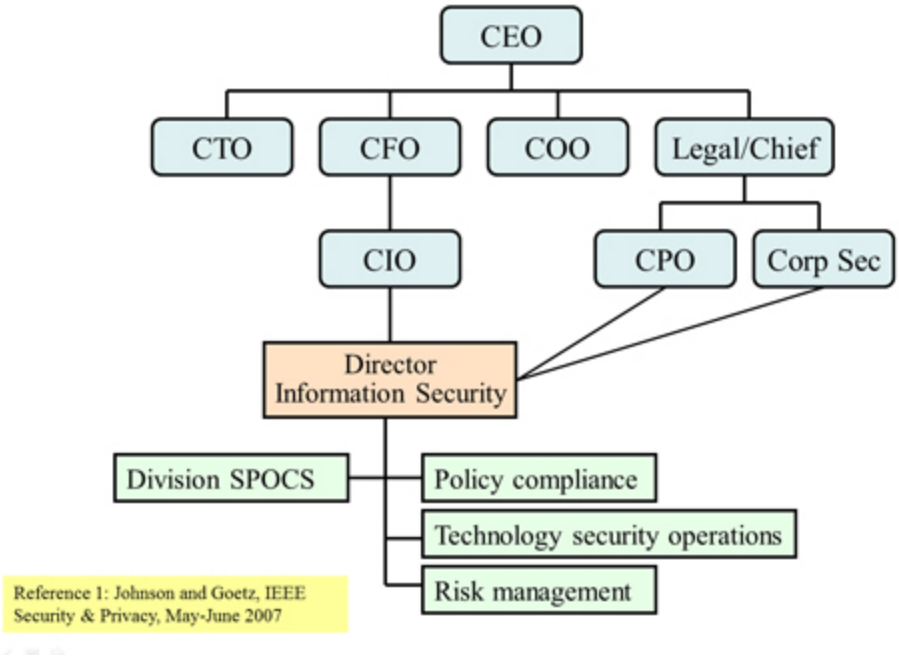
Monitor potential risks or threats within the company or team.

Create plans to address threats or potential breaches.

3. **Suggest a reporting structure (as a diagram) for ABC Inc., assuming that it has 2 million customers, 2000 employees, approximately 20000 transactions each day, and $2 billion sales. Give a brief justification.**

The structure from the image but add a board of directors at the top.

This structure creates clear lines of authority but impresses its importance of security. I would change the CFO to its own branch and place CIO in direct communication with the CEO. This would impress the importance of information security within the company. Allowing the CIO the ability to communicate any incidents that are of concern or could arise.



4. **Describe an incident response plan for ABC Inc. Write it as a list of steps with a brief description for each**

1. **Planning** - Create an incident response plan. This should take into account what teams and groups of professionals that will be involved. Highlighting each role, team, and professionals that will be involved. Ensure that everyone understands what they have to do and what their role is within the response plan. Store this incident response plan in an accessible location so people can refer to it.

2. **Detection-** Establish proper detection methods for different incidents. Setting up ways to detect incidents that may arise. This could be by implementing IDSs or other means of being alerted about unusual activity.
3. **Reaction -** This is how the company goes about containing the breach or threat. Proper documentation should be kept on what assets and individuals are involved. Establish a legal defense and conduct countermeasures.
4. **Recovery-** Restore or regain control and uptime of assets that were compromised. Conduct digital forensics in order to determine how the attack played out. This will also allow the company to understand what assets were impacted. Understand the impact the threat had and report findings to those impacted. Update systems or patch the path that was exploited.