sBooks Pte Ltd

sBooks Pte Ltd intends to operate an online web-based portal to allow authors to publish & sell their ebooks. This portal will be developed in-house. Authors will pay ***sBooks*** a nominal publishing fee for each ebook publised on the portal and a percentage of the proceeds from each ebook sold.

Customers must register with the ***sBooks*** portal and provide credit card details before they are allowed to purchase ebooks with their credit cards. eBooks are copyrighted, hence, customers should not be able to reproduce or distribute them in an unauthorized manner. For customers who prefer a hardcopy version, ***sBooks*** will ship a hardcopy to a physical address that the customer supplies. P.O. Box addresses will not be accepted as a valid shipping location. Customers will be charged accordingly for the printing and shipping.

Customers must be allowed to search for ebooks and be presented with a list of products that match their search query with recommendations of related products.

Before purchasing an item, customers should be allowed to view an excerpt from the ebook as well as read reviews and ratings provided by existing customers. Customers can purchase the entire ebook or just selected chapters.

There will be a "current promotions" page where selected ebooks will be put up for sale at discounted prices. Only specific staff from the marketing department of ***sBooks*** should be able to update this page.

Slow-selling products will be put up for sale at *eBid.com*, an existing online auction portal owned by a third-party company. Only specific staff from the Marketing department of ***sBooks*** should be able to list products for auction. Customers of ***sBooks*** should be able to bid & pay for products without having to create a new account on *eBid.com*. The highest bidder at the end of the auction period will be the winner of the product. A "*B2B Authentication & Authorization Policy*" must be drawn up to handle authentication & authorization between ***sBooks*** and *eBid.com.*

The portal will be implemented in a 3-Tier architecture. Oracle database will be used. Java is the preferred development platform.

The business owners have completed data classification as detailed overleaf.

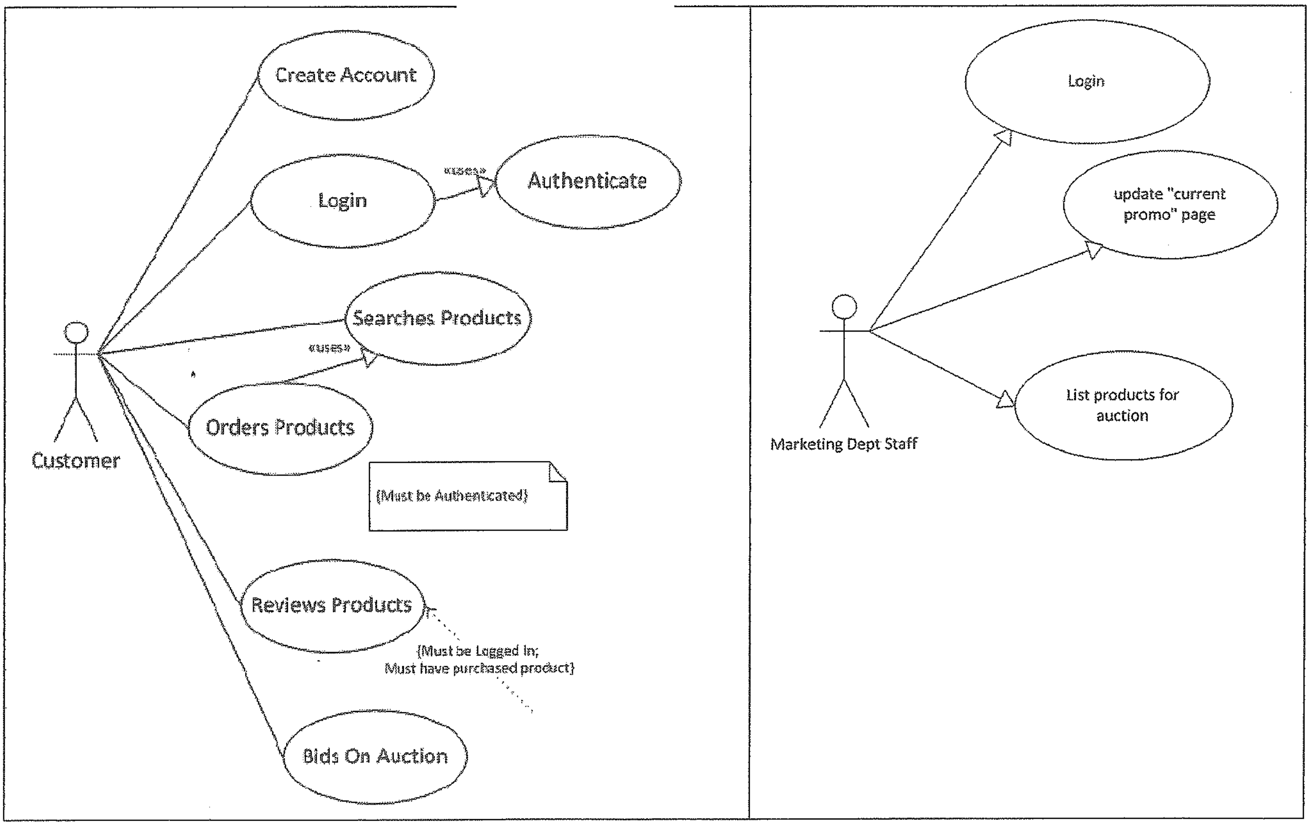
You have just earned your Certified Secure Software Lifecycle Professional (CSSLP®) certification and have been assigned to this project as its security advisor. Answer the questions that follow.

Data Classification

	Impact of loss of		
Data	**Confidentiality**	**Integrity**	**Availability**
Customer			
Personal Info	High	High	High
Shipping address	Medium	High	Medium
order	Medium	High	High
Credit Card	High	High	High
Product			
Item (ebook/chpt)	High	High	High
Pricing	High	High	High
Rating	Low	Low	Low
Reviews	Low	Medium	Low
Cross Domain Credentials	High	High	High

All information classified high and medium confidentiality must be rendered unreadable in transit, in storage and during processing. All information classified high and medium integrity must be protected from tampering.

Use Cases



Question 1

For each use case, find some misuse cases.

Question 2

Assist the project team in deriving the security requirements that need to be incorporated into the software development project.

Hint

Sources of security requirements:

- Business functional requirements (the team has already described some of the busines software requirements in the table below).
- Corporate Governance requirements
- Compliance requirements (Law, Regulations, etc)
- Misuse cases [use your answers for Question 1]

S/N	Software Requirement	Security Requirement
1	Customers must register with the ***sBooks*** portal before they are allowed to purchase ebooks with their credit cards	
2	eBooks are copyrighted, hence, customers should not be able to reproduce or distribute them in an unauthorized manner.	
3	P.O. Box addresses will not be accepted as a valid shipping location.	
4	Customers must be allowed to search for ebooks.	
5	Customers can provide ratings & reviews only about the products they have purchased.	
6	Customers should be allowed to view an excerpt from the ebook.	
7	Customers can purchase the entire ebook or just selected chapters.	
8	Only specific staff from the Marketing department of ***sBooks*** should be able to update the "current promotions" page and list products for auction.	
9	Customers of ***sBooks*** need not create a new account on *eBid.com.*	
10	The highest bidder at the end of the auction period will be the winner of the product	
11	This portal will be developed in-house.	