IT Security Policy Program

UB Inc.

Supreet Kaur

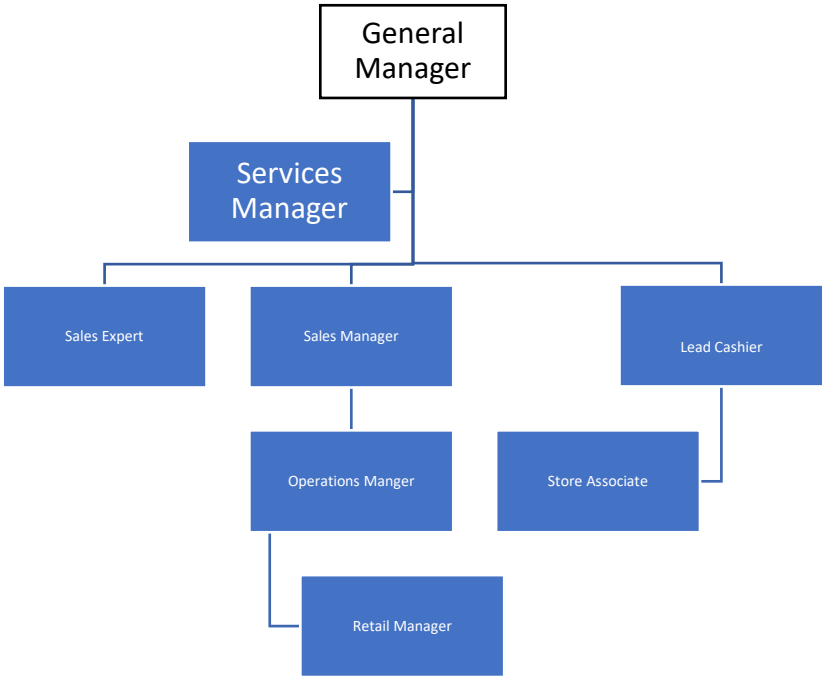
ISA-652, Fall 2020

Information Security and Assurance

George Mason University

Organizational Chart

The organizational hierarchy followed at UB Inc. is shown in figure1.



Organizational Roles

The present roles of UB Inc. are described, these roles may change or update over time.

Role Name	Symbol	Description
User .	USR	General role of all employees that have ability to read access
General Manager	GMUSR	Read/write access to timecard, price adjustment, scheduling
Services Manager	SMUSR	Read/write access to the price adjustment
Sales Expert	SEUSR	Read access to prices
Merchandise Sales Manager	MSMUSR	Price adjustment, discount validation, employee checkout
Operation Manager	OMUSR	Read/write to price adjustment, employee checkout, inventory adjustment
Retail Manager	RMUSR	Read/write to price adjustment, employee checkout, timecards
Lead Cashier	LCUSR	Read/write to price adjustment and employee checkout
Store Associate	SAUSR	Only read access to new guest sign up, guest checkout

Employee Role Assignment Structure

All employees have role assigned to their title that are described in the table below:

Position Title	Role Set
General Manager	{USR,GMUSR}
Services Manager	{USR,SMUSR}
Sales Expert	{USR,SEUSR}
Merchandize Sales Manager	{USR,MSMUSR}
Operations Manager	{USR,GMUSR,OMUSR}
Retail Manager	{USR,GMUSR,RMUSR}
Lead Cashier	{USR,LCUSR}
Store Associate	{USR,SAUSR}

Organizational Objects

The various objects that are held by the UB Inc. and are protected by access control are described in the table below:

Object Name	Description
Guest user database	Database contains all the information of UB Inc. customers including their name, address, DOB and history of purchase
Merchandize Prices	Merchandize that is marked at a certain price by the corporate
Timecards	Time logs of employees, clocking in and out, lunch breaks
Employee database	Database contains all the information of employee information and history of purchase
Sales Transactions	Merchandize that is being purchased by a guest
Inventory	Number of items of sales merchandize
Budget	Allocation of budget towards goals and employees
Floor Plan	Floor plan set up by corporate for better sales
Workstations/register	Workstation for sales transactions

1. **Discretionary Access Control**

Within UB Inc., DAC has been implemented on various objects. Two objects that are controlled by DAC are timecards and sales transactions. It reduces the work load for a manager of assigning

permissions by giving the owner the ability to assign permissions on their own. Sale transactions are frequently by the employees. Mandatory Access Control based will not be suitable for these two objects as it may take forever if the manager were to give permission each time.

Nomenclature:

S = Set of all Subjects $\{S_1,S_2,\ldots..S_n\}$

O = Set of all objects $\{O_1,O_{2,\ldots\ldots}O_n\}$

P = Set of all permissions $\{P_{read}, P_{write,} P_{delete}, P_{owner}, P_{null,\ldots\ldots}P_n\}$

P_{owner} has owner permissions which is the ability to edit on any object and P_{null} is to no permissions.

Perm P = {red, write, create, edit}

Policy for Timecards and Sales transactions:

$\forall s \in S, o \in O$, $P_{read,} P_{write,} P_{delete}, P_{owner} \in P$

IFF S_1 => GRANT $(S_1,O_{1,}P_{owner})$ THEN ➔ GRANT $(S_2,O,P_{red/write},P_{delete}))== P_{owner}$

$\forall s \in S, o \in O$, P_{null} , $P_{owner} \in P$

IFF PERM (S_1,O_1, P_{null})➔ DENY

2. Secrecy Based Mandatory Access Control (MAC)

Secrecy Based MAC is system that is meant to protect sensitive data. At UB Inc. secrecy based MAC based control is used of Employee Checkout and Price Adjustments. These two are only accessible to subjects only that have desired clearance. Mangers and Lead cashier possess the access to these two information, they would be able to access the sensitive information. This helps against any unauthorized or illegal activity to happen unlike DAC.

Nomenclature:

S = Set of all Subjects $\{S_1,S_2,\ldots..S_n\}$

O = Set of all objects $\{O_1,O_{2,\ldots\ldots}O_n\}$

P = Set of all permissions $\{P_{read}, P_{write,} P_{delete}, P_{owner}, P_{null,\ldots\ldots}P_n\}$

R = Set of roles $\{R_{MGUSR},R_{SMUSR},R_{SAUSR,\ldots\ldots}R_n\}$

Policy for Employee Checkout and Price Adjustments:

$\forall s \in S, o \in O$, $R_{MGUSR} \in R$, $P_{write} \in P$

IFF ROLE(R_{GMUSR})➔Object($O_{price\ adjustment/employee\ checkout}$)➔ALLOW

IFF ROLE(R_{SAUSR})➔ Object($O_{price\ adjustment/employee\ chechout}$) ➔DENY

3. Integrity Based Mandatory Access Control (MAC)

Integrity based MAC provides assurance and protects against grant of lenient permission to subjects on accessible objects. This helps object from being compromised in a way and maintaining its integrity. Biba based model can catch integrity compromises due to improper information flow well. At UB Inc integrity based MAC is used as permission control on price adjustments and applying discounts. Given the nature of it, higher authorities such as managers or lead cashier should be trusted upon when it comes to making a decision.

Nomenclature:

S = Set of all Subjects {S_1,S_2,…..S_n}

O = Set of all objects {$O_{Price\ adjustment}$, $O_{discount}$}

P = Set of all permissions {P_{read}, $P_{write,}$ P_{delete}, P_{owner}, $P_{null,}$…….P_n}

R = Set of roles {R_{MGUSR},R_{SMUSR},$R_{SAUSR,}$……R_n}

Policy for price adjustment and discount application:

$\forall s \in S, o \in O$, R_{MGUSR} ,$R_{SAUSR} \in R$, $P_{write/read} \in P$

IFF R_{MGUSR}➔ $O_{price\ adjustement/discount\ application}$➔ $P_{read/write}$➔ALLOW

IFF R_{SAUSR}➔$O_{price\ adjustment/discount\ application}$➔$P_{null}$➔DENY

4. Role Based Access Control (RBAC)

RBAC policy control access to objects depending on the roles that subjects have with in a system and on rules stating the specific access permission allowed for subjects within those roles. At UB Inc, RBAC is used as a permission control system on workstation or register. All employees are given access to the workstation and registers and mobile devices.

Nomenclature:

S = Set of all Subjects $\{S_1, S_2, \ldots..S_n\}$
O = Set of all Objects $\{O_{workstation/mobile\ devices}\}$
R = Set of all roles $\{ R_{usr} \ldots..R_n\}$
P = Set of all permissions $\{P_{read,}\ P_{write} \ldots..P_n\}$

Policy for Workstation and mobile devices:

$\forall s \in S, o \in O$, $R_{USR} \in R$, $P_{write} \in P$

IFF $R_{usr} \rightarrow O_{workstations/mobile\ devices} \rightarrow P_{read} \rightarrow$ ALLOW

5. Attribute-based Access Control (ABAC)

ABAC is an access system where access permissions are granted to the subjects based on policies which contains attributes together. At UB Inc. ABAC model for access control is used for Guest User Database and Merchandize pricing. ABAC provides better control over the policies which is locked in RBAC. Since sales expert often need to access to merchandize pricing, they have the read access to the complete merchandize prices.

Nomenclature:

S = Set of all Subjects $\{S_1, S_2, \ldots..S_n\}$
O = Set of all Objects $\{O_{merchandize\ pricing}\}$
R = Set of all roles $\{R_{USR,} R_{SEUSR} \ldots R_n\}$
P = Set of all permissions $\{P_{read,}\ P_{write} \ldots..P_n\}$

Policy for Merchandize prices and Guest user Database:

$\forall s \in S, o \in O$, $R_{SEUSR} \in R$, $P_{read} \in P$

IFF $R_{SEUSR} \rightarrow O_{merchandize\ pricing} \rightarrow P_{read} \rightarrow$ ALLOW

6. Separation of Duties

At UB Inc. the separation of duty model is practiced to control access to the budget. The budgeting department at UB Inc is salary and profit. The object belonging to the budgeting can only be accessed by the team. The separation of duty makes the budgeting

much more efficient as only one or two employees will have access to it which makes it more coherent and less prone to errors.

Nomenclature:

S = Set of all Subjects $\{S_1, S_2, \ldots..S_n\}$
O = Set of all Objects $\{O_{budgteting}\}$
R = Set of all roles $\{R_{USR}, R_{GMUSR}\ldots.R_n\}$
P = Set of all permissions $\{P_{read}, P_{write}\ldots..P_n\}$

Policy for Budgeting:

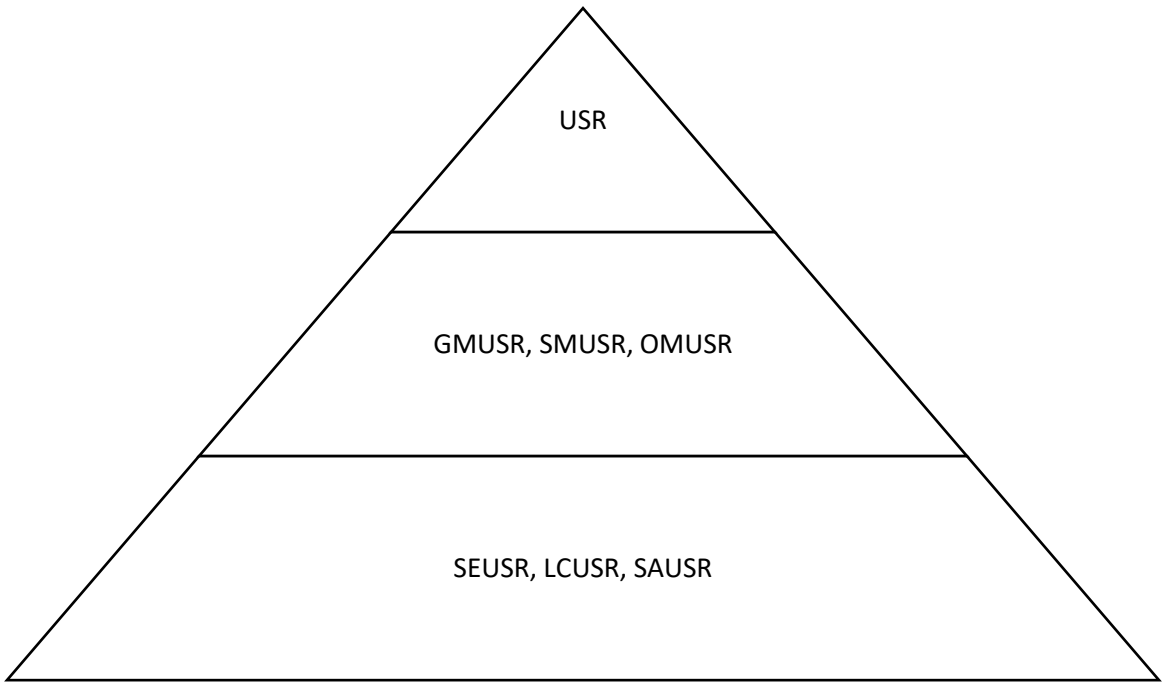
$\forall s \in S, o \in O$, $R_{MGUSR} \in R$, $P_{read} \in P$

IFF $R_{MGUSR} \rightarrow O_{budgeting} \rightarrow P_{read/write} \rightarrow$ ALLOW

IFF $R_{USR} \rightarrow O_{budgeting} \rightarrow P_{read/write} \rightarrow$ DENY

7. Hierarchical Relationship Policy

At UB Inc. user roles account is organized in a hierarchical structure, each employee is assigned a generic rule USR and then further roles are added based on the requirements of their jobs.



8. Applied Negative and Positive Permission

UB Inc. uses positive permission because of its closed nature of the permission and hierarchical layered structure. Negative permissions can be resource and time intensive to apply for all users, hence they were not used. Applied positive permission model is used for inventory. Operations Manager have the read/write access to the inventory.

Nomenclature

S = Set of all Subjects $\{S_1, S_2, \ldots..S_n\}$
O = Set of all Objects of inventory $\{O_1, O_2 \ldots O_n\}$
R = Set of all roles $\{R_{USR,ROMUSR \ldots} R_n\}$
P = Set of all permissions $\{P_{read,} P_{write \ldots..} P_n\}$

Policy for Inventory:

$\forall s \in S, o \in O$, $R_{OMUSR} \in R$, $P_{read} \in P$

IFF $R_{OMUSR} \rightarrow O_{Inventory} \rightarrow P_{read/write} \rightarrow$ ALLOW

IFF $R_{USR} \rightarrow O_{Inventory} \rightarrow P_{read/write} \rightarrow$ DENY

9. Temporal Authorization Policy:

Temporal authorization policies involve access permission that are constrained by time-based reasoning. At UB Inc. temporal authorization policies are used to control access to workstations by employees between 9 pm and 10 am everyday. This time slot has been determined to be only time when the store is closed to the customers. During this time the workstations are updated to avoid any crashing of the system.

Nomenclature:

S = Set of all Subjects $\{S_1, S_2, \ldots..S_n\}$
O = Set of all Objects $\{O_{budgteting}\}$

R = Set of all roles $\{R_{USR}, R_{GMUSR}, \ldots R_n\}$

P = Set of all permissions $\{P_{read}, P_{write}, \ldots P_n\}$

T = Set of all time $\{t_1, t_2 \ldots t_n\}$

Where t_1 = 9pm to 10 am , $t_2 = T - t_1$ (rest of the time)

Policy:

$\forall s \in S, o \in O$, $R_{USR} \in R$, $P_{read} \in P$

IFF $R_{USR} \rightarrow t_2 \rightarrow P_{read/write} \rightarrow$ ALLOW

IFF $R_{USR} \rightarrow t_1 \rightarrow P_{read/write} \rightarrow$ DENY

10. Administrative Policy

UB Inc. is a customer service oriented company and contains a lot data from the customers which included their history of purchases, mode of payments, personal information and hence the information security for the company need to be clean in order to protect a customer's information and be competitive in the market. UB Inc. used closed model for permission control with a layered hierarchical approach. This enables fine-grained control as well as an efficient way to obtain integrity and confidentiality, This document will allow employees in the organization to have a good understanding of policy structure. Meeting should be held annually to keep the employees up to date. If there is need to change the policy a proposal should be made to IT security team. If for any reason, the proposed policy revision gets denied, the proposal need to resubmitted to IT security.

References

[1] Access Control: Policy, Models and Mechanisms by Pierengela Samarati and Sabrina De Capitani di Vemercati http://www.drkodali.info/isa652/Pier01.pdf

11. UB Inc. Auditing Program

COBIT Domain	Control Category	COBIT Sub Domains	Policy	Test Codes
DS11 Manage Data PO4 Define IT Processes, organization and relationships	Discretionary Access Control (DAC)	DS11.6 Security Requirements for Data Management PO4.9 Data and System Ownership	• $\forall s \in S, o \in O$, P_{read}, P_{write}, P_{delete}, $P_{owner} \in P$ • IFF S_1 => GRANT (S_1,O_1,P_{owner}) THEN ➔ GRANT (S_2,O,$P_{red/write}$,P_{delete}))== P_{owner} • $\forall s \in S, o \in O$, P_{null} , $P_{owner} \in P$ • IFF PERM (S_1,O_1, P_{null})➔ DENY	a)Validate only creator of an Object on Timecard has read/write/delete and own permissions. b) Validate that the owner of an object within the timecars and sales transactions can grant write/owner permissions to the users. c)Validate when the owner of an object in the timecard and sale transactions grants P_{null} permission to a user, all the permission thereafter are revoked.
PO2 Define Information Architecture PO4 Define IT process, organization and relationships	Secrecy Based MAC	PO2.3 Data Classification Scheme PO4.6 Establishment of Roles and Responsibility AC3 Accuracy, completeness and authenticity checks	• $\forall s \in S, o \in O$, $R_{MGUSR} \in R$, $P_{write} \in P$ • IFF ROLE(R_{GMUSR})➔Object($O_{price\ adjustment/employee\ checkout}$)➔ALLOW • IFF ROLE($R_{SAUSR}$)➔ Object($O_{price\ adjustment/employee\ chechout}$) ➔DENY	a)Validate that when a subject's secrecy classification is lower that of the object in Employee Checkout the the object cannot be allowed to read and write. b)Validate that if secrecy level of subject is higher in Employee Checkout, then the subject can both read and write to it.

PO2 Define Information Architecture AC3 Accuracy, Completeness and Authenticity Checks AC4 Processing Integrity and Validity	Integrity Based MAC	PO2.4 Integrity Management DS9.3 Configuration Integrity Review	• $\forall s \in S, o \in O$, R_{MGUSR} ,$R_{SAUSR} \in R$, $P_{write/read} \in P$ • IFF $R_{MGUSR} \rightarrow O_{price\ adjustement/discount\ application} \rightarrow P_{read/write} \rightarrow$ ALLOW • IFF $R_{SAUSR} \rightarrow O_{price\ adjustment/discount\ application} \rightarrow P_{null} \rightarrow$ DENY	a)Validate that when a subject's classification is lower than that of the object on Price Adjustment the then the subject cannot be allowed to read and write on the object. b)Validate that when subjects classification is higher than the object then the subject can read and write on it.
DS9 Manage the Configuration DS5 Ensure Systems Security	Roles Based Access Control (RBAC)	DS5.3 Identify Management	• $\forall s \in S, o \in O$, $R_{USR} \in R$, $P_{write} \in P$ • IFF $R_{usr} \rightarrow O_{workstations/mobile\ devices} \rightarrow P_{read} \rightarrow$ ALLOW	a)Validate that all users can read on the workstations that are provided.
PO4 Define IT process, organization and relationships DS11 Manage Data	Attribute Based Access Control (ABAC)	PO4.6 Establishment of Roles and Responsibility Ds5.4 User Account Management	• $\forall s \in S, o \in O$, $R_{SEUSR} \in R$, $P_{read} \in P$ • IFF $R_{SEUSR} \rightarrow O_{merchandize\ pricing} \rightarrow P_{read} \rightarrow$ ALLOW	a)Validate that all sales expert can read on merchandizing pricing. b)Validate that all can users cannot write on the merchandize pricing.
PO4 Define IT process, organization and relationships DS11 Manage Data	Separation of Duties	PO4.11 Segregation of Duties PO4.6 Establishment of Roles and Responsibility	• $\forall s \in S, o \in O$, $R_{MGUSR} \in R$, $P_{read} \in P$ • IFF $R_{MGUSR} \rightarrow O_{budgeting} \rightarrow P_{read/write} \rightarrow$ ALLOW IFF $R_{USR} \rightarrow O_{budgeting} \rightarrow P_{read/write} \rightarrow$ DENY	a)Validate that only general manager can read and write on budgeting. b)Validate that access is denied to any other subject.

PO4 Define IT proccesses	Hierarchical Relationships	PO4.5 IT Organizational Structure PO4.10 Supervision	Refer to section 7.	a)Validate that periodic reviews are conducted to measure the impact of organizational change as that affect the overall organization. b)The skills, experience, authority, responsibility for each task is formalized.
DS11 Manage Data ME2 Monitor and Evaluate Internal Control	Positive and Negative Permissions	ME2.3 Control Expectations PO4.6 Establishment of Roles and Responsibilities PO4.11 Segregation of duties	• $\forall s \in S, o \in O$, $R_{OMUSR} \in R$, $P_{read} \in P$ • IFF $R_{OMUSR} \rightarrow O_{Inventory} \rightarrow P_{read/write} \rightarrow$ ALLOW • IFF $R_{USR} \rightarrow O_{Inventory} \rightarrow P_{read/write} \rightarrow$ DENY	a)Validate that subjects assigned to Inventory have the read and write ability. b)Validate that subject not assigned Inventory cannot read and write on it.
DS13 Manage Operations	Temporal Authorization policy	DS13.2 Job Scheduling DS13.5 Preventative Maintenance of Hardware	• $\forall s \in S, o \in O$, $R_{USR} \in R$, $P_{read} \in P$ • IFF $R_{USR} \rightarrow t_2 \rightarrow P_{read/write} \rightarrow$ ALLOW • IFF $R_{USR} \rightarrow t_1 \rightarrow P_{read/write} \rightarrow$ DENY	a)Validate that no subject can access to the workstations between 9pm and 10am EST.
DS13 Manage Operations PO1 Define a Strategic IT Plan	Administrative Policy	PO4.2 IT Strategic Committee DS13.1 Operations, Procedures And Instruction	Refer to section 10.	a)Validate that support personal are trained in operational procedures and related tasks for which they are responsible. b)Validate that segregation of duties is in line with the associated risk, security and audit requirements. c)Validate that procedures and

				responsibilities are well documented.