DATA AND WEB DEVELOPMENT

[CC6012NI]

WEEK - 07

Database Security

Definition

Database Security concerns the use of broad range of INFORMATION SECURITY controls to PROTECT databases against compromises of CONFIDENTIALITY, INTEGRITY AND AVAILABILITY.

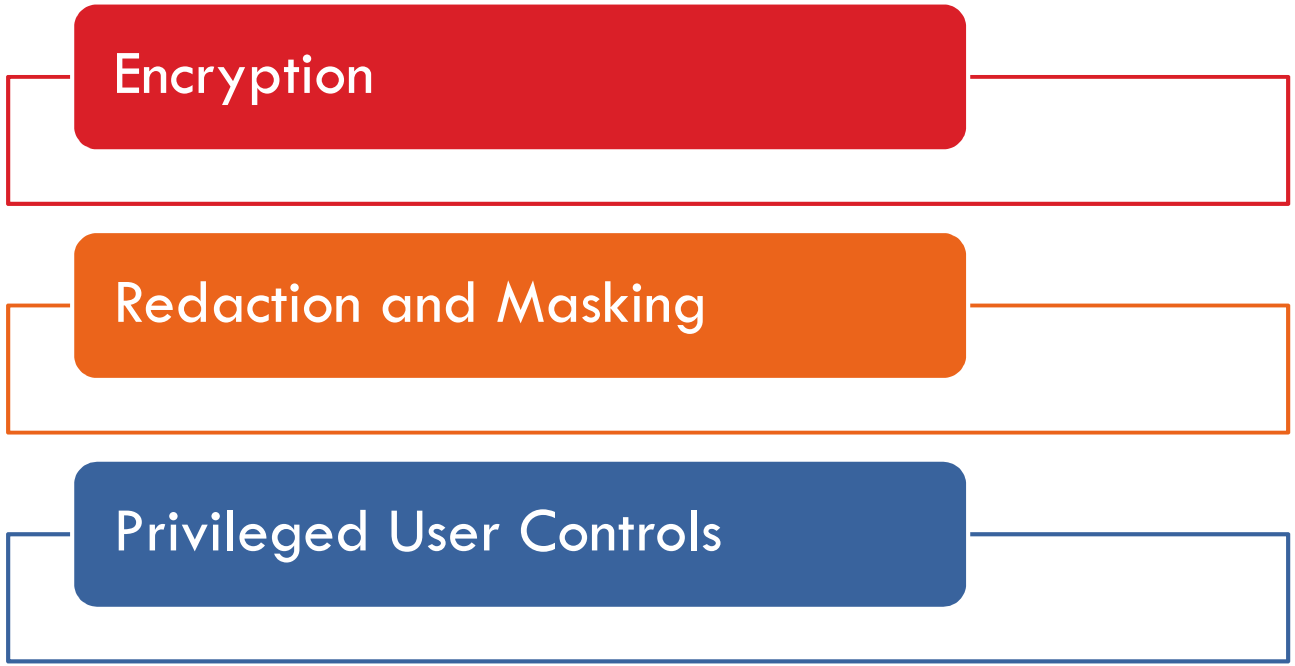
Definition

Database security covers and enforces security on all aspects and components of database. This includes

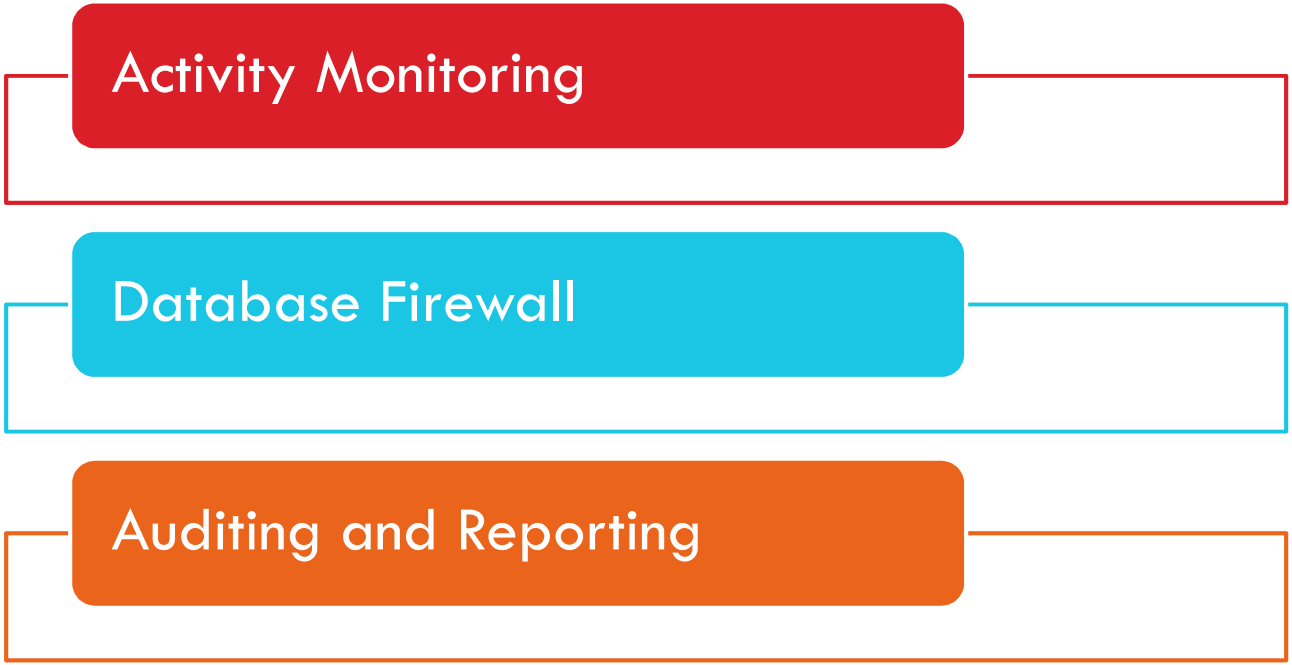
- Data Stored in Database
- Database Server
- Database Management System
- Other Database Associated Applications

Oracle Database Security Solutions

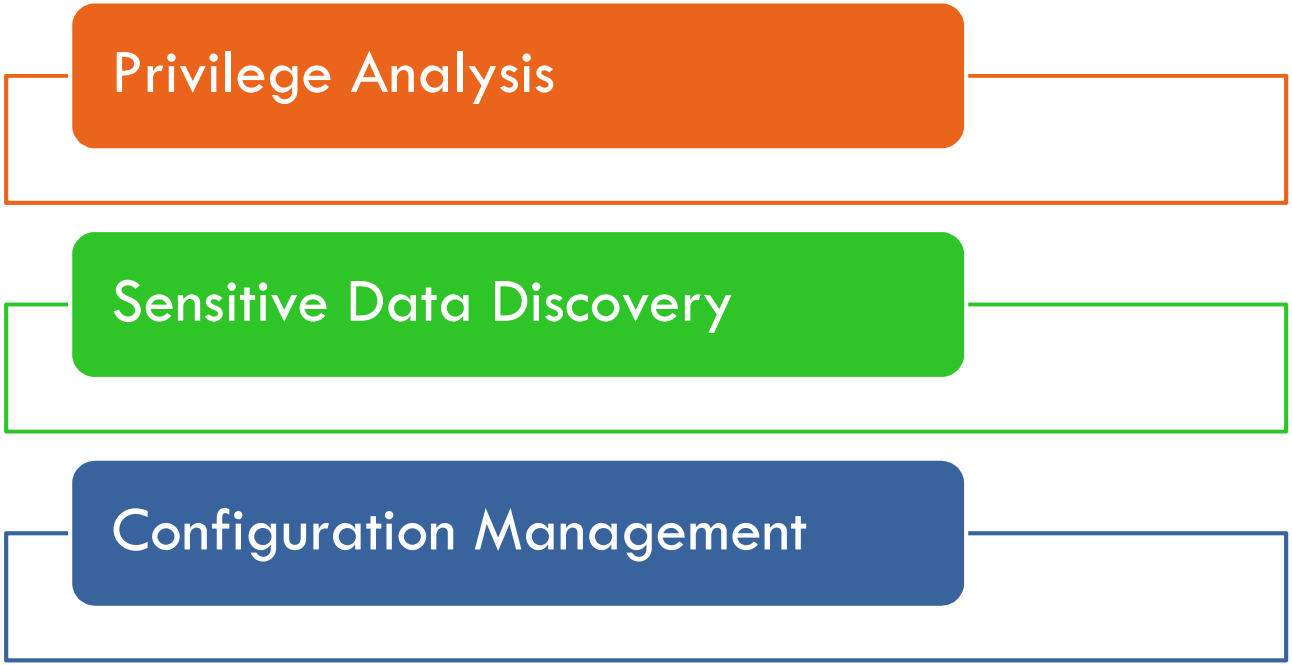
Preventive Security Solution



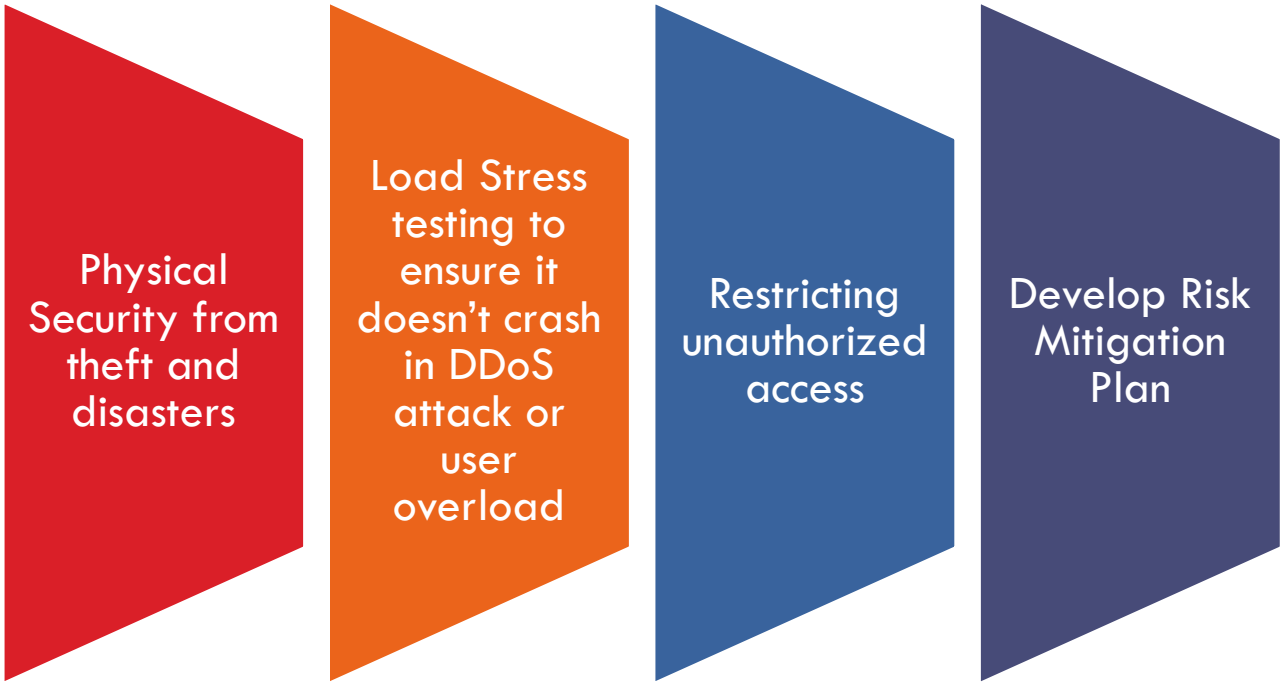
Detective Security Solution



Administrative Security Solution



Ways of Security Implementation



Security VERSUS Integrity

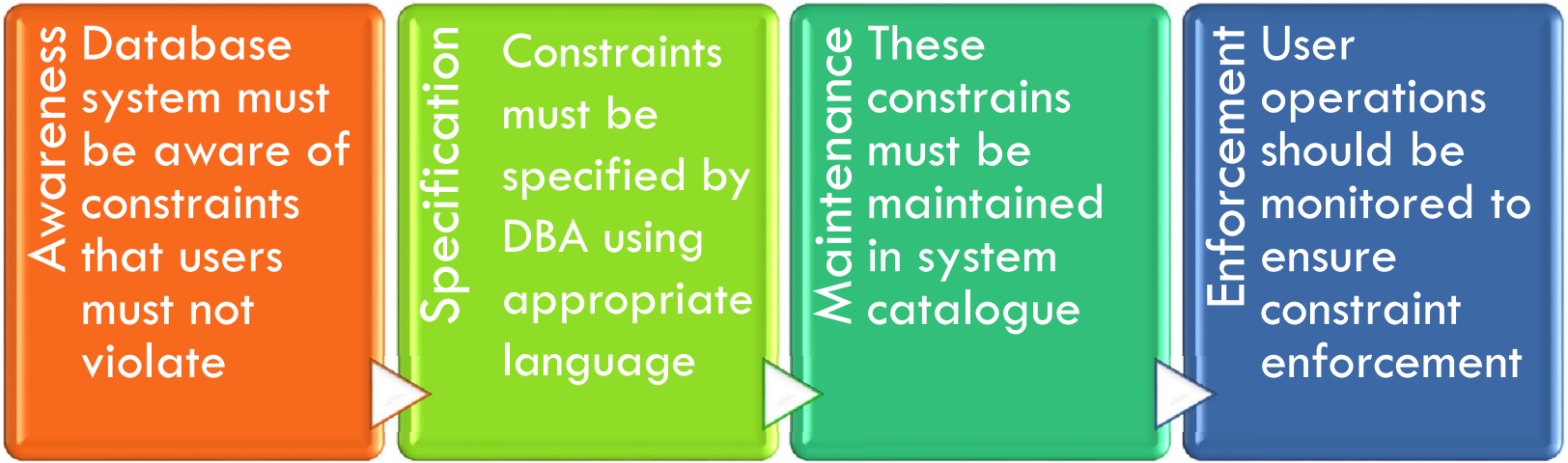
Database Security

How to protect data from unauthorized use

Database Integrity

How to ensure accuracy or validity of data

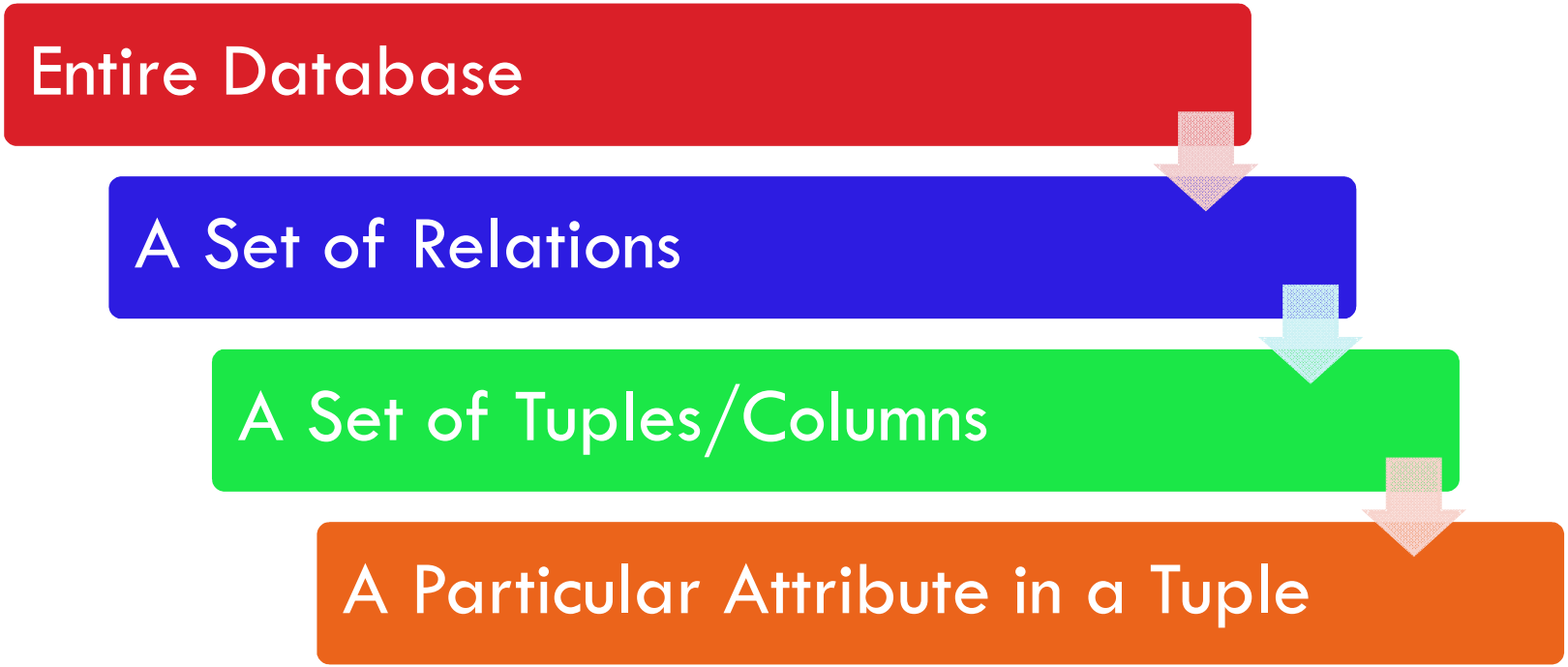
Security VERSUS Integrity - Commons



Access Request - Aspects

- User
  - Requesting access
- Operation
  - Insert, update, delete
- Data Object
  - Table, Views, Columns

Granularity of Data Object



Authorization Sub System

Provided by database security mechanism to check and verify user's identity for ensuring the security of database against unauthorized access

Authorization Sub System

- Before accessing database, a user must
  - Identity themselves
  - Authenticate their identification
  - Additional information may also be asked

Database Security Approaches

Discretionary Access Control

Control is exercised by assigning users different access rights on different data objects

Mandatory Access Control

Control is exercised by assigning data objects classification levels and assigning users with clearance levels

Discretionary Access Control Methods

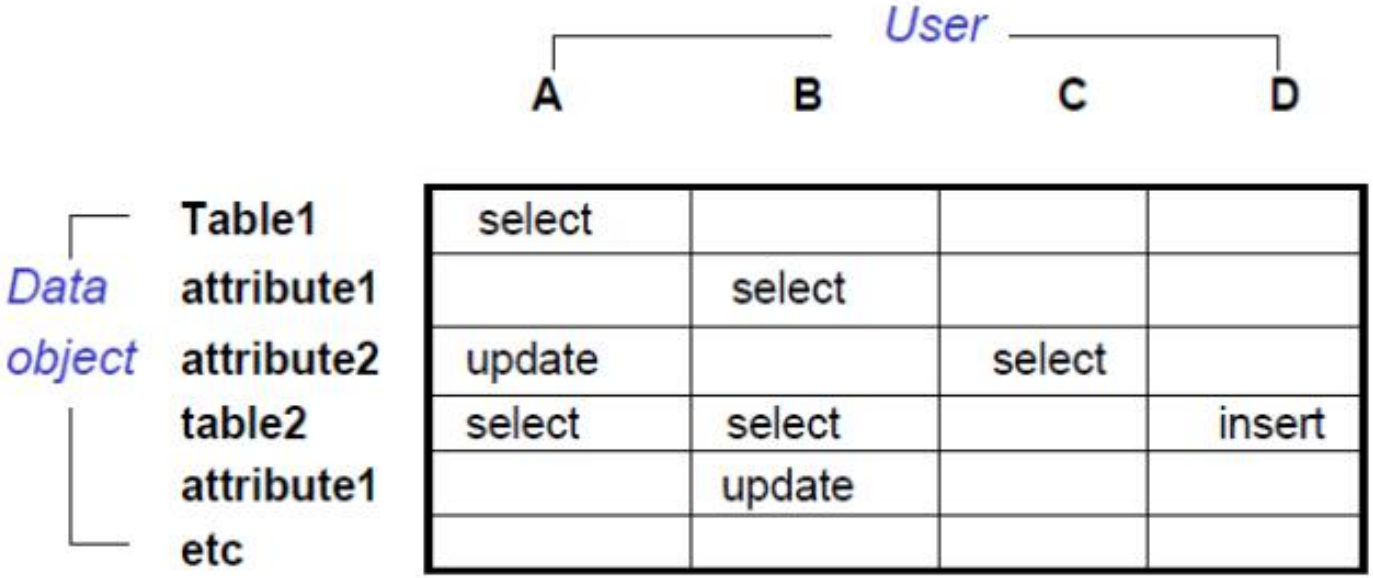
Access Matrix

Uses table(s) to specify access privilege for different users on different data objects

Security Rules

Uses a suitable language to specify user's access rights

Access Matrix - Example



Access Matrix - Example

	User Roles															
	DB Administration				Management				Sales				Shipping			
Tables	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D
Category	X	X	X	X		X				X				X		
CityTax	X	X	X	X		X				X				X		
CustDemog	X	X	X	X		X			X	X	X			X		
Customer	X	X	X	X		X			X	X	X			X		
Demographic	X	X	X	X		X				X				X		
OrderLine	X	X	X	X		X	X		X	X	X			X	X	
Order	X	X	X	X		X	X		X	X	X			X		
Preferences	X	X	X	X		X	X			X	X			X	X	
ProdCat	X	X	X	X		X				X				X		
Product	X	X	X	X		X				X				X		
References	X	X	X	X		X				X				X		
SalesUnit	X	X	X	X		X				X				X		

Access Matrix - Example

Access Matrix may contain many empty cells, hence it's information may be stored as User Profile or Object Profile

User Profiles (from the example)	
User A	table1:select; table1, attr2:update; table2:select
User B	table1,attr1:select; table2:select; table2, attr1:update
Object Profiles (from the example)	
Table 1	userA:select
Table 2	userA:select; userB:select; userD:insert

Security Rules

Supported by SQL standard and facilitated by two statements GRANT and REVOKE

GRANT operation

ON data object

TO user(s)

Violation response

Security Rules - Examples

Value Independent Rules

- **GRANT SELECT ON TABLE Employee TO Ram, Shyam, Hari;**

Value Dependent Rules

- GRANT SELECT ON TABLE Supplier where Supplier-city = 'London' TO Ganesh;

Context Dependent Rules

- **GRANT UPDATE ON TABLE Product WHEN Day() in ('Mon', 'Tue', 'Wed', 'Thu', 'Fri') AND Now() >= Time '09:00:00' AND NOW() >= Time '17:00:00' TO Order-Dept;**

Security Rules - Examples

REVOKE – Deletion of Security Rules

```
REVOKE SELECT ON TABLE Employee FROM Ram;
REVOKE UPDATE ON TABLE Employee FROM Ram;
REVOKE DELETE ON TABLE Employee FROM Ram;
REVOKE INSERT ON TABLE Employee FROM Ram;
```

Security Rules - Examples

REVOKE – Deletion of Security Rules

```
REVOKE SELECT, INSERT ON TABLE Employee FROM Ram;
```

```
REVOKE ALL ON TABLE Employee FROM Ram;
```

Mandatory Access Control

- Enhances security of database
- Gives consistent view of operations
- Adds to complexity

Mandatory Access Control

Examples

- Statistical analysis of medical records (providers and researchers have different view of same data)
- Accounting records (updated by structured programs and accessed by unstructured programs)

Mandatory Access Control - Example

User	Clearance level
Directors:	*4 (top secrecy)*
Senior managers	*3*
Managers	*2*
Authorised clerks	*1*
Anybody	*0*

Objects	select	update	delete
table 1	2	3	4
attribute 1	1	2	3
attribute 2	1	2	2
table 2	1	1	2
attribute 1	0	1	1

Mandatory Access Control - Classification

- What is Manager's access rights ?
  - Select table 1 and 2
  - Update table 2 and attributes 1 and 2 of table 1
  - Delete table 2 and attribute of table 1

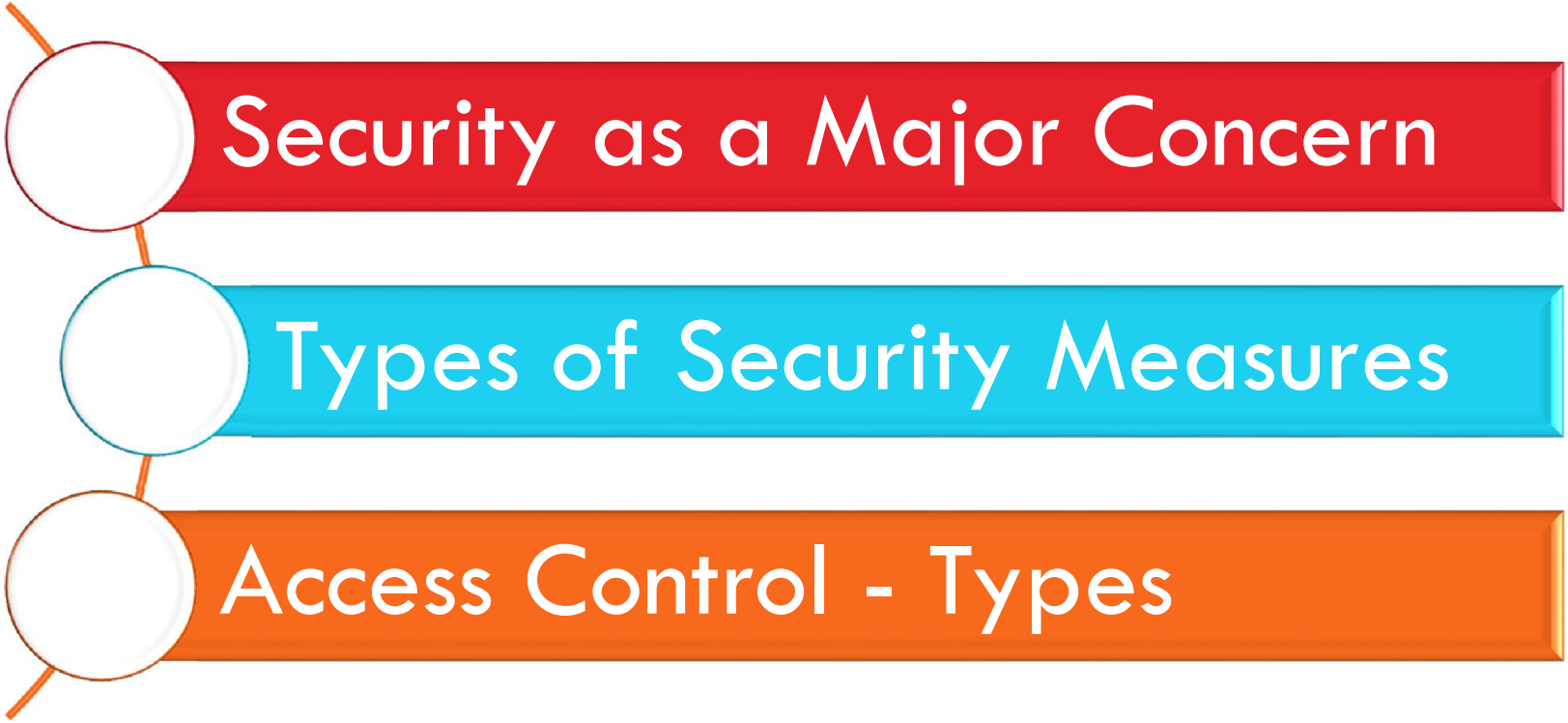
Mandatory Access Control - Questions

- Is manager allowed to delete a data item from the attribute 1 of table 1 ?

Mandatory Access Control - Questions

- Who can select attribute 1 of table 2?

SUMMARY


Security as a Major Concern
Types of Security Measures
Access Control - Types

Thank You