Enterprise Information System (EIS)

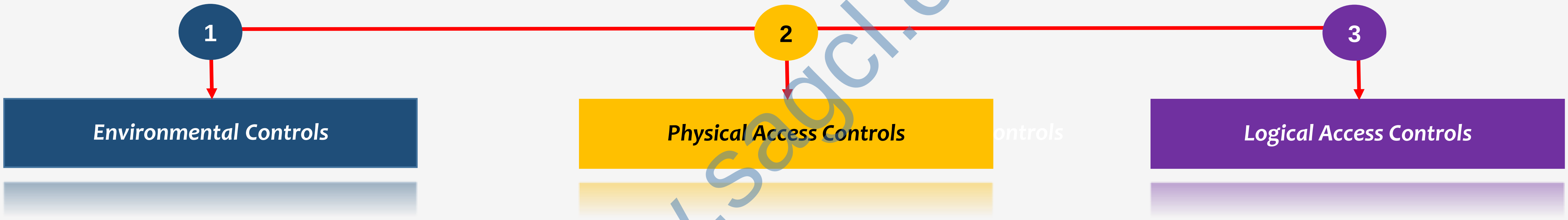
Chapter 3

Information Systems and Its Components

Classification based on “Nature of Information System (IS) Resources”

Information Systems and Its Components

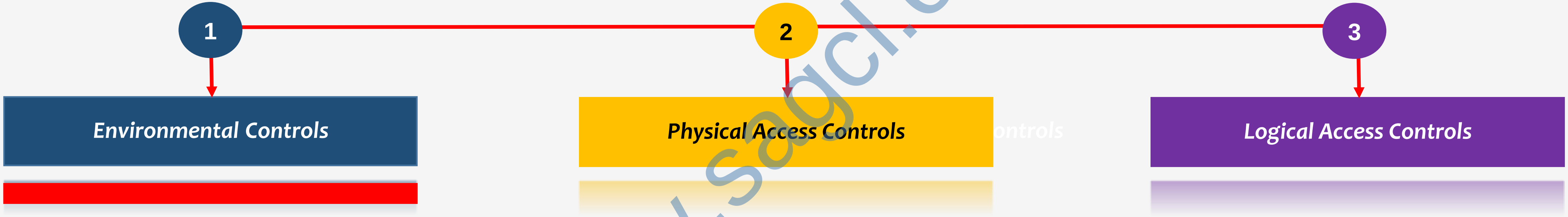
Classification of Information Systems’ Controls



Classification based on “Nature of Information System (IS) Resources”

Information Systems and Its Components

Classification of Information Systems' Controls



1

Environmental Controls

2

Physical Access Controls

3

Logical Access Controls

Classification based on "Nature of Information System (IS) Resources"

Classification based on "Nature of Information System (IS) Resources" : 1. Environmental Controls

Information Systems and Its Components

Classification based on “Nature of Information System Resources”

A

Fire Damage

B

Water Damage

C

Pollution Damage

D

Power Spikes

1 **Environmental Controls**

Information Systems and Its Components

Classification based on "Nature of Information System Resources"

Environmental Controls

A	Fire Damage
1	*Location of computer room:* *NOT in basement or ground floor of multi-storied building*
2	*Fire resistant materials:*
a.	■ *Use of less wood and plastic in computer room*
b.	■ *Fireproof walls, floors and ceiling surrounding the computer room*
c.	■ *Use of fire resistant material such as wastebaskets, curtain, desks, cabinets*
3	*Wiring placed in the fire resistant electrical panel and conduit*
4	*Smoke detectors:* *Above and below ceiling tiles, on activation – Audible alarm and linked to monitoring station*
5	*Fire Alarms:* *Manual and automatic with control panel*
6	*Fire suppression system:* *a. Dry pipe sprinkling system b. Water based system c. Gas based system d. Halon*
7	*Manual fire extinguishers*
8	*Regular inspection by fire department*
9	*Procedural manual for staff members to use the fire system*
10	*Documented and tested emergency evacuation plan*

1. Environmental Controls :: [A] Fire Damage

Information Systems and Its Components

Classification based on “Nature of Information System Resources”

Environmental Controls

B	Water Damage
1	Location of computer room: Flood area - NOT in basement or top floor of multi-storied building
2	Use of waterproof walls, ceilings and floors
3	Water proofing
4	Adequate drainage system
5	Water detectors: Audible alarm heard by security and central personnel to detect moistures and water
6	Use of water leakage alarm

REASON :: Water pipe bursts, Cyclones, Tornadoes, Floods etc.

1. Environmental Controls :: [B] Water Damage

Information Systems and Its Components

Classification based on “Nature of Information System Resources”

Environmental Controls

C	Pollution Damage
1	Air conditioner
2	Prohibiting eating, drinking and smoking within the information processing facility
3	Using separate slippers for computer room
4	Use of vacuum cleaner
5	Regular cleaning

1. Environmental Controls :: [C] Pollution Damage

Information Systems and Its Components

Classification based on "Nature of Information System Resources"

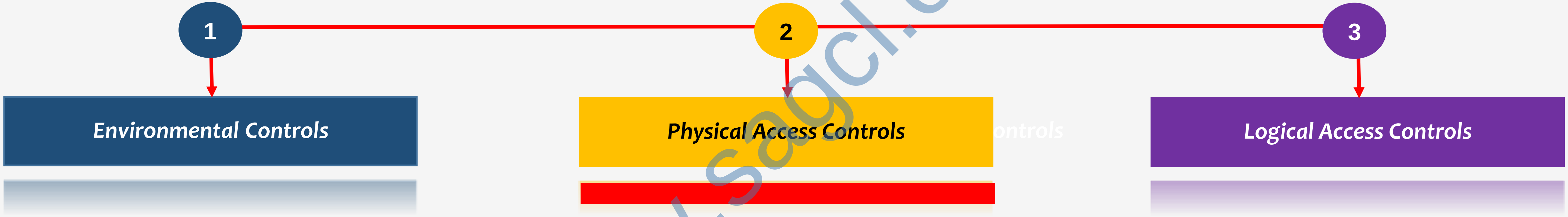
Environmental Controls

D	Power Spikes
1	Electrical surge protectors : Built into Un-interruptible Power System (UPS) for power spikes
2	Un-interruptible Power System (UPS) / Generators : Back-up power supply source, Flow for days or few minutes
3	Voltage regulators and circuit breakers : Protect hardware from temporary +/- power
4	Emergency power-off switch : Computer room fire or evacuation, easily accessible & secured from unauthorized access
5	Power lead from two sub-station : Ensure regular power supply in case of interruption

1. Environmental Controls :: [D] Power Spikes

Information Systems and Its Components

Classification of Information Systems’ Controls



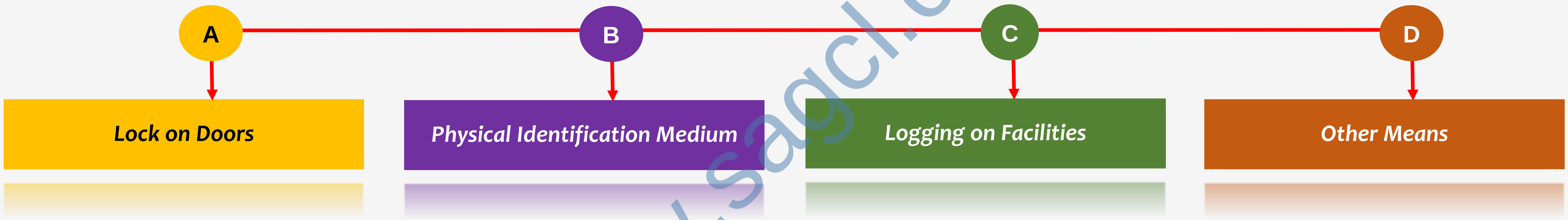
1. Environmental Controls
2. Physical Access Controls
3. Logical Access Controls

Classification based on “Nature of Information System (IS) Resources”

Classification based on "Nature of Information System (IS) Resources" : 2. Physical Access Control

Information Systems and Its Components

Classification based on “Nature of Information System Resources”



A — Lock on Doors

B — Physical Identification Medium

C — Logging on Facilities

D — Other Means

2 **Physical Access Controls**

Information Systems and Its Components

Classification based on "Nature of Information System Resources"

Physical Access Control

A	Lock on Doors
i	*Bolting door locks*
ii	*Cipher locks (Combination door locks)*
iii	*Electronic door locks*
iv	*Biometric door locks*

B	*Physical Identification Medium*
i	*Personal Identification Number (PIN)*
ii	*Plastic Cards*
iii	*Identification badges*

C	*Logging on Facilities*
i	*Manual logging*
ii	*Electronic logging*

D	*Other Means of Controlling Physical Access*
i	*Video Cameras*
ii	*Security Guards*
iii	*Controlled visitor access*
iv	*Bonded personnel*
v	*Dead man doors*
vi	*Non-exposure of sensitive facilities*
vii	*Computer terminal locks*
viii	*Alarm system*
ix	*Perimeter fencing*
x	*Control of out of hours of employees*
xi	*Secured report/ Document distribution cart*

2. Physical Access Controls

Information Systems and Its Components

Classification based on "Nature of Information System Resources"

Physical Access Control

A Lock on Doors

i Bolting door locks

- ▶ Metal key to open
- ▶ Key should not be duplicated

ii Cipher locks (Combination door locks)

- ▶ Ten digit numbered key mounted on door
- ▶ Used for low security area
- ▶ Many entry and exit points
- ▶ User uses 4 digit number
- ▶ Door open for ten to thirty seconds

iii Electronic door locks

- ▶ A magnetic or embedded chip based plastic key

iv Biometric door locks

- ▶ Uses a person's physical unique characteristic like fingerprint, hand geometry, eye scan or voice

2. Physical Access Controls :: [A] Lock on Doors

Information Systems and Its Components

Classification based on "Nature of Information System Resources"

Physical Access Control

B Physical identification medium

i Personal Identification Number (PIN)

- *Some means of identifying the individual provided*
- *Additionally a secret number inform of PIN provided*

ii Plastic Cards

- *Identification purpose*
- *Safeguard from not falling into unauthorized hands*

iii Identification badges

- *Special identification badges*
- *Identification of employees or visitors*
- *Use of color combinations*
- *Use of photo ID with electronic keys*

2. Physical Access Controls :: [B] Physical Identification Medium

Information Systems and Its Components

Classification based on "Nature of Information System Resources"

Physical Access Control

C Logging on Facilities

i Manual logging

Name	Company represented	Purpose of visit	Person to see	Contact No.	Time in	Time out	Signature

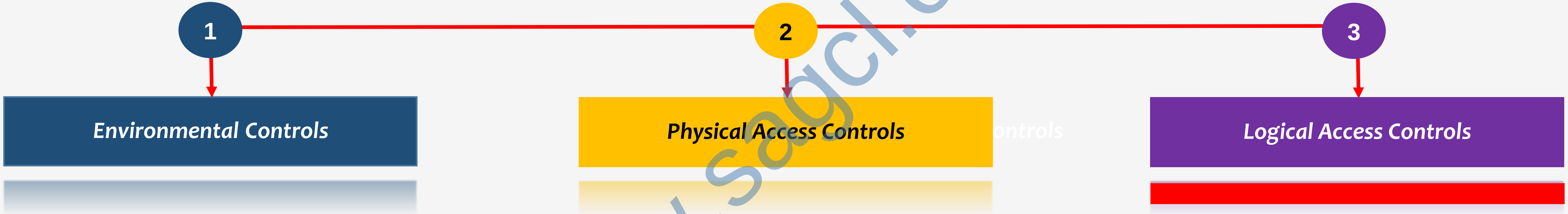
- Primarily used for visitors
- Logging may require both at reception or computer room
- Identification required – Driving license, business card, or vendor identification

ii Electronic logging

- Log in monitored and unsuccessful attempt highlighted

Information Systems and Its Components

Classification of Information Systems' Controls

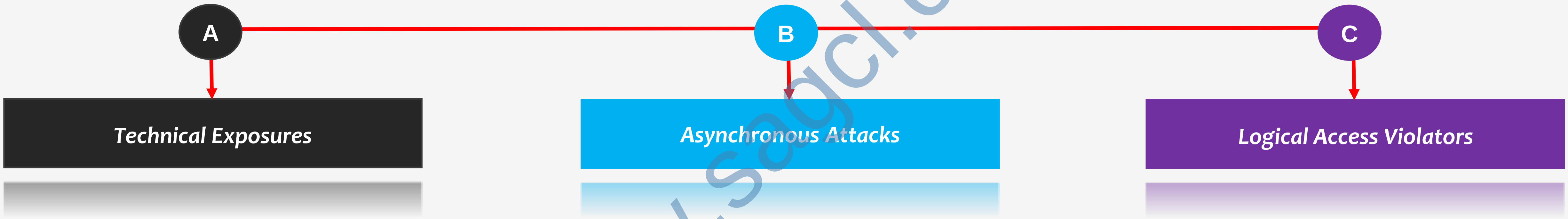


Classification based on "Nature of Information System (IS) Resources"

Classification based on "Nature of Information System (IS) Resources" : 3. Logical Access Controls

Information Systems and Its Components

Classification based on “Nature of Information System Resources”



Technical Exposures

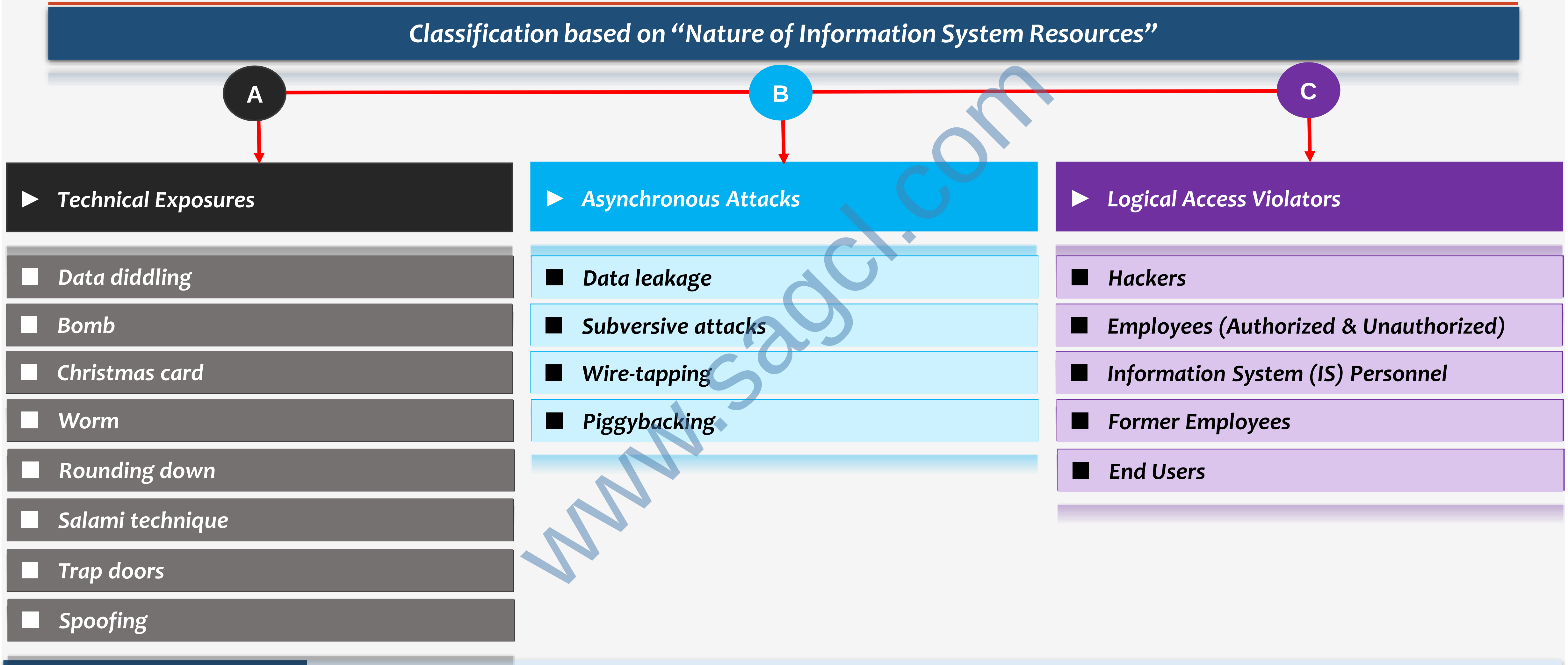
Asynchronous Attacks

Logical Access Violators

3

Logical Access Controls : Exposures

Information Systems and Its Components



Classification based on “Nature of Information System Resources”

A

▶ Technical Exposures

- □ Data diddling
- □ Bomb
- □ Christmas card
- □ Worm
- □ Rounding down
- □ Salami technique
- □ Trap doors
- □ Spoofing

B

▶ Asynchronous Attacks

- ■ Data leakage
- ■ Subversive attacks
- ■ Wire-tapping
- ■ Piggybacking

C

▶ Logical Access Violators

- ■ Hackers
- ■ Employees (Authorized & Unauthorized)
- ■ Information System (IS) Personnel
- ■ Former Employees
- ■ End Users

Information Systems and Its Components

Classification based on “Nature of Information System Resources”

A. Technical Exposures

■ Data diddling

- ■ Unauthorized altering of data before or after entering into computer system
- ■ Original information is changed by:
  - ▶ A person typing in the data ;
  - ▶ A virus programmed to change the data ;
  - ▶ The programmer of database or application ; or
  - ▶ Anyone involved in the process of creating, recording, encoding examining, checking, converting or transmitting data
- ■ Simplest method of committing, because even a computer amateur can do it
- ■ It occurs before computer security can protect the data

Information Systems and Its Components

Classification based on "Nature of Information System Resources"

A. Technical Exposures

Bomb

- It is a logic bomb in form of a piece of code inserted into an operating system or software application
- It is planted by an insider or supplier of a program
- A logical even triggers a bomb or it is time based
- These programs does not infect other programs
- These programs do not circulate by infecting other programs
- Logic bombs can also be used with viruses, worms, and trojan horses to time them
- These can do maximum damage before being noticed
- They perform actions like corrupting or altering data, reformatting a hard drive, and deleting important files.

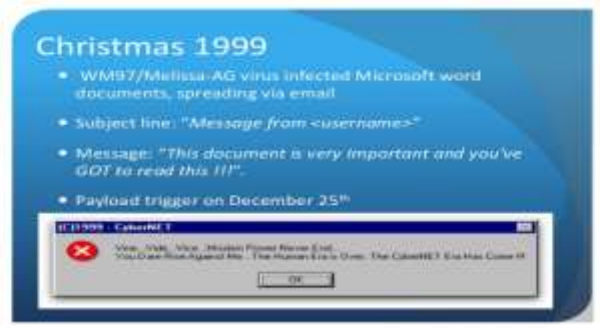
Information Systems and Its Components

Classification based on “Nature of Information System Resources”

A. Technical Exposures

■ Christmas Card

- It is a well known example of Trojan horse
- It was detected on internal E-Mail of IBM system
- On typing “Christmas”, it will draw the image of Christmas tree
- It will also send copies of similar output to other users connected to the network
- Other user can not save their half finished job because of this message



Christmas 1999

- WM97/Melissa-AG virus infected Microsoft word documents, spreading via email
- Subject line: *"Message from <username>"*
- Message: *"This document is very important and you've GOT to read this !!!".*
- Payload trigger on December 25th

ICQ1999 - CyberNET

Veni, Vidi, Vici ..Mission Power Never End...
You Dare Rise Against Me... The Human Era is Over. The CyberNET Era Has Come !!

Information Systems and Its Components

Classification based on "Nature of Information System Resources"

A. Technical Exposures

■ Worm

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers
- It does not require a host program in order for them to run, self-replicate and propagate
- A worm usually makes its way onto system, usually via a network connection or as a downloaded file
- it then make multiple copies of itself and spread via the network or internet connection infecting inadequately-protected computers and servers on the network

Information Systems and Its Components

Classification based on “Nature of Information System Resources”

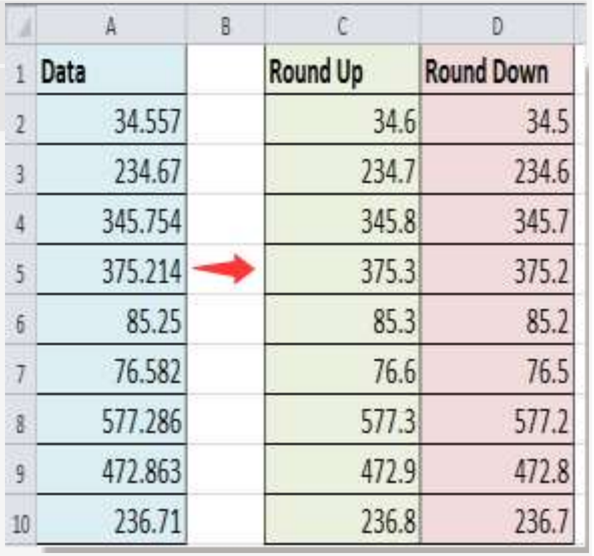
A. Technical Exposures

Rounding down

- Refers to rounding of small fractions of a denomination and transferring that small fractions into an unauthorized account
- Amount is small, it rarely gets noticed

Example

Instructing the computer to round down all interest calculations to two decimal points. The fraction of a cent rounded down on each calculation is put into the programmers’ account



	A	B	C	D
1	Data		Round Up	Round Down
2	34.557		34.6	34.5
3	234.67		234.7	234.6
4	345.754		345.8	345.7
5	375.214	→	375.3	375.2
6	85.25		85.3	85.2
7	76.582		76.6	76.5
8	577.286		577.3	577.2
9	472.863		472.9	472.8
10	236.71		236.8	236.7

Information Systems and Its Components

Classification based on "Nature of Information System Resources"

A. Technical Exposures

Salami Technique

- It is a slicing of a small amounts of money from a computerized transaction or account
- Example:
- The transaction amount 10,000. 69 is truncated to either 10,000.60 or 10,000.00

Information Systems and Its Components

Classification based on “Nature of Information System Resources”

A. Technical Exposures

- Trap doors

- Trap doors also called a backdoor is a means of accessing information resources that bypasses regular authentication and/or authorization
- The secret backdoor access is sometimes a planned installation by system developers or service providers as a remote means for diagnostics, troubleshooting or other system tests.
- Backdoor access can also be a system weakness or flaw or a malicious program which attackers can use to exploit the system and create their own backdoor.
- A backdoor virus, therefore, is a malicious code which, by exploiting system flaws and vulnerabilities, is used to facilitate remote unauthorized access to a computer system or program
- The system becomes vulnerable to illicit file copying, modification, data stealing, and additional malicious injections

Information Systems and Its Components

Classification based on “Nature of Information System Resources”

A. Technical Exposures

■ Spoofing

- A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls
- Some of the most common methods include IP address spoofing attacks, ARP spoofing attacks and DNS server spoofing attacks.
- A penetrator makes the user think that he/she is interacting with the operating system
- The penetrator duplicates the login procedure, captures the user’s password, attempts for a system crash and makes the user login

Information Systems and Its Components

Classification based on “Nature of Information System Resources”

B. Asynchronous Attacks

- Data leakage

▶ *This involved leaking of information out of the computer by means of dumping files to paper or stealing computer reports and tape.*

- Subversive attacks

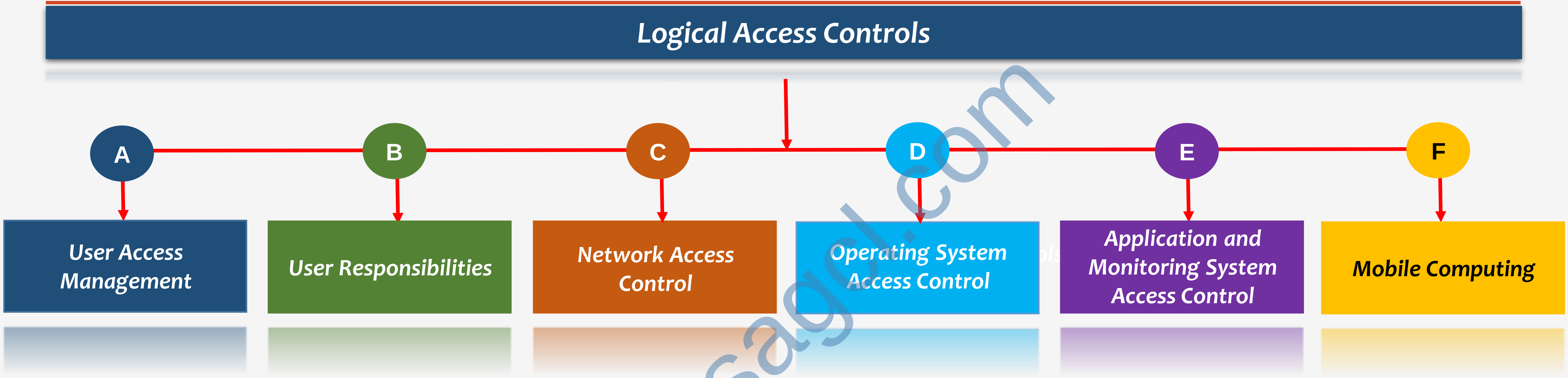
▶ *This can provide intruders with important information about messages being transmitted and the intruder may attempt to violate the integrity of some components in the sub-system.*

- Wire-tapping

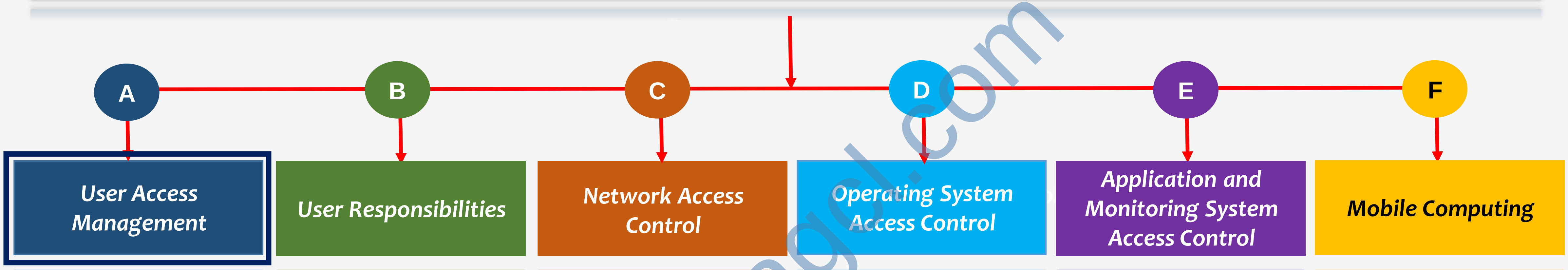
▶ *This involved spying on information being transmitted over communication network.*

- Piggybacking

▶ *This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions. This involves intercepting communication between the operating system and the user and modifying them or substituting new messages.*


Logical Access Controls
A
B
C
D
E
F
User Access Management
User Responsibilities
Network Access Control
Operating System Access Control
Application and Monitoring System Access Control
Mobile Computing

Logical Access Controls



User Registration

Privilege Management

User Password Management

Review of User Access Rights

Logical Access Control : Approach : : A. User Access Management

Logical Access Controls

A. User Access Management

User Registration

- User details documented for registration process
- Question – Who and why granted the question
- Data owner approved
- User accepted the responsibility
- De-registration process also documented

Privilege Management

- Access based on roles and responsibilities

User Password Management

- Allocations, storage, revocation and re-issue process
- Educating users

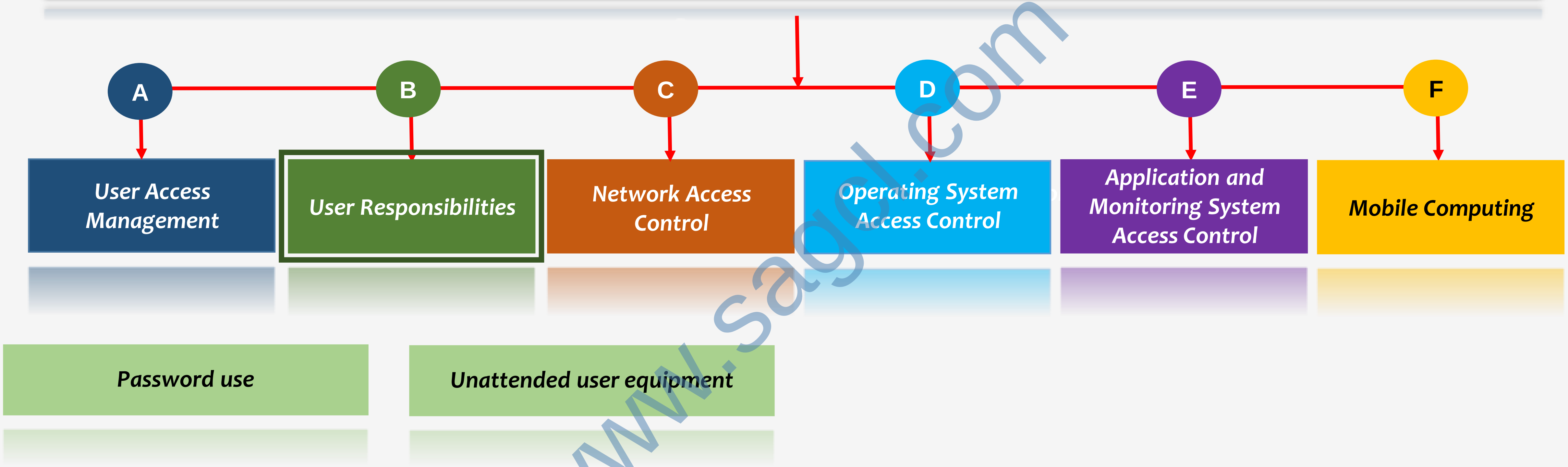
Review of User Access Rights

- Change and current job profile

Logical Access Control : Approach : : A. User Access Management

E-Commerce, M-Commerce and Emerging Technologies

Logical Access Controls



A

User Access Management

B

User Responsibilities

C

Network Access Control

D

Operating System Access Control

E

Application and Monitoring System Access Control

F

Mobile Computing

Password use

Unattended user equipment

3

Logical Access Control : Approach : : B. User Responsibilities

Logical Access Controls

B. User Responsibilities

Password use

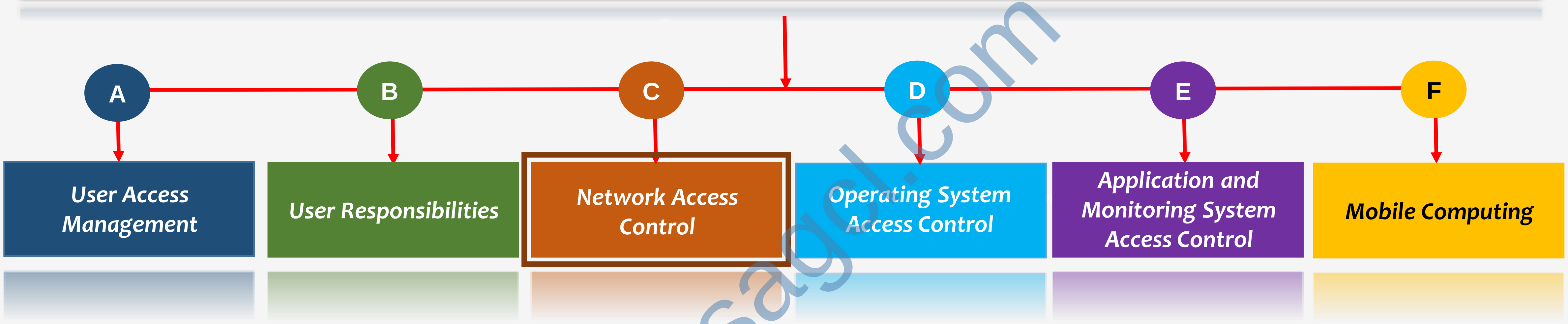
- Strong password
- Maintain the confidentiality

Unattended user equipment

- Equipment NOT left unprotected
- Securing by password
- NOT accessible to others

E-Commerce, M-Commerce and Emerging Technologies

Logical Access Controls



A User Access Management

B User Responsibilities

C Network Access Control

D Operating System Access Control

E Application and Monitoring System Access Control

F Mobile Computing

Policy on use of network services	Security of network services
Enforced paths	Firewall
Segregation of networks	Encryption
Network connection and routing controls	Call back devices

Logical Access Control : User Access Management

Logical Access Controls

C. Network Access Control

Policy on use of network services

- Policy for internet service requirement
- Alignment with business needs
- Selection of appropriate services
- Approval to access

Enforced paths

- Specify the exact path or route connecting the networks
- Internet access by employees routed through a firewall and proxy

Segregation of networks

- Sensitive information handling function e.g. VPN connection between head office and branch office
- Network isolated from the internet usage service

Network connection and routing controls

- Traffic between networks restricted
- Basis policy of source and authentication access

Logical Access Control : Approach : : C. Network Access Control

Logical Access Controls

C. Network Access Control

Security of network services

- Authentication and authorization process
- Implemented across the organization's network

Firewall

- Enforces access control between two networks
- All external traffic passes through it.

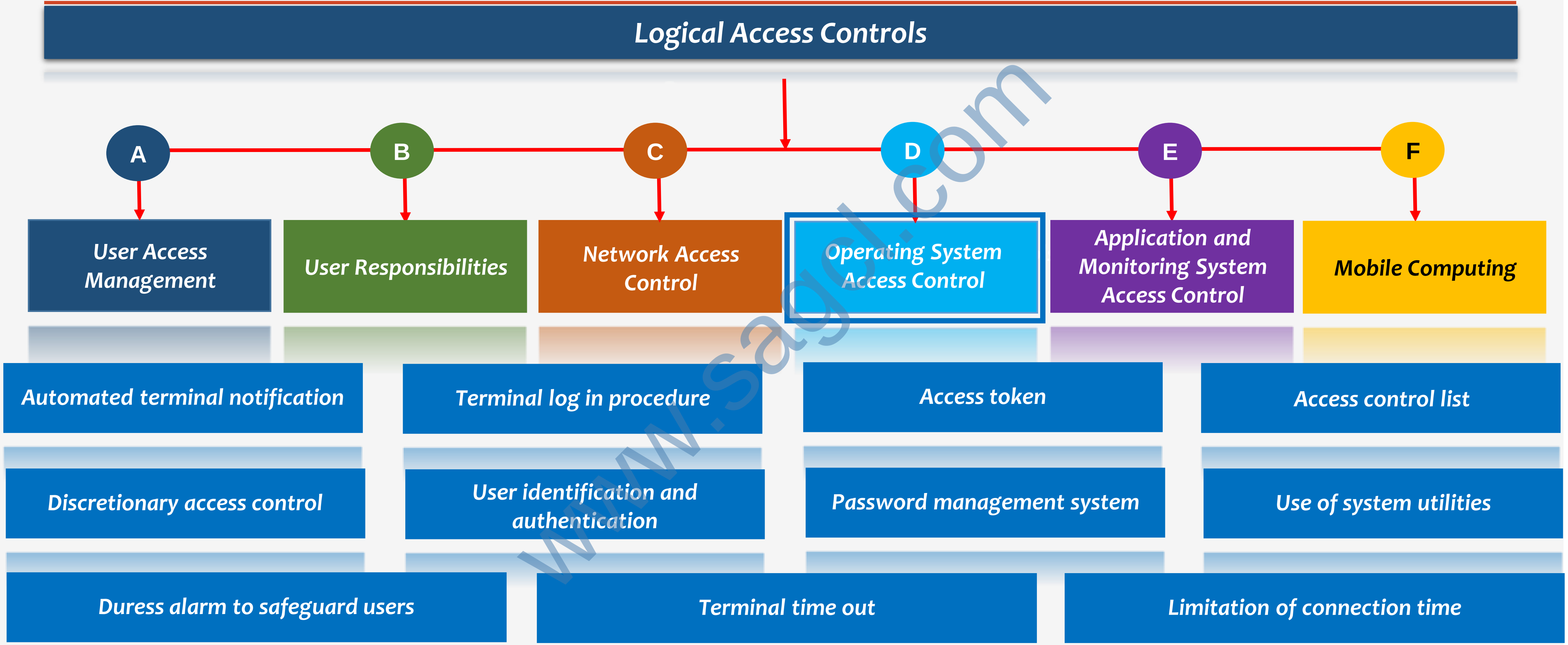
Encryption

- Transmission over network through encryption and decryption
- Clear text into cipher text
- Use of private key and private key for encryption and decryption

Call back devices

- Principle of keeping the intruder off the intranet rather post connected to the intranet
- It requires user to enter a password, then system breaks the connection
- On authentication, call back device dials the callers' number to establish the new connection

E-Commerce, M-Commerce and Emerging Technologies



Logical Access Controls

A – User Access Management

B – User Responsibilities

C – Network Access Control

D – Operating System Access Control

E – Application and Monitoring System Access Control

F – Mobile Computing

- Automated terminal notification
- Terminal log in procedure
- Access token
- Access control list
- Discretionary access control
- User identification and authentication
- Password management system
- Use of system utilities
- Duress alarm to safeguard users
- Terminal time out
- Limitation of connection time

4

Logical Access Control : Approach : : D. Operating System Access Control

Logical Access Controls

D. Operating System Access Control

Automated terminal notification

- Specified session can be initiated from a certain location or computer terminal

Terminal log in procedure

- Matching of User ID and password with login credentials for authorization

Access token

- Access token contains:
  - User IDs
  - Password
  - User group
  - Privileges granted

Access control list

- Contains about the access privileges
- Compares with access token

Logical Access Controls

D. Operating System Access Control

Discretionary access control

- Resource owner granted discretionary access control
- Grant access privileges to other users

User identification and authentication

- Users identified and authenticated
- Stringent methods like Biometric authentication, or cryptographic means like digital certificates

Password management system

- Enforcement of selection of strong password
- Internal storage uses one way hashing algorithms
- Password file not accessible to users

Use of system utilities

- Contains about the access privileges
- Compares with access token

Logical Access Controls

D. Operating System Access Control

Duress alarm to safeguard users

- Users forced to execute some instructions under threat, system provides a mean to alert the authorities

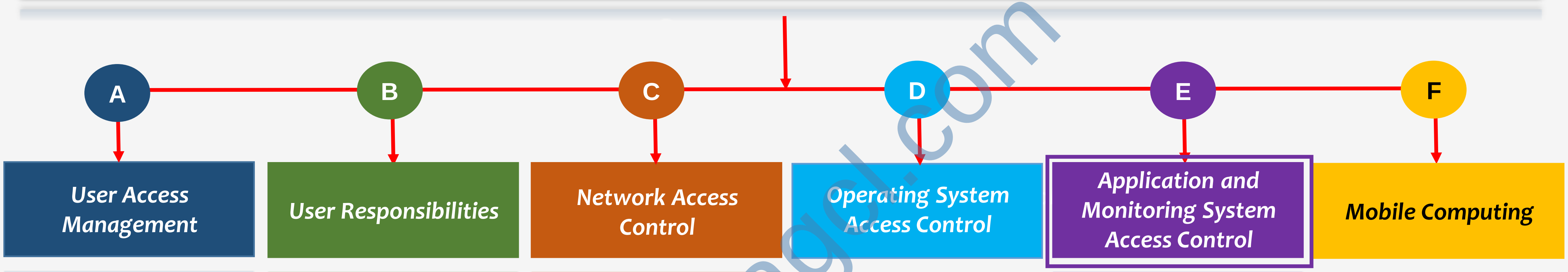
Terminal time out

- Terminal inactive for a defined period, logs out the user
- Prevent misuse in absence of the legitimate user

Limitation of connection time

- Define the available time slot
- DO NOT allow transactions beyond this time

Logical Access Controls



Information access restriction	Sensitive system isolation	Event logging	Monitor system use	Clock synchronization

Logical Access Controls

D. Operating System Access Control

Information access restriction

- Access based on authorization
- Read, write, delete and execute

Sensitive system isolation

- Criticality of system constitution, run the system in isolated environment
- Detective control – monitoring system access and use
- Detect and report unauthorized activities

Event logging

- Enable logging and archiving the logs
- Intruder using combinations of log in id and password
- All logs recorded
- Completed details along-with terminal locations recorded

Monitor system use

- Monitoring of critical system
- Details of type of accesses, operations, events, and alerts
- Extent of details and frequency of review
- Periodical review of logs
- Attention for gaps in the logs

Clock synchronization

- Synchronizing clock time across the network as per standard time mandatory

Logical Access Control : Approach : : E. Application & Monitoring System Access Control

Thanks

Sudarshan™
Agrawal
Classes