

- Context: the Big Picture
- User Access
- Audit Trails
- Encrypting Data At-rest

In-Scope: corporate user access via on-premise applications and databases.

Out-of-Scope: Internet user access, e.g., .com, Cloud computing, Privileged access, e.g., DBAs.

Scope Illustrated...

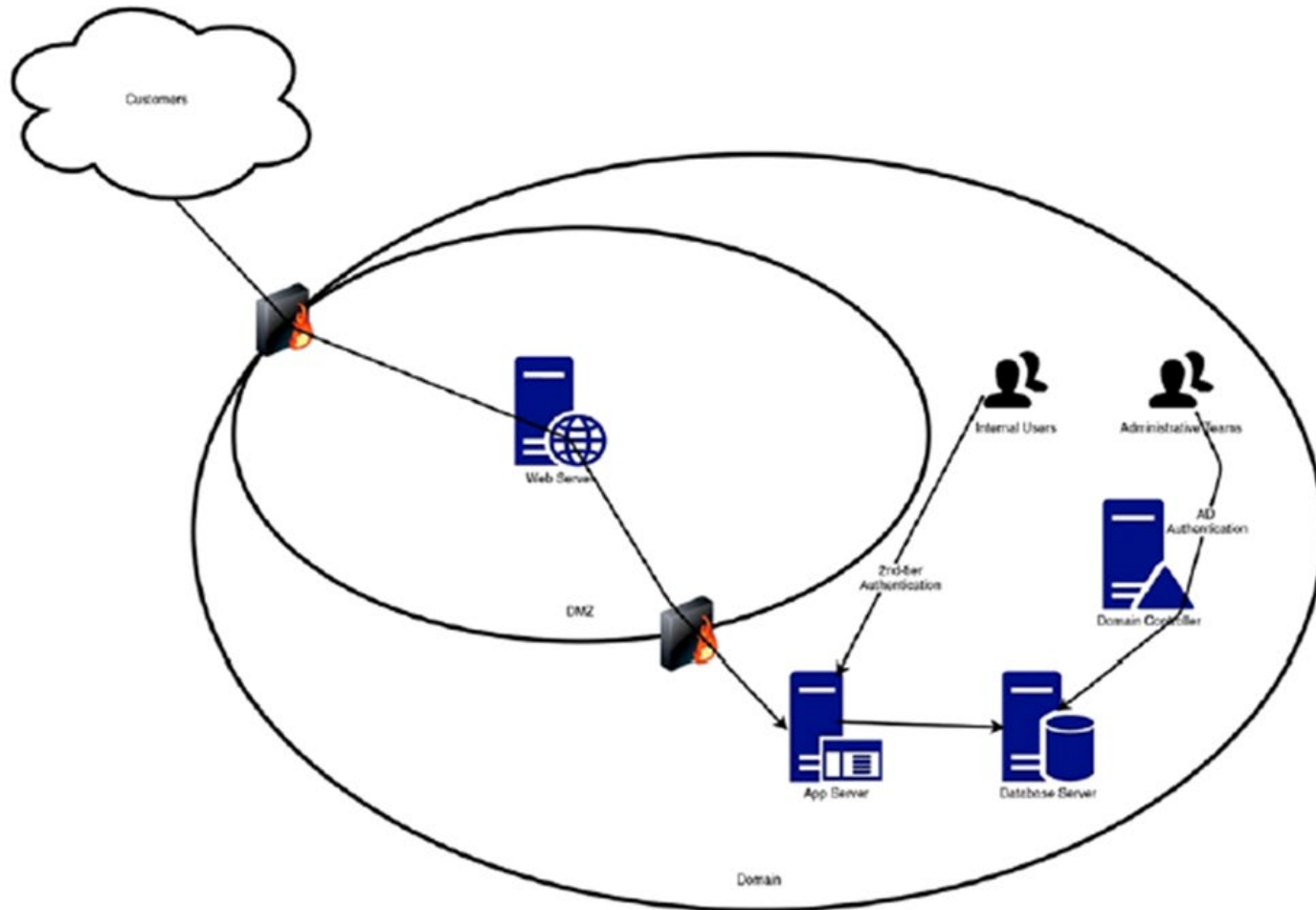
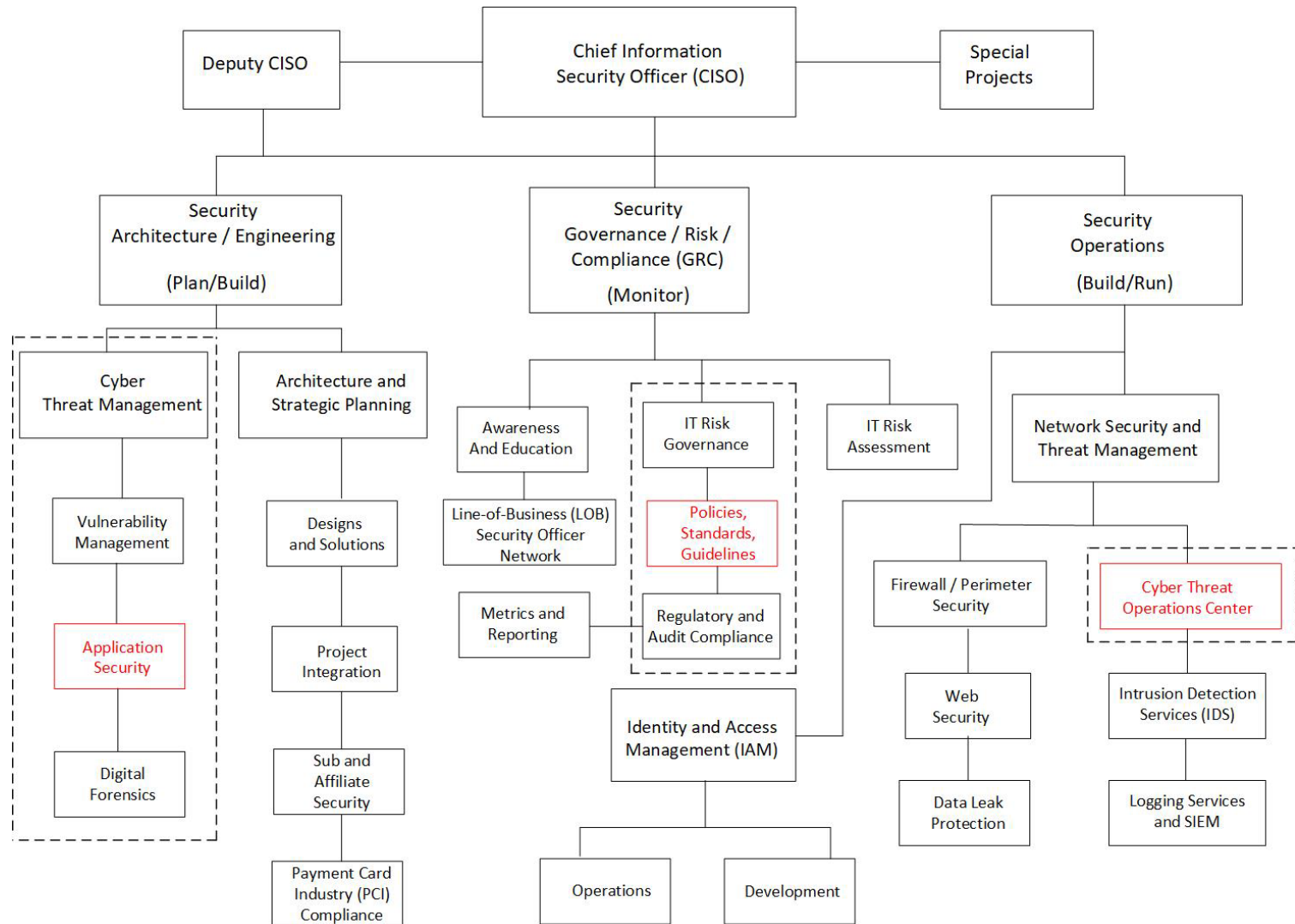


Figure 1-1. Architecture diagram

Databases in Corporate America over the years...

- 1980s: IT activities highly centralized via IT dept. though business units begin to gain some decentralization via desktop PCs and LANs, e.g., word processing, spreadsheets, databases, e.g., Dbase, Rbase, FoxPro.
- 1990s: Hybrid IT with a semi-centralized IT dept. and business units gaining more decentralized control of their IT activities.
- Mid-to-late-90s: introduction of WWW and Corporate Internet access greatly increases corporate concern over controls of corporate data and access to the Corporate network causing return of highly-centralized IT activities.
- 2000s: highly centralized IT activities are firmly re-established.
- 2010s-to-today: centralized control of IT systems and data increases.
- Net result today for controls over applications, databases, and data: highly-centralized under IT dept. controls. Local business unit's acquisition, development, and maintenance of databases, e.g., MySQL, MS Access, and the data they contain seldom allowed, because IT dept. does it all.

IT Security Functional Org Chart...



Name the Three Most Popular Database Products...

Popular Database Management Systems

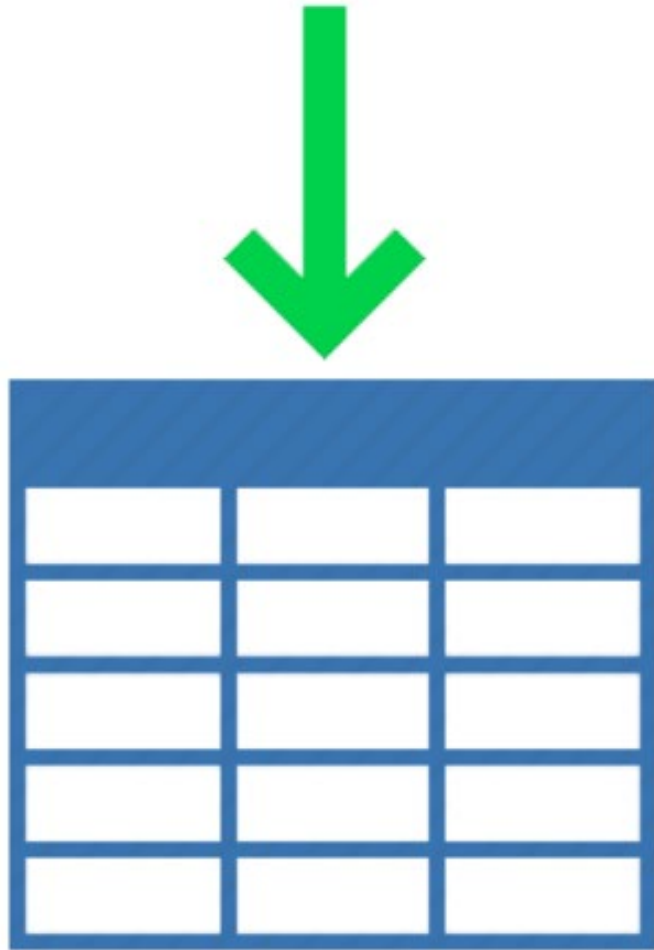


www.gcreddy.com

Database Words...

- Online Transaction Processing (OLTP) applications
- Data Warehouse applications
- Principals, Securables, Permissions
- Database
- Database Instance
- Database Administrator (DBA)
- Data Center
- Structured Query Language (SQL)
- Tables
- Schema
- Authentication
- Authorizations
- Directory Service, e.g., MS Active Directory
- Role-based Access Control (RBAC)
- Java Database Connection (JDBC)
- Single Sign-on (SSO)
- Service Accounts
- Encryption of Data at-rest

Databases are all about Tables...



Each tables contains a category of data...

Here is an example to show you some of the tables that might be stored in a school information database:

Table	Type of data stored
Student information table	name, address, contact details
Student attendance table	Days attended, days absent, reasons for absence
Student exams table	Scores for end of year exams
Staff table	name, address, contact details, qualifications, pay scale

DEFINITION: A table stores all of the records for a particular category

Table Columns = fields and Rows = records...

Databases store data or information in tables, just like the one below:

First Name	Last Name	Address	City	Age
Mickey	Mouse	123 Fantasy Way	Anaheim	73
Bat	Man	321 Cavern Ave	Gotham	54
Wonder	Woman	987 Truth Way	Paradise	39
Donald	Duck	555 Quack Street	Mallard	65
Bugs	Bunny	567 Carrot Street	Rascal	58
Wiley	Coyote	999 Acme Way	Canyon	61
Cat	Woman	234 Purrfect Street	Hairball	32
Tweety	Bird	543	Itottlaw	28

The Schema defines relationships between tables...

Applying our knowledge of primary keys and foreign keys, we can establish the relationships between these five tables and draw a database schema as shown in [Figure 1-6](#). A *database schema* is a diagram showing tables, their columns, and their relationships. All the primary keys and foreign keys are connected by arrows. The non-tipped side of the arrow ties to a primary key, while the tipped side points to a foreign key. These arrows visualize how each parent table supplies data to a child table.

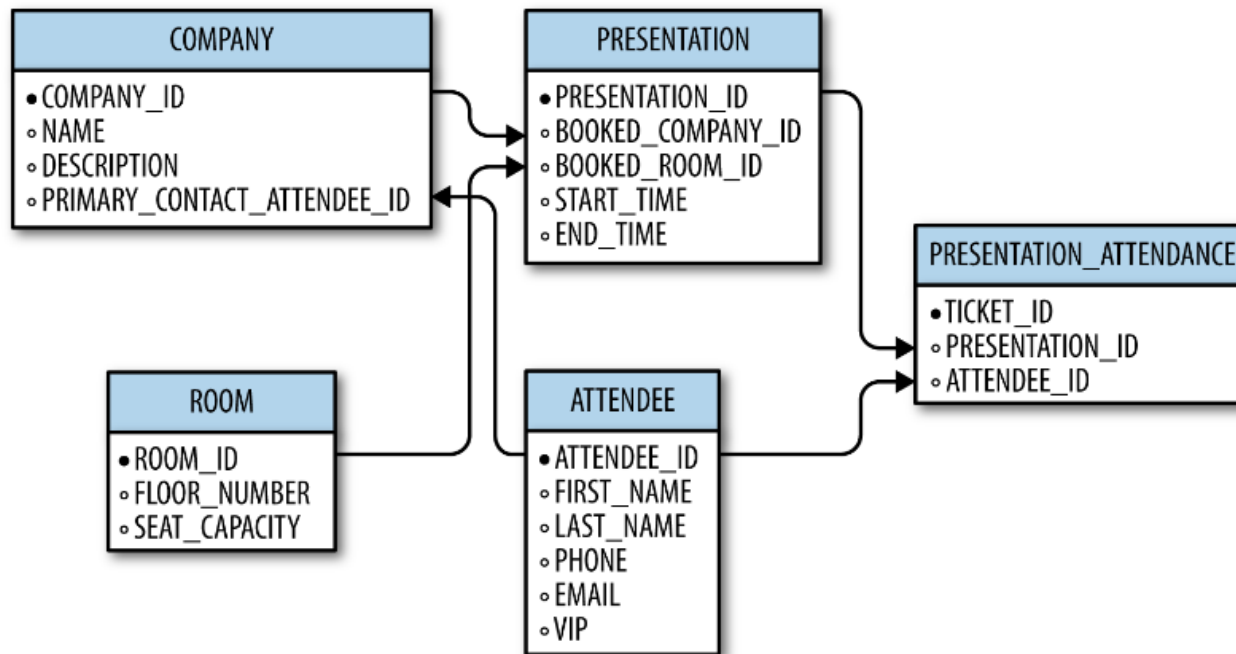


Figure 1-6. The database schema for the SurgeTech conference, with all tables and relationships

Database Security Requirements under PCI Standard...

Testing Requirement 8 (Contd.)



Requirement 8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:

- All user access to, user queries of, and user actions on databases are through programmatic methods
- Only database administrators have the ability to directly access or query databases
- Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes)

Testing Procedures

8.7.a Review database and application configuration settings and verify that all users are authenticated prior to access .

8.7.b Examine database and application configuration settings to verify that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are **through programmatic methods only** (for example, through stored procedures) .

8.7.c Examine database access control settings and database application configuration settings to verify that user **direct access to or queries of databases are restricted to database administrators** .

8.7.d Examine database access control settings, database application configuration settings, and the related application IDs to verify that **application IDs can only be used by the applications** (and not by individual users or other processes) .

User Access to Database via Applications Only...

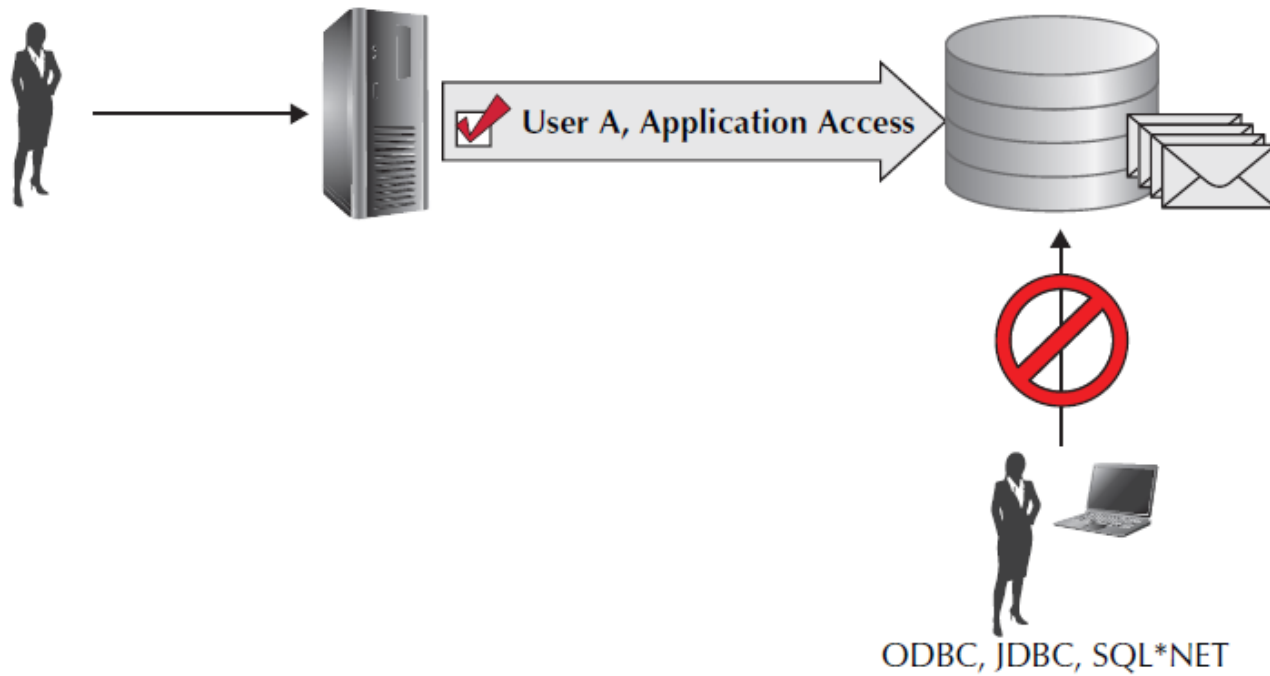
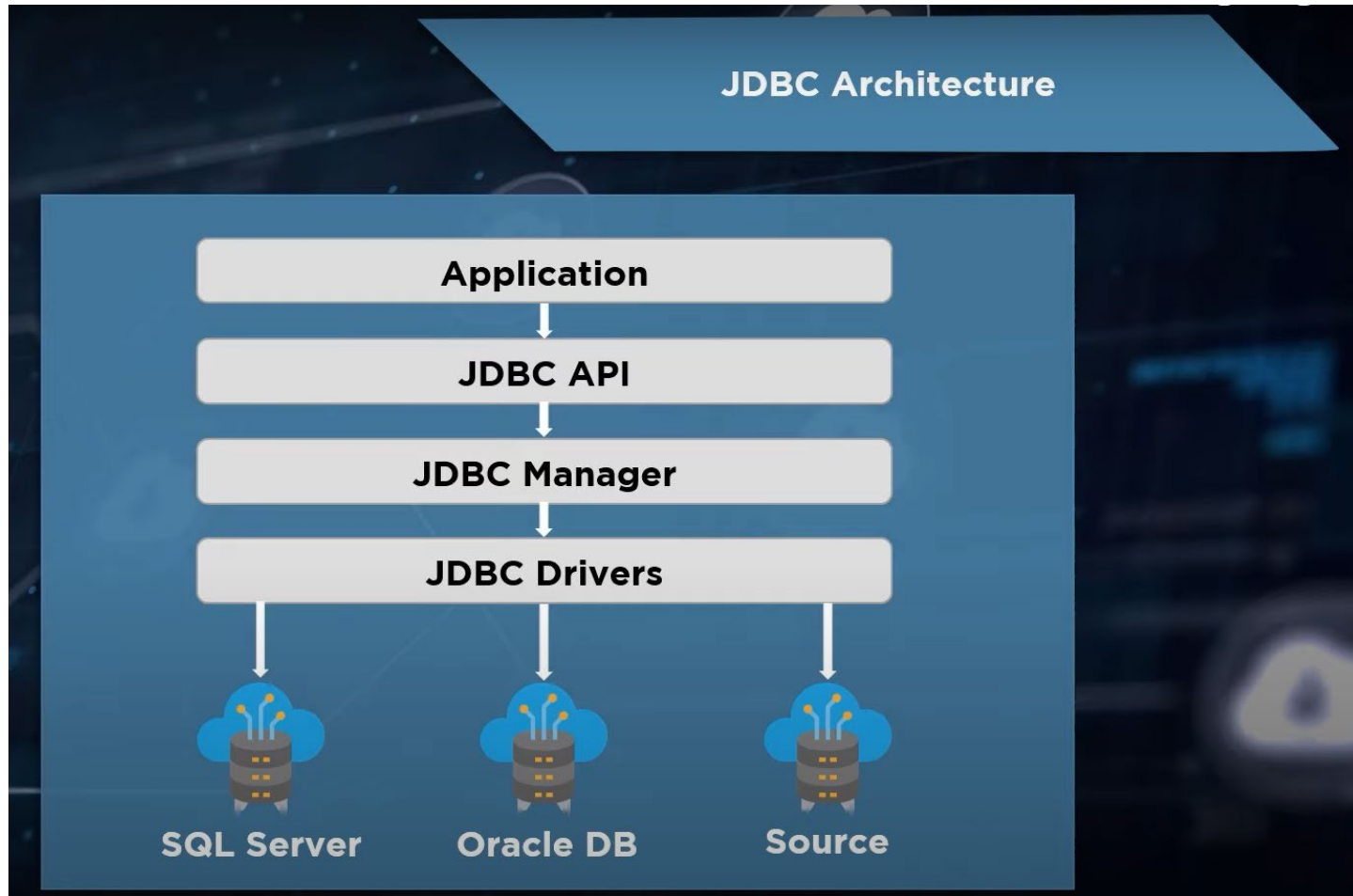


FIGURE 4-3. *Access application tables only via the application*

Java Database Connection (JDBC)

JDBC is a database access solution that enables you to connect a Java application to a database and run SQL statements and queries to the database.



JDBC defined...

- The Java Database Connectivity (JDBC) standard is used by Java applications to access and manipulate data in relational databases.
- JDBC is an industry-standard application programming interface (API) that lets application developers access a relation database management system (RDBMS) using Structured Query Language (SQL) from Java applications.
- Each database vendor implements the JDBC specification with its own extensions hence you must deploy a JDBC driver specific to the database product you are connecting to.

How do Enterprise Users Connect to and Access a Database?

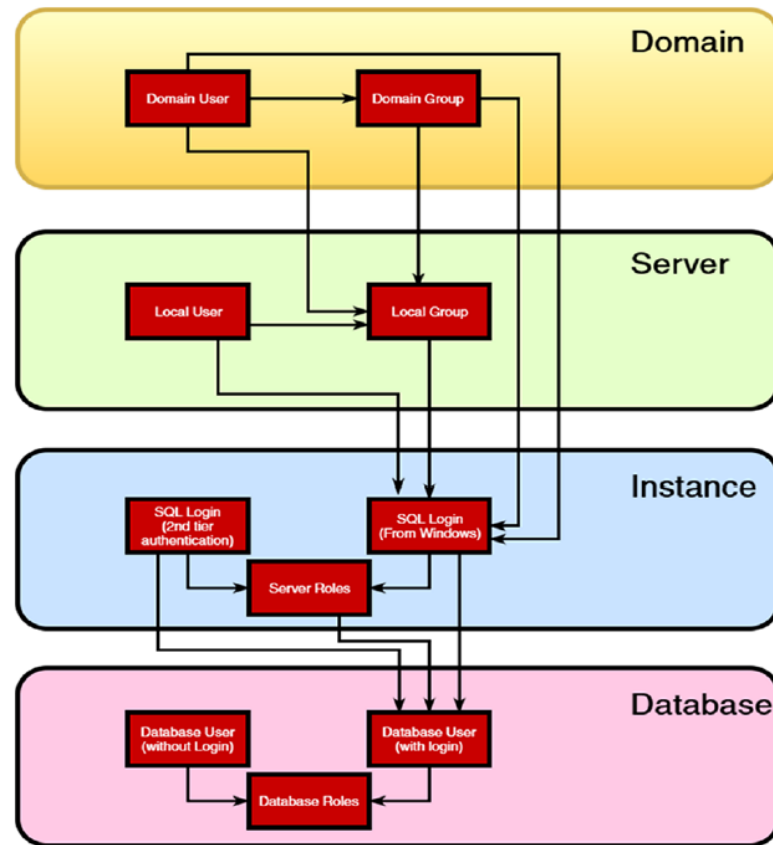


Figure 2-1. Security hierarchy

The diagram shows that a Login, created within the SQL Server instance, can be mapped to a local Windows user or group or to a domain user or group. Usually, in an Enterprise environment, this is a domain user or group. (A group is a collection of users that are granted permissions as a unit.) This eases the administration of security.

The Technology Stack in words...

Identifying the Technology Stack

We can now list out what technology is (or will be) used, for each area of the topology. Table 1-1 demonstrates how this would look for the CarterSecureSafe application.

Table 1-1. Technology Implementations

Technology	Topology Component	Details
Active Directory (AD)	Authentication	Used to authenticate internal users and administrative teams
Domain Controller (DC)	Authentication	Server used by AD authenticate users
Demilitarized Zone (DMZ)	Networking	Subnet that exposes external-facing services
Domain	Networking	A logical container of users, groups, workstations, servers, and other objects, whose authentication is controlled by a Domain Controller
IIS	Web Server	Used to authenticate external users and pass traffic to the application server
.NET	Core Application & Authentication	The core web application has been built using the .NET framework. It also provides forms authentication for internal users.
SQL Server 2016	Database Tier	The databases that drive the application are stored and managed on a SQL Server 2016 instance.
IPsec	Cryptography	Data is encrypted in transit, between the application and database server, using IPsec.
HTTPS	Protocol	External users access the web application via HTTPS.

Active Directory Groups...

The screenshot displays the Windows Computer Management console. The left-hand tree view shows the hierarchy: Computer Management (Local) > System Tools > Local Users and Groups > Users > Groups. The 'Groups' folder is selected, and the 'Users' group is highlighted. The main pane shows a list of system groups with their names and descriptions. The 'Users' group is selected, and its properties dialog box is open in the foreground.

Name	Description
Access Control Assistance Operators	Members of this group can remotely query authorization attributes and permissions for resources on this computer.
Administrators	Administrators have complete and unrestricted access to the computer/domain
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Cryptographic Operators	Members are authorized to perform cryptographic operations.
Device Owners	Members of this group can change system-wide settings.
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM objects on this machine
Event Log Readers	Members of this group can read event logs from local machine
Guests	Guests have the same access as members of the Users group by default, except for the
Hyper-V Administrators	Members of this group have complete and unrestricted access to all features of Hyper-V
IIS_IUSRS	Built-in group used by Internet Information Services.
Network Configuration Operators	Members in this group can have some administrative privileges to manage configuration
Performance Log Users	Members of this group may schedule logging of performance counters, enable trace pr
Performance Monitor Users	Members of this group can access performance counter data locally and remotely
Power Users	Power Users are included for backwards compatibility and possess limited administrativ
Remote Desktop Users	Members in this group are granted the right to logon remotely
Remote Management Users	Members of this group can access WMI resources over management protocols (such as
Replicator	Supports file replication in a domain
System Managed Accounts Group	Members of this group are managed by the system.
Users	Users are prevented from making accidental or intentional system-wide changes and ca

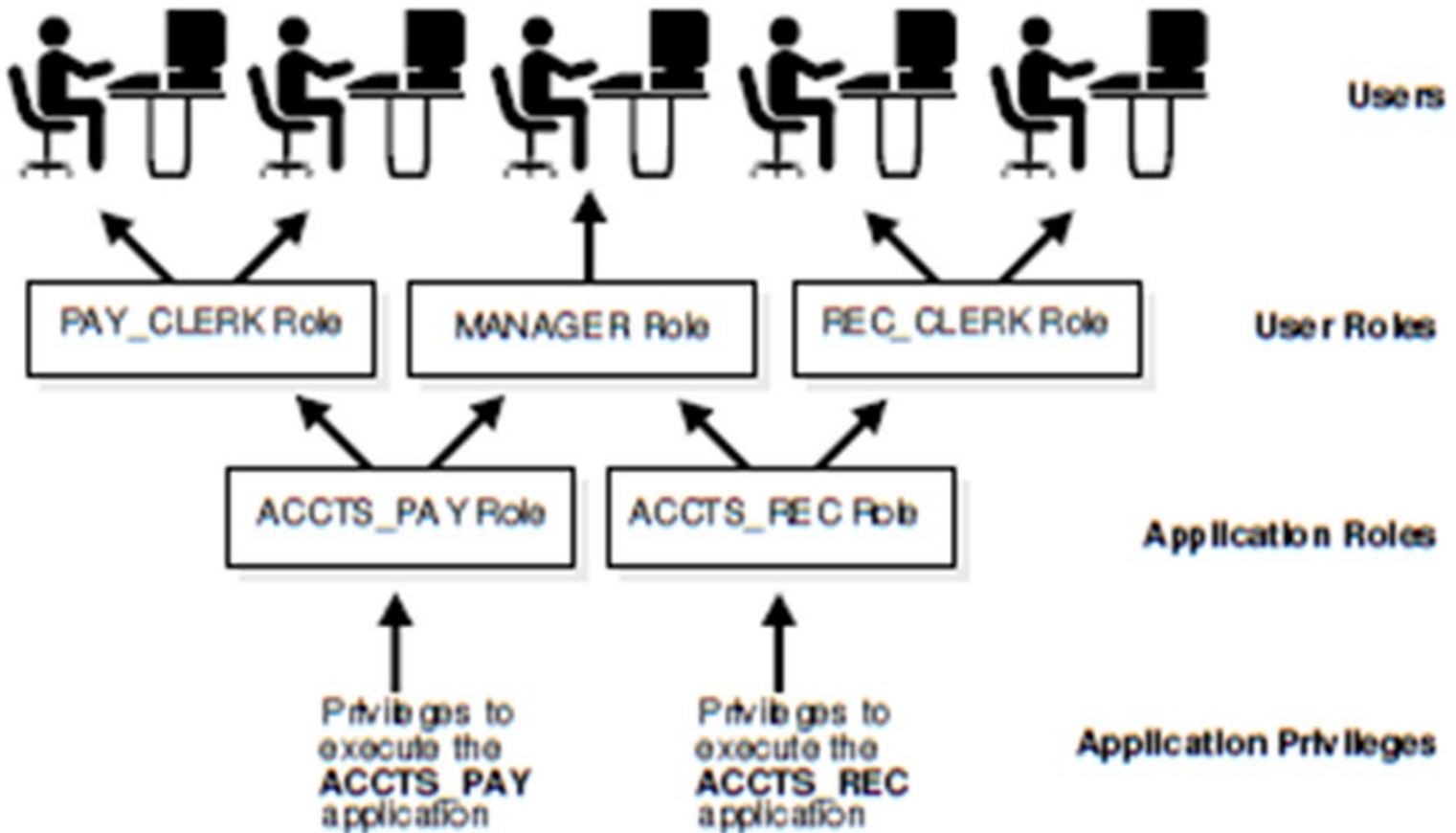
Users Properties dialog box (General tab):

- Name:** Users
- Description:** Users are prevented from making accidental or intentional system-wide changes and can run most
- Members:**
 - monga
 - NT AUTHORITY\Authenticated Users (S-1-5-11)
 - NT AUTHORITY\INTERACTIVE (S-1-5-4)

Buttons: Add..., Remove, OK, Cancel, Apply, Help

Footnote: Changes to a user's group membership are not effective until the next time the user logs on.

Application Access is based on People's Jobs, i.e., Role...



The Wrong and Right way to grant access to Databases...

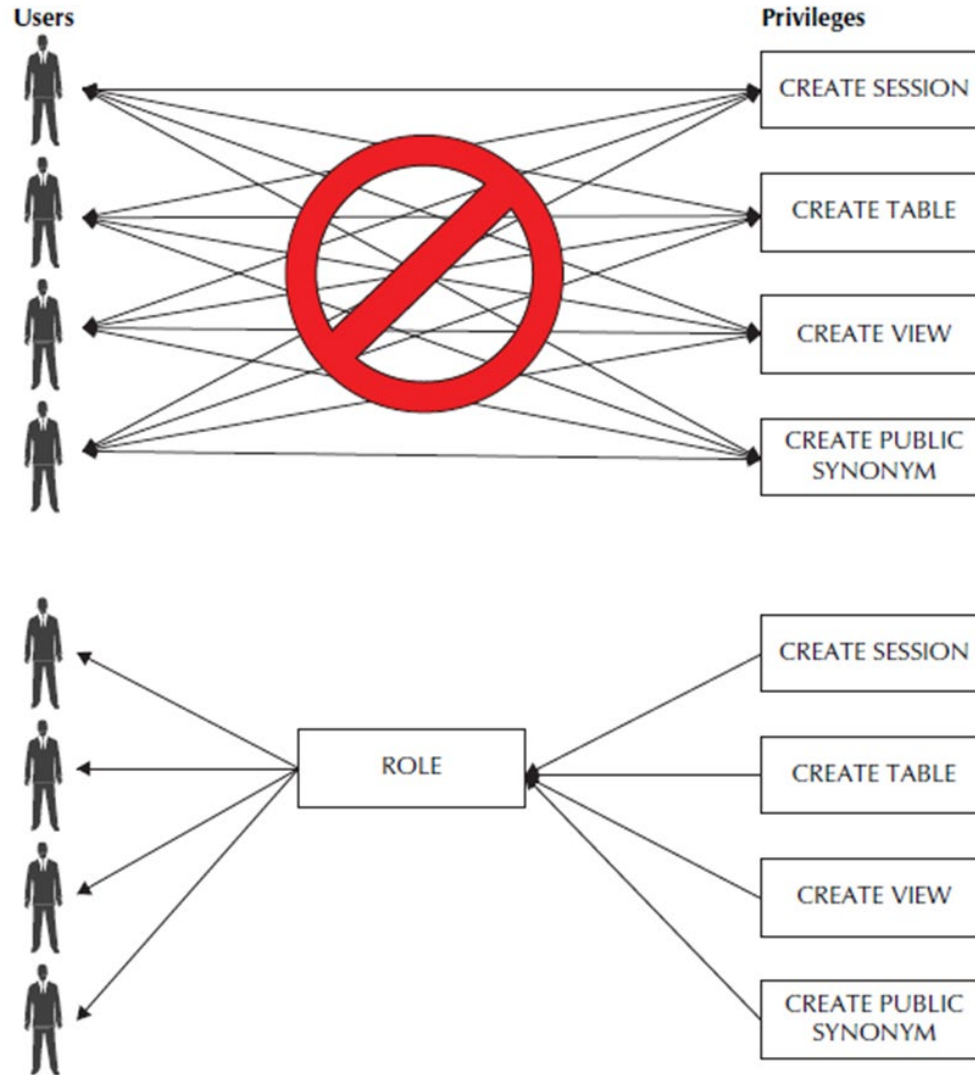
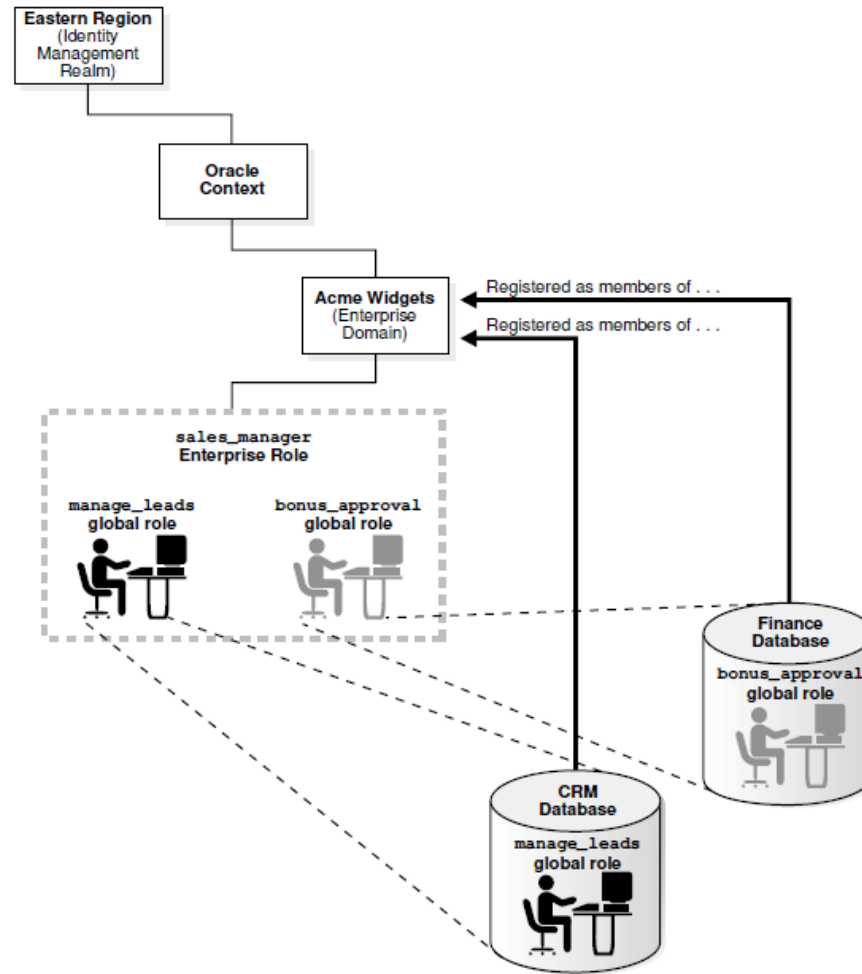


FIGURE 4-2. Database roles simplify privilege management

Role-based Access Control (RBAC)...

Figure 1-2 Example of Enterprise Roles



Single Sign-on (SSO) applied to Database Access...

- Databases are commercial off-the-shelf software (COTS) products that by default are separate and independent of Corporate Directory Services, Applications, and other Access Control mechanisms.
- Hence the default state of a database is that no user access is available until app/database developers design and deploy a user access solution.
- Because all user access to databases must occur via applications that users access after accessing the Corporate Directory Service, e.g., MS Active Directory (AD), the most efficient solution is to leverage AD authentication and authorization controls for database access.
- AD is a directory service that stores user, group, and other information (objects). In addition to storing and managing objects, AD also provides authentication, authorization, group policy administration, and more.
- AD identities and groups can act as pass-thru solutions to the application and its connected databases for user identities and roles; hence, greatly minimizing the volume of identity and access management (IAM) tasks required for users to access applications/databases.

Database Connectors and Service Accounts...

- A Service Account is a 'user' loginID and password that is entered once by an administrator in one software system's configuration that allows it to access another software system automatically, e.g., an application accessing a database via JDBC.

- The Service Account acts as a catch-all 'proxy' login for all application users accessing the database; hence, application database access is invisible to application users.

- Two security concerns with this...
 - 1) Lose of user's identities

 - 2) Account take-over

A config setup page for JDBC to the database...

Connecting to Third Party Databases

A common third party database is Oracle. Below is an example configuration.

Type of connection: JDBC

Connection name: connectOracle

User: VICKY

Password:

Driver name: oracle.jdbc.OracleDriver

URL: jdbc:oracle:thin:@myhost:1521:orcl

Class path: /Users/mli/tmp/ojdbc7_12g.jar
(May be a comma separated list if multiple jar files are required.)

Properties: includeSynonyms=false;restrictGetTables=true

Do not use delimited identifiers by default:

Use COALESCE:

Use NVL() instead of IFNULL():

Conversion in composite Row IDs: Do not convert non-character values
 Use CAST as VARCHAR
 Use CAST as CHAR
 Use {fn convert ...}

Test Connection Save Close

Connection successful.

As you can see, the driver name and URL have different patterns than what we used for the previous connection. In addition, I specified a class path in this example, because I need to use Oracle's driver to connect to their database.

As you can imagine, SQL Server uses different URL and driver name patterns.

Knowledge-check...

- See Word doc...

User Audit Trail Requirements under PCI Standard...



Testing Requirement 10

Requirement 10.1 Implement audit trails to link all access to system components to each individual user.

Requirement 10.2 Implement automated audit trails for all system components to reconstruct the following events:

- All individual accesses to cardholder data
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects

Testing Procedures

10.1 Verify, through observation and interviewing the system administrator, that:

- Audit trails are enabled and active for system components.
- Access to system components is **linked to individual users**.

More Specifically...



Testing Requirement 10 (Contd.)

Requirement 10.3 Record at least the following audit trail entries for all system components for each event:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource.

Testing Procedures
10.3 Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following:
10.3.1 Verify user identification is included in log entries.
10.3.2 Verify type of event is included in log entries.
10.3.3 Verify date and time stamp is included in log entries.
10.3.4 Verify success or failure indication is included in log entries.
10.3.5 Verify origination of event is included in log entries.
10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.

Audit Report: with no user identity...

Spid	Transaction ID	Login_or_User	Transaction Type	Begin Time
59	0000:000004cd	login: ASPNET	INSERT	2012/01/15 20:30:09:730
59	0000:000004cc	login: ASPNET	CREATE TABLE	2012/01/15 20:30:09:713
59	0000:000004c7	login: ASPNET	INSERT	2012/01/15 20:30:00:370
59	0000:000004c6	login: ASPNET	CREATE TABLE	2012/01/15 20:30:00:323
62	0000:000004c4	login: ASPNET	CREATE TABLE	2012/01/15 20:29:53:920
67	0000:000004c3	login: ASPNET	CREATE TABLE	2012/01/15 20:28:12:223
57	0000:000004b9	login: ASPNET	INSERT EXEC	2012/01/15 20:28:07:090
57	0000:000004b8	login: ASPNET	CREATE TABLE	2012/01/15 20:28:07:057
68	0000:000004b1	login: ASPNET	INSERT EXEC	2012/01/15 20:28:02:593
68	0000:000004b0	login: ASPNET	CREATE TABLE	2012/01/15 20:28:02:547
74	0000:000004aa	login: ASPNET	INSERT EXEC	2012/01/15 20:28:00:337
74	0000:000004a9	login: ASPNET	CREATE TABLE	2012/01/15 20:28:00:320
56	0000:000004a2	login: ASPNET	CREATE TABLE	2012/01/15 20:27:58:040
56	0000:000004a3	login: ASPNET	INSERT EXEC	2012/01/15 20:27:58:040
60	0000:0000049b	login: ASPNET	INSERT EXEC	2012/01/15 20:27:54:050



Audit Report: with user identity...

Database Activity Log

Sample Company

Database Activity Log

Date Range: 8/29/2018 to 8/29/2018

Filter: (Application User Active Status Is true)

Application User	Machine Name	Date/Time	Activity	Entity Name	Record ID	Description
JustaFay		8/29/2018 10:54:52 AM	Create	AppUserLogin	1	IsLoggedIn=False
JustaFay		8/29/2018 10:54:55 AM	Create	AppUserPreference	1	TaskMore
JustaFay		8/29/2018 10:54:55 AM	Create	AppUserPreference	2	TaskNormal
JustaFay		8/29/2018 10:54:55 AM	Create	AppUserPreference	3	TaskLess
JustaFay		8/29/2018 10:58:39 AM	Create	AppUserLogin	2	IsLoggedIn=False
JustaFay		8/29/2018 11:05:27 AM	Edit	AppUserLogin	1	IsLoggedIn=False
JustaFay		8/29/2018 11:10:48 AM	Create	AppUserLogin	3	IsLoggedIn=False
JustaFay		8/29/2018 11:11:11 AM	Create	ReportTemplate	1	Monthly Assignment Calendar by Shift,
JustaFay		8/29/2018 11:11:42 AM	Create	AppUserPreference	4	DailyMore
JustaFay		8/29/2018 11:11:42 AM	Create	AppUserPreference	5	DailyNormal
JustaFay		8/29/2018 11:11:42 AM	Create	AppUserPreference	6	DailyLess
JustaFay		8/29/2018 11:11:52 AM	Edit	ShiftAssignment	2467	Day Shift, , 8/1/2018
JustaFay		8/29/2018 11:11:58 AM	Edit	ShiftAssignment	2486	Day Shift, , 8/1/2018
JustaFay		8/29/2018 11:12:03 AM	Edit	ShiftAssignment	2488	Day Shift, , 8/1/2018
JustaFay		8/29/2018 11:14:07 AM	Edit	AppUserLogin	2	IsLoggedIn=False
JustaFay		8/29/2018 11:14:10 AM	Edit	Shift	1	Day Shift
JustaFay		8/29/2018 11:18:20 AM	Edit	Definition	62	Schedule Email
JustaFay		8/29/2018 11:18:42 AM	Edit	Definition	62	Schedule Email
JustaFay		8/29/2018 11:19:24 AM	Edit	Definition	62	Schedule Email
JustaFay		8/29/2018 11:28:09 AM	Edit	Definition	62	Schedule Email
JustaFay		8/29/2018 11:28:47 AM	Create	AppUserPreference	7	DShiftMore
JustaFay		8/29/2018 11:28:47 AM	Create	AppUserPreference	8	DShiftNormal

Capturing AD identities in Oracle database audit trails...

We can access an end-user's Active Directory (AD) Distinguished Name (DN) via SQL.

You can add the association of the end user's identity with any auditable database action in the Oracle audit trail by simply calling the PL/SQL procedure `DBMS_SESSION.SET_IDENTIFIER` as shown in the following example:

```
DBMS_SESSION.SET_IDENTIFIER(SYS_CONTEXT('userenv', 'external_name'));
```

This call to `DBMS_SESSION` can be included in an Oracle database logon trigger. Once this is done the `CLIENT_ID` column of the `DBA_AUDIT_TRAIL` view will be populated with the DN of the enterprise user.

AD Distinguished Name defined...

The table below explains the different components of an Active Directory DN.

String	Attribute type
DC	domainComponent
CN	commonName
OU	organizationalUnitName
O	organizationName
STREET	streetAddress
L	localityName
ST	stateOrProvinceName
C	countryName
UID	userid

What the AD DN can tell you...

```
CN=Victor Ashiedu,OU=Writers,DC=itechguides,DC=local
```

So, when you look at the DN of an AD object, you can tell the full path to the object in the directory. For example, I can tell that the name of the object in the above DN is “Victor Ashiedu.”

In addition to that, I can tell that the object belongs to an OU (Organizational Unit) called “Writers.” Finally, I know that the object is in the domain “itechguides.local.”

Encryption of Data at-Rest: two methods...

- 1) Storage device encryption: automatic encryption of all writes to the device and automatic decryption of all reads from the device. Occurs at hardware-level of storage equipment, invisible to application end-users and user administrators.

 - 2) Encryption of data contained in databases: encrypt selected columns/rows in tables. Automatically decrypts when 'authorized users' access data in tables.
- What good does this do as a security access control over data contained in databases?

Encryption at-rest under PCI Standard v3.2.1...

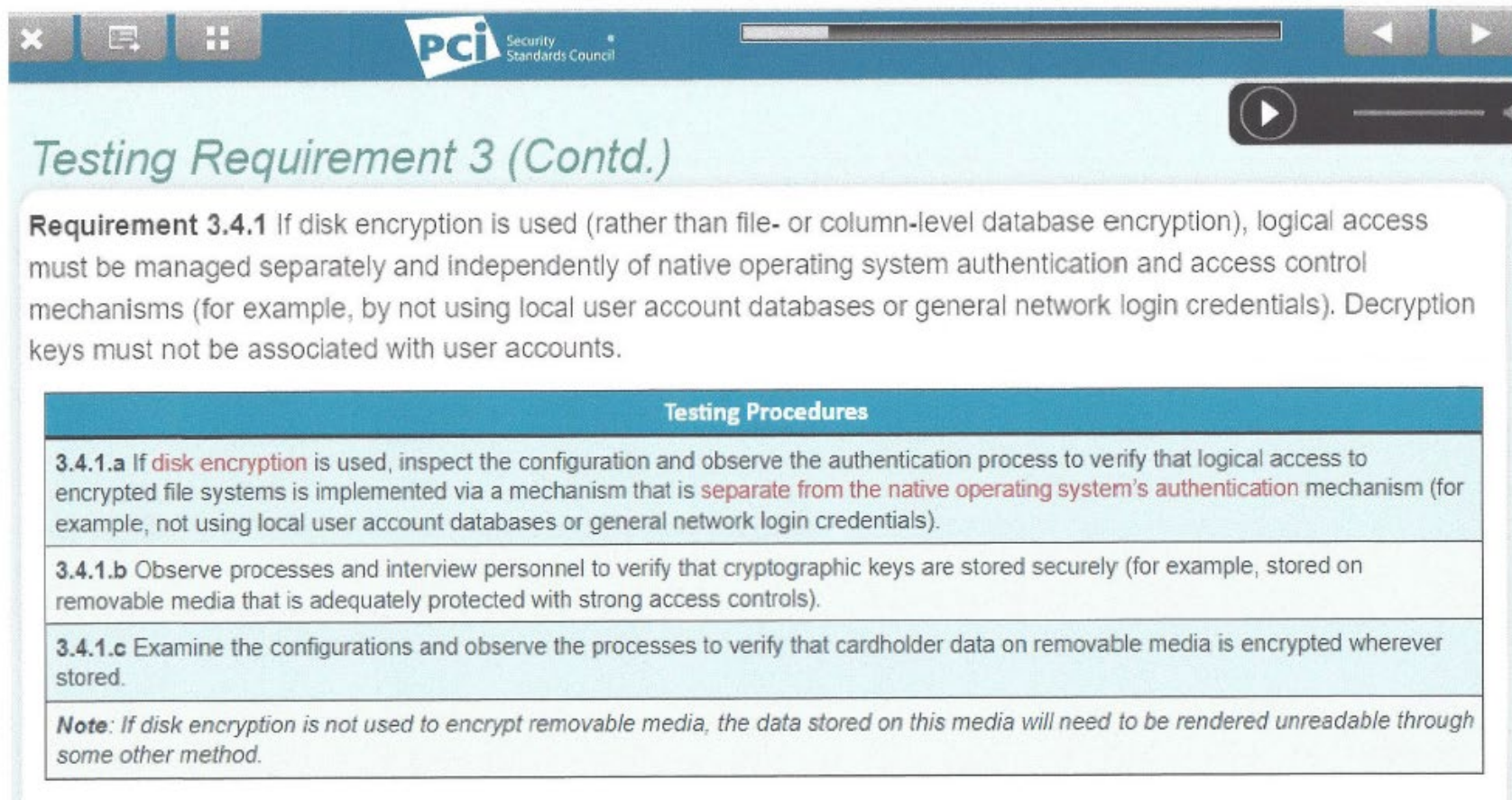
PCI Security Standards Council

Testing Requirement 3 (Contd.)

Requirement 3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: one-way hashes based on strong cryptography, truncation, index tokens and pads, or strong cryptography with associated key-management processes and procedures.

Testing Procedures
<p>3.4.a Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods:</p> <ul style="list-style-type: none">• One-way hashes based on strong cryptography• Truncation• Index tokens and pads, with the pads being securely stored• Strong cryptography, with associated key-management processes and procedures
<p>3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (not stored in plain-text).</p>
<p>3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable .</p>
<p>3.4.d Examine a sample of audit logs including payment application logs, to confirm that PAN is rendered unreadable or is not present.</p>
<p>3.4.e If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN .</p>

More Encryption at-rest under PCI Standard v3.2.1...



PCI Security Standards Council

Testing Requirement 3 (Contd.)

Requirement 3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

Testing Procedures
3.4.1.a If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating system's authentication mechanism (for example, not using local user account databases or general network login credentials).
3.4.1.b Observe processes and interview personnel to verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).
3.4.1.c Examine the configurations and observe the processes to verify that cardholder data on removable media is encrypted wherever stored.
Note: <i>If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.</i>

Encryption at-rest under PCI Standard v4.0...



Requirements and Testing Procedures	Guidance
<p>Applicability Notes</p> <p>While disk encryption may still be present on these types of devices, it cannot be the only mechanism used to protect PAN stored on those systems. Any stored PAN must also be rendered unreadable per Requirement 3.5.1—for example, through truncation or a data-level encryption mechanism. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic media storage devices.</p> <p>Media that is part of a data center architecture (for example, hot-swappable drives, bulk tape-backups) is considered non-removable electronic media to which Requirement 3.5.1 applies.</p> <p>Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.</p> <p><i>This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.</i></p>	

Knowledge-check...

- See Word doc...

Database Security: summary...

- User Access
- Audit Trails
- Encrypting Data At-rest