CS660 – Database systems

Dr. John Conklin

DATABASE ADMINISTRATION

Unit 4: Techniques & Best Practices

UNIT 4 OVERVIEW

1. **Transaction Management**
   ACID properties, concurrency control, and isolation levels
2. **Database Security**
   Authentication, authorization, encryption, and compliance
3. **Backup and Recovery**
   Backup strategies, recovery techniques, and disaster planning
4. **Business Continuity**
   High availability, failover, and continuity planning
5. **Risk Management**
   Identifying, assessing, and mitigating database risks

TRANSACTION MANAGEMENT

What is a Transaction?

A transaction is a logical unit of work that contains one or more SQL statements. All statements in a transaction must succeed or fail together, ensuring data consistency and integrity.

Example: Bank Transfer

```
BEGIN TRANSACTION;
  UPDATE Accounts SET Balance = Balance - 100 WHERE AccountID = 1;
  UPDATE Accounts SET Balance = Balance + 100 WHERE AccountID = 2;
COMMIT;  -- Success: Both updates or neither
-- If error: ROLLBACK;  -- Undo all changes
```

Transaction Lifecycle

ACID PROPERTIES

Foundation of reliable database transactions

A **Atomicity**
All or nothing - transaction fully completes or fully fails

Example: Transfer succeeds completely or not at all

C **Consistency**
Database moves from one valid state to another

Example: Total money in system remains constant

I **Isolation**
Concurrent transactions don't interfere with each other

Example: Two transfers don't corrupt each other's data

D **Durability**
Committed changes are permanent, survive crashes

Example: After COMMIT, data survives power failure

CONCURRENCY CONTROL

Transaction Isolation Levels

READ UNCOMMITTED *Lowest isolation, highest performance*	Dirty: Yes	Non-Rep: Yes	Phantom: Yes
READ COMMITTED *Prevents dirty reads*	Dirty: No	Non-Rep: Yes	Phantom: Yes
REPEATABLE READ *Prevents dirty & non-repeatable reads*	Dirty: No	Non-Rep: No	Phantom: Yes
SERIALIZABLE *Highest isolation, like sequential execution*	Dirty: No	Non-Rep: No	Phantom: No

DATABASE SECURITY

Defense in Depth Strategy

Authentication

Verify user identity

Passwords, MFA, SSO, certificates

Authorization

Control access permissions

Roles, privileges, row-level security

Encryption

Protect data at rest & in transit

TLS/SSL, TDE, column encryption

Auditing

Track database activities

Audit logs, compliance monitoring

SECURITY BEST PRACTICES

✓ Principle of Least Privilege
Grant minimum permissions needed for job function

✓ Regular Security Audits
Review access logs, permissions, and vulnerabilities

✓ Network Segmentation
Isolate database servers from public networks

✓ SQL Injection Prevention
Use parameterized queries, input validation

✓ Strong Password Policies
Enforce complexity, expiration, and MFA where possible

✓ Patch Management
Keep database software updated with security patches

✓ Encryption Everywhere
Encrypt data at rest, in transit, and in backups

✓ Backup Security
Encrypt and secure backup files, test restores

BACKUP AND RECOVERY

Types of Database Backups

Full Backup

Complete copy of entire database

✓ Pros: Simplest recovery, complete data

⚠ Cons: Time-consuming, large storage

Frequency: Weekly or monthly

Differential Backup

Changes since last full backup

✓ Pros: Faster than full, moderate storage

⚠ Cons: Requires full backup for restore

Frequency: Daily

Incremental Backup

Changes since last backup (any type)

✓ Pros: Fastest, smallest size

⚠ Cons: Complex restore (need all incrementals)

Frequency: Hourly or continuous

RECOVERY STRATEGIES

Key Recovery Objectives

RTO	**Recovery Time Objective** Maximum acceptable downtime	**RTO: 4 hours**
RPO	**Recovery Point Objective** Maximum acceptable data loss	**RPO: 15 minutes**

Recovery Process Steps

1. Assess Damage
2. Restore Backup
3. Apply Logs
4. Verify Data
5. Resume Operations

BUSINESS CONTINUITY

1. **Disaster Recovery Planning**
   Define RTOs and RPOs for all critical database systems

2. **Backup & Restore Procedures**
   Schedule full, differential, and transaction log backups

3. **Failover Mechanisms**
   Configure automatic failover to minimize service interruption

4. **Data Replication**
   Maintain synchronized copies across multiple locations

5. **Testing & Validation**
   Regularly test recovery procedures to verify data integrity

HIGH AVAILABILITY

1. **Clustering**
   Multiple nodes share workload and provide redundancy

2. **Load Balancing**
   Distribute read queries across replicas to prevent overload

3. **Automatic Failover**
   Standby nodes take over instantly upon primary failure

4. **Redundant Storage**
   Use RAID and distributed storage to eliminate single points of failure

5. **Uptime SLAs**
   Target 99.9% or higher availability with continuous monitoring

RISK MANAGEMENT

1. **Risk Identification**
   Catalog all potential threats including hardware, software, and human factors

2. **Impact Assessment**
   Evaluate business impact using quantitative and qualitative analysis

3. **Mitigation Strategies**
   Implement encryption, access policies, and audit logging controls

4. **Monitoring & Alerting**
   Deploy real-time tools that detect anomalies and trigger alerts

5. **Compliance Requirements**
   Meet regulatory standards such as GDPR, HIPAA, and SOX

DATABASE RISK CATEGORIES

1. **Security Risks**
   SQL injection, unauthorized access, and insider threats

2. **Operational Risks**
   Hardware failures, software bugs, and capacity shortages

3. **Environmental Risks**
   Natural disasters, power outages, and network failures

4. **Data Integrity Risks**
   Corruption from application bugs or concurrent write conflicts

5. **Compliance Risks**
   Violations of data retention, privacy, or audit requirements

INCIDENT RESPONSE

1. **Detection & Identification**
   Use monitoring and log analysis to detect and classify incidents
2. **Containment**
   Isolate affected systems while preserving forensic evidence
3. **Eradication & Recovery**
   Remove root cause, restore from backups, and validate integrity
4. **Communication Protocols**
   Notify stakeholders and regulators per the response plan
5. **Post-Incident Review**
   Document lessons learned and update procedures accordingly

KEY TAKEAWAYS

INDIVIDUAL PROJECT

Individual Project

The case study retail store is concerned about the possibilities of losing data because of database system malfunctions or downtime. Security is also a major concern to the company because it is common knowledge that engaging in online business can be risky because of known vulnerabilities on the Internet. The company also realizes that its in-store database system is the top priority at this time. What solutions can you propose to effectively manage database transactions, maintain security, and recover the data that are lost from system failure or downtime?

The assumptions are as follows:

- A high volume of the orders often occurs during the daytime.
- One person will serve the role of database administrator.
- The database administrator account will serve as database owner.
- The transaction log must be backed up.
- Point-in-time recovery is required.
- There is an always-on availability group.
- The ability to purchase products online will be addressed in a future database project.

The project deliverables are as follows:

- What solutions can you propose to effectively manage database transactions, maintain security, and recover the data that are lost from system failure or downtime?
- What is your rationale for the transaction management plan, database security procedure, backup plan, and recovery model that you proposed for the case study organization?
- Database Administration Plan (4–5 pages)
  - Create a database administration plan that is specific to the needs of your retail store.
  - Include a transaction management plan that includes a flowchart for how each transaction will be handled (including rollback and commit cases).
  - Include a database security procedure that includes provisions for access control, user authentication, and availability.
  - Include a backup plan and a recovery model
  - Provide your analysis as to how this part of the project fulfills the mission and 1 or more goals of the case study organization.
- All sources should be cited both in-text and in References using APA format.
- Name the document "yourname_CS660_IP4.doc."

Contact Information

Email:	Jconklin@coloradotech.edu
Phone:	602.796.5972
Website:	http://drjconklin.com
Office Hours:	Wednesdays: 6:00 PM – 7:00 PM (CST)
	Saturdays: 11:00 AM – 12:00 PM (CST)
Live Chats:	Wednesdays: 6:00 PM – 7:00 PM (CST)