SIT103/SIT772 Database Fundamentals

Week 10

Database Security &
Unit Review

Dr Iynkaran Natgunanathan

Last week

- Operational and Decision Support Data
- Business Intelligence
- Data Warehouse and Data Marts
- Data Analytics and Data Mining
- Data Visualisation
- Big Data
- NoSQL Databases

Last Week's OnTrack Task

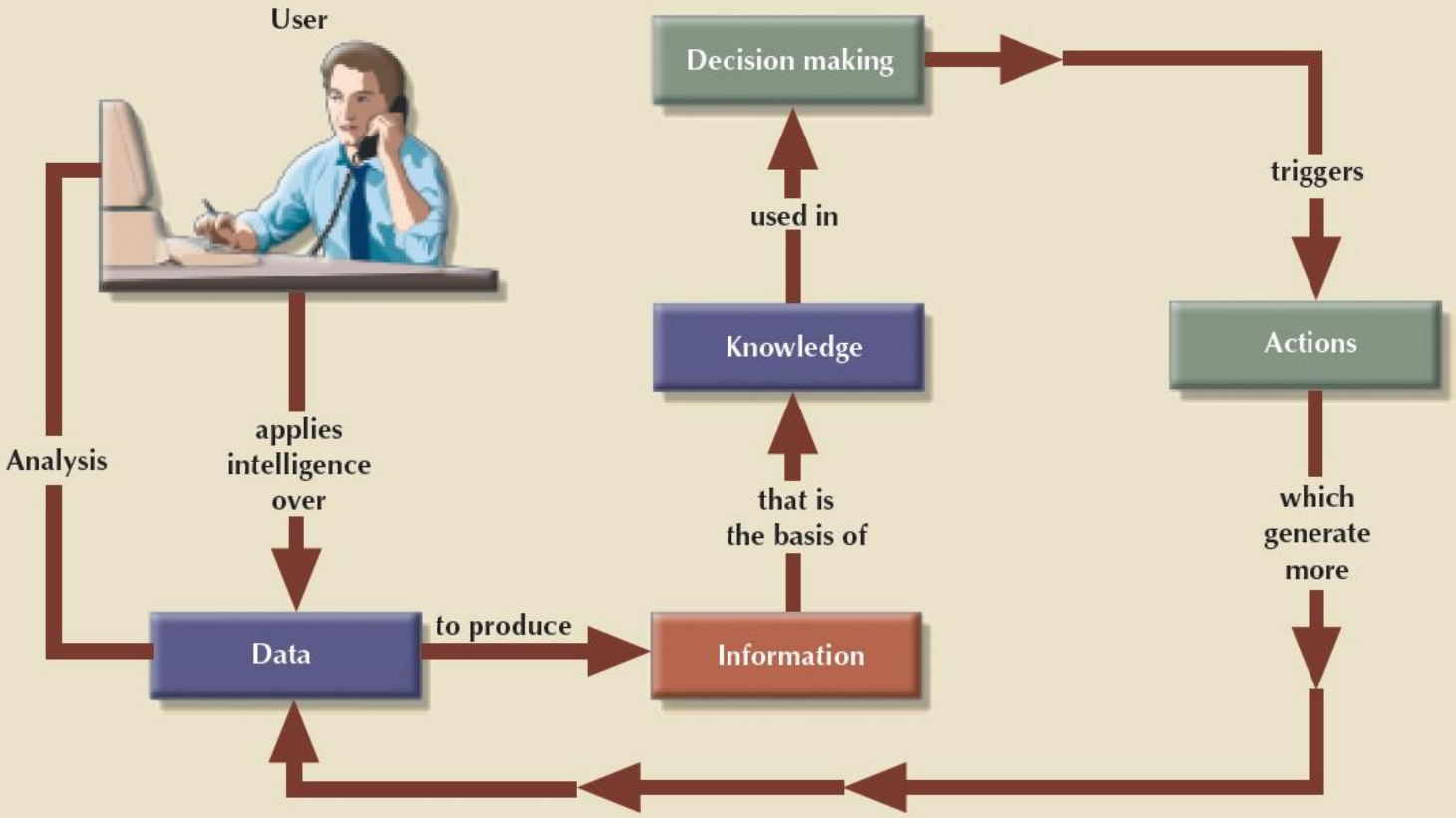
- 9.1P Data Analysis and Visualization using Excel
- 9.2D Interaction with a database via an user interface

This week

- Data and Database Security
  - Confidentiality
  - Integrity
  - Availability
- Professional Practice and Ethics
- Unit Review
- What next?

Data: A critical Corporate Asset

FIGURE 16.1 THE DATA-INFORMATION-DECISION-MAKING CYCLE



Data as a Corporate Asset (2)

- In today's information-driven environment, data is a valuable asset that requires careful management.
- How many opportunities are lost if the data is lost? What is the actual cost of data loss?
- Data loss puts any company in a difficult position. The company might be unable to handle daily operations effectively.
- Accurate and timely data can enhance the company's competitive position and generate revenue

  - data inaccuracies and inconsistencies becomes a great threat

Data Quality

- A comprehensive approach to ensuring the accuracy, validity, and timeliness of data
- More than just cleaning data; it also focuses on preventing future inaccuracies and building user confidence in the data

  - also, includes availability, integrity, security, and privacy

- Large-scale data quality initiatives tend to be complex and expensive projects, so the alignment of these initiatives with business goals is a must, as is buy-in from top management
- Requires good data governance – administration and management of data

  - policies, practices, procedures, standards, tools and technologies

Data Security

- Protecting data against accidental and intentional threats
- Involves securing all the processes and systems around data, including hardware systems, software applications, the network and its devices, internal and external users, procedures, and the data itself
- Requires a comprehensive, company-wide approach
- Security goals – CIA principles
  1. Confidentiality
  2. Integrity
  3. Availability

Confidentiality

- Ensure that data is used by authorised users for authorised purpose only
- Safeguard against privacy breaches that could lead to legal actions
  - National, State and Industry-specific laws and regulations, e.g., Privacy Act 1988 (Federal), Privacy and Data Protection Act 2014 (VIC), My Health Records Act 2012, Telecommunication Act 1997, Banking Act 1959, etc.
- **Compliance and Audit**: ensures that data privacy and security requirements and reporting guidelines in terms of data capture, storage and access are met

Integrity

- Ensure that data is accurate, valid and consistent
- Database design plays crucial role here
- Organisational processes and usage patterns must maintain integrity
- Maintaining data integrity is a process that starts with data collection and continues with data storage, processing, usage, and archiving
- The rationale behind integrity is to treat data as the most-valuable asset in the organization and to ensure that rigorous data validation is carried out at all levels within the organization

Availability

- Accessibility of data whenever required by authorized users and for authorized purposes
- To ensure data availability, the entire system must be protected from service degradation or interruption caused by any internal or external source
- Service interruptions could be very costly for companies and users
- System availability is an important goal of security.

Security Policies

DEAKIN UNIVERSITY

- A security policy is a collection of standards, policies, and procedures created to guarantee the security of a system and ensure auditing and compliance
- Database security officer and the database administrator(s), who work together to establish a cohesive data security strategy
- Such a strategy begins with defining a sound and comprehensive security policy
- The security audit process starts by identifying security vulnerabilities and identifying measures to protect the system and data against those vulnerabilities.

Security Vulnerabilities

- A security vulnerability is a weakness in a system component that could be exploited to allow unauthorized access or cause service disruptions
- Such vulnerabilities could fall under one of the following categories:
  1. **Technical**: e.g., a flaw in the operating system or web browser
  2. **Managerial**: e.g., users might not be educated about critical security issues
  3. **Cultural**: e.g., users might hide passwords under their keyboards or forget to shred confidential reports
  4. **Procedural**: e.g., company procedures might not require complex passwords or the checking of user IDs.
- When a security vulnerability is left unchecked, it could become a Security Threat

Security Threats

A security threat is any situation or event, whether intentional or accidental, that may adversely affect a system and consequently the organization

- cause harm to the organisation (e.g., financial, brand damage) and/or customer (e.g., loss of privacy)

THREAT	THEFT AND FRAUD	LOSS OF CONFIDENTIALITY	LOSS OF PRIVACY	LOSS OF INTEGRITY	LOSS OF AVAILABILITY
Using another person's means of access	✓	✓	✓		
Unauthorized amendment or copying of data	✓			✓	
Program alteration	✓			✓	✓
Inadequate policies and procedures that allow a mix of confidential and normal output	✓	✓	✓		
Wire tapping	✓	✓	✓		
Illegal entry by hacker	✓	✓	✓		
Blackmail	✓	✓	✓		
Creating "trapdoor" into system	✓	✓	✓		
Theft of data, programs, and equipment	✓	✓	✓		✓
Failure of security mechanisms, giving greater access than normal		✓	✓	✓	
Staff shortages or strikes				✓	✓
Inadequate staff training		✓	✓	✓	✓
Viewing and disclosing unauthorized data	✓	✓	✓		
Electronic interference and radiation				✓	✓
Data corruption owing to power loss or surge				✓	✓
Fire (electrical fault, lightning strike, arson), flood, bomb				✓	✓
Physical damage to equipment				✓	✓
Breaking cables or disconnection of cables				✓	✓
Introduction of viruses				✓	✓

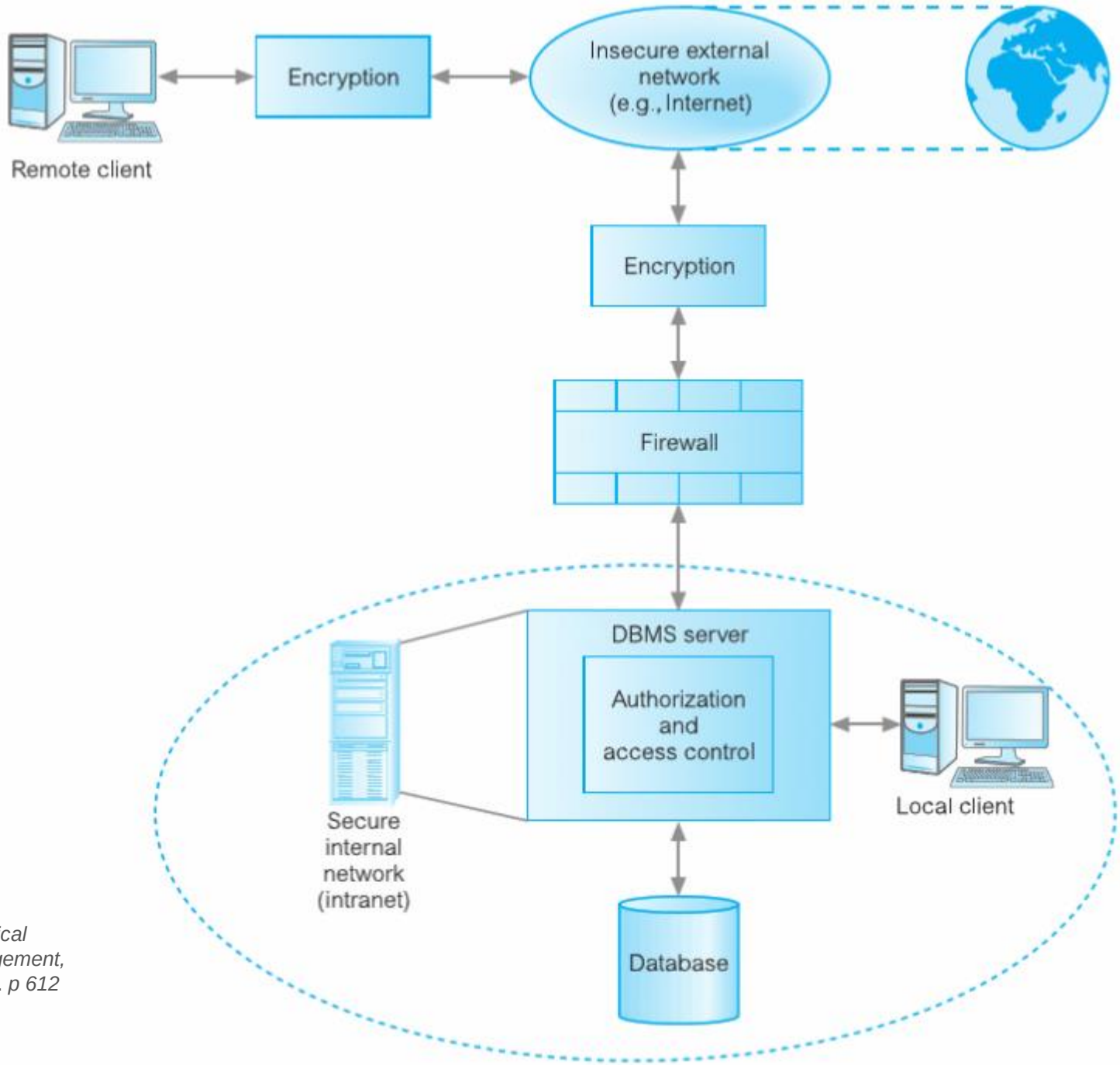
Begg, Carolyn, et al. *Database Systems: a Practical Approach to Design, Implementation, and Management,* Global Edition, Pearson Education Limited, 2014. *p 610*

Countermeasures

- Physical security
- Firewall and Network Security
- Authorization and Authentication
- Views
- Encryption
- Backup and Recovery

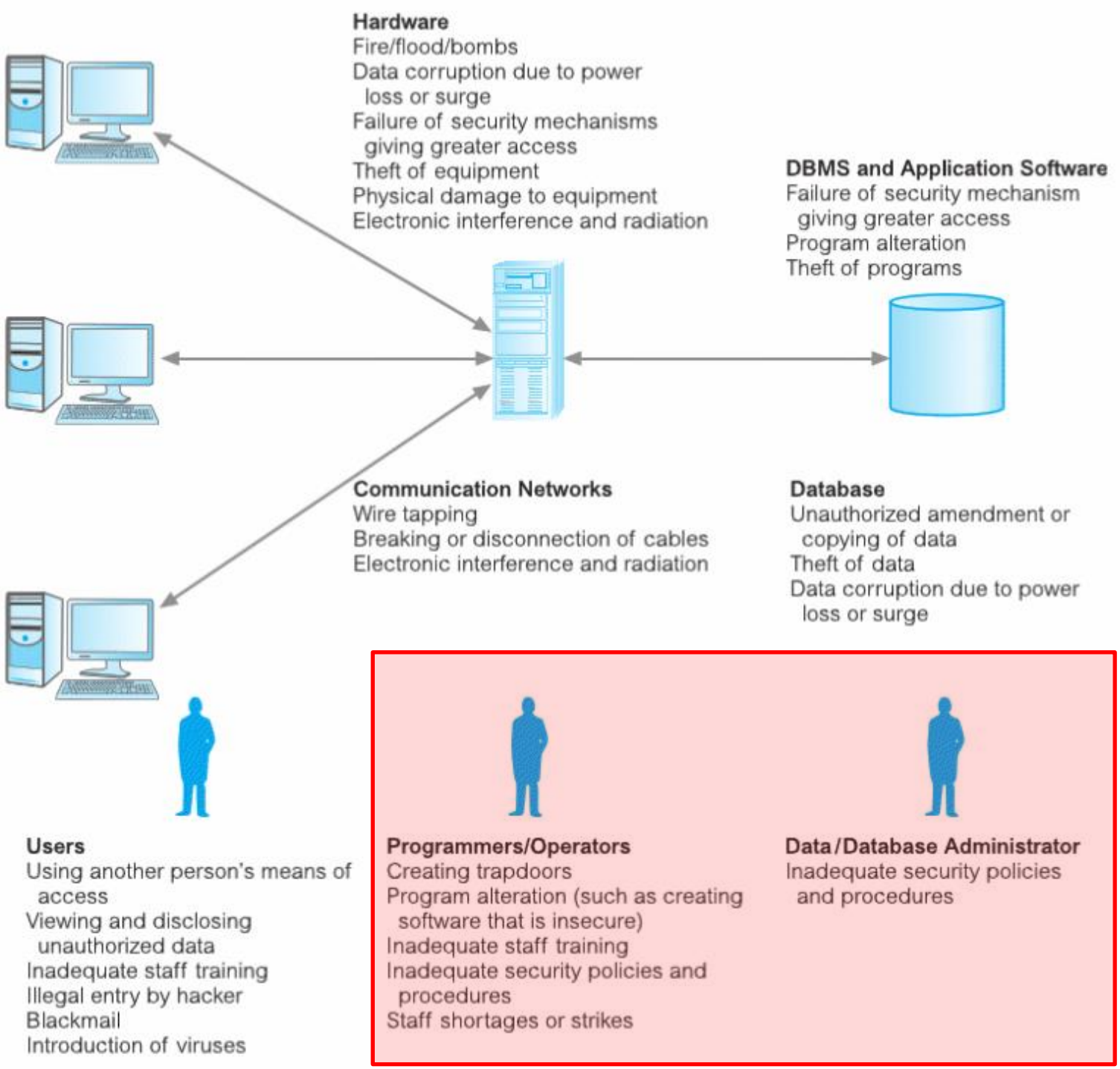
SYSTEM COMPONENT	SECURITY VULNERABILITY	SECURITY MEASURES
People	• The user sets a blank password. • The password is short or includes a birth date. • The user leaves the office door open all the time. • The user leaves payroll information on the screen for long periods of time.	• Enforce complex password policies. • Use multilevel authentication. • Use security screens and screen savers. • Educate users about sensitive data. • Install security cameras. • Use automatic door locks.
Workstation and servers	• The user copies data to a flash drive. • The workstation is used by multiple users. • A power failure crashes the computer. • Unauthorized personnel can use the computer. • Sensitive data is stored on a laptop computer. • Data is lost due to a stolen hard disk or laptop. • A natural disaster occurs.	• Use group policies to restrict the use of flash drives. • Assign user access rights to workstations. • Install uninterrupted power supplies (UPSs). • Add security locks to computers. • Implement a kill switch for stolen laptops. • Create and test data backup and recovery plans. • Protect the system against natural disasters—use co-location strategies.
Operating system	• Buffer overflow attacks • Virus attacks • Root kits and worm attacks • Denial-of-service attacks • Trojan horses • Spyware applications • Password crackers	• Apply OS security patches and updates. • Apply application server patches. • Install antivirus and antispyware software. • Enforce audit trails on the computers. • Perform periodic system backups. • Install only authorized applications. • Use group policies to prevent unauthorized installations.
Applications	• Application bugs—buffer overflow • SQL injection, session hijacking, etc. • Application vulnerabilities—cross-site scripting, nonvalidated inputs • Email attacks—spamming, phishing, etc. • Social engineering emails	• Test application programs extensively. • Build safeguards into code. • Do extensive vulnerability testing in applications. • Install spam filters and antivirus software for email systems. • Use secure coding techniques (see *www.owasp.org*). • Educate users about social engineering attacks.
Network	• IP spoofing • Packet sniffers • Hacker attacks • Clear passwords on network	• Install firewalls. • Use virtual private networks (VPNs). • Use intrusion detection systems (IDSs). • Use network access control (NAC). • Use network activity monitoring.
Data	• Data shares are open to all users. • Data can be accessed remotely. • Data can be deleted from a shared resource.	• Implement file system security. • Implement share access security. • Use access permission. • Encrypt data at the file system or database level.

Operational Environment



Begg, Carolyn, et al. *Database Systems: a Practical Approach to Design, Implementation, and Management,* Global Edition, Pearson Education Limited, 2014. *p 612*

Potential Threats



Begg, Carolyn, et al. *Database Systems: a Practical Approach to Design, Implementation, and Management,* Global Edition, Pearson Education Limited, 2014. *p 611*

Professional Practice and Ethics

- As an IT (Database) professional, in addition to being a good citizen and acting within the law, it is very important to uphold the highest standards of integrity, responsible behaviour, and ethical conduct in professional activities.
- Code of Professional Conduct and Ethics
  - Australian Computer Society (ACS)
  - Institute of Electrical and Electronics Engineers (IEEE)

ACS Code of Professional Conduct

- The Primacy of the Public Interest

You will place the interests of the public above those of personal, business or sectional interests

- The Enhancement of Quality of Life

You will strive to enhance the quality of life of those affected by your work

- Honesty

You will be honest in your representation of skills, knowledge, services and products

- Competence

You will work competently and diligently for your stakeholders

- Professional Development

You will enhance your own professional development, and that of your staff

- Professionalism

You will enhance the integrity of the ACS and the respect of its members for each other

That's All

That's it in terms of content in the unit!

Any Questions?

Next, we will:

- Review the unit
- What next?

This Week's OnTrack Task

- 10.1P Learning Summary Report
  - First part of your **Final Learning Portfolio**
  - Has two parts
    1. Portfolio Overview
       - Outlines how tasks attached in the portfolio demonstrate that you met the ULOs at the level required for your target grade
    2. Your Reflection
       - Review and revisit your learning journey/experience in the unit
       - What did you learn/improved, what you find useful
  - Template is provided in the task resources and unit site

Final Learning Portfolio

- **The ONLY summative assessment that is GRADED**
  - Note that 10.1P Draft Learning Summary Report is NOT your Portfolio
- Complete all tasks required for your target grade
  - You can address comments provided on your tasks (even if they are marked as 'complete') to improve their quality Your final mark/grade depend on the quality of tasks included in the portfolio
- Once you complete all tasks and draft learning summary, you need to generate your **Final Learning Portfolio** using OnTrack

  https://alex.deakin.edu.au/Mediasite/Channel/ontrack/watch/5c0aa70cac9f418082ae3b9ae7efe5ca1d
- Due date: Monday 26 May

Readings and References:

- Chapter 16

Database Systems : Design, Implementation, & Management 13TH EDITION, by Carlos Coronel, Steven Morris

- Chapter 20

Database Systems: a Practical Approach to Design, Implementation, and Management Global Edition, by Begg, Carolyn, et al.

Next Week

-A brief technical review of the important things we learned in this unit

- We'll discuss jobs related to DB/DBMS

- **You can still go to WORKSHOPS, if you want to discuss something!**

- **YES, HELPHUB Sessions will run as usual**

Unit Review: Take-aways

- Relational Database Modelling (Week 1 to Week 4)

  - **Understanding data requirements**: business scenario analysis, system input output analysis (Context Diagram)

  - **Entity Relationship Diagram (ERD):** Entities, Attributes, Relationships, Keys

  - **Normalisation**: 1NF, 2NF, 3NF

- SQL and PL/SQL (Week 5 to Week 8)

  - **DDL:** CREATE, ALTER, DROP TABLE

  - **DML**: SELECT, INSERT, UPDATE, DELETE, JOIN

- Security and Business Intelligence (Week 9-Week 10)

  - Aggregation, summarisation and visualisation of data

  - Business Intelligence and Big data challenges and opportunities

  - Security issues with data and database

Unit Learning Outcomes

ULO1: **Interpret** and **explain** fundamental concepts of data, information, and knowledge and demonstrate an understanding of differences between traditional file systems

ULO2: **Analyse** real-world problems to identify data requirements and **apply** data modelling concepts to **design** and **develop** Entity Relationship Diagrams for efficient data representation and storage , and consider security and privacy considerations.

ULO3: **Design**, **implement**, **evaluate** and **maintain** relational database systems using SQL and Database Management Systems and **explain** the purpose of various SQL commands and operations.

ULO4: **Analyse** and **critique** the achievements of learning outcomes and **justify** meeting specified outcomes through providing relevant evidence and **evaluating** the quality of that evidence against given criteria.

Additional one in SIT772

ULO5: **Conduct** research on and critically **evaluate** tools and technologies used in contemporary business information systems to manage and analyse data.

Our Hope

- We introduce you to the world of data and enthuse to explore further
- You now understand:

  Why database is important for IT graduates?

  Why this unit is core in most of our UG/PG courses?

- You can analyse system's data requirements and design and develop a Database to meet the needs
- You are aware that you will work with some databases regardless of what IT career you are planning after graduation

  - Design, maintain and manages databases (Database or System Administrators, Network Engineers and Security Analysts)

  - Interact with and/or use databases (Web/App Developers, Data/Business Analysts, System/Helpdesk Support, Sales and Marketing)

What next for you?

- In today's world, everything is about data
  - Data is the foundation for Artificial Intelligence (AI) and Machine Learning (ML) systems which are now becoming ubiquitous
- Data security and privacy is one of the biggest challenge
  - Most organisations and government agencies are struggling with this
- There is a huge demand of professionals in these fields
  - plenty of opportunities in industry and research
- You may want explore further to learn more
  - further studies (advanced units as electives, specialised courses, self-study)
  - internships/placements (work-integrated learning, capstone projects)
  - research (Honour's thesis, Coursework master thesis)

Unit Feedback

- Hope you found the unit interesting and enjoyed it
- **Please let us know your feedback**

  - what you liked
  - what we did well
  - where we could improve
- You constructive feedback is very important for us to improve the unit and me personally to improve my teaching

Last but not least

Big Thank you to you all

for a good interactive trimester and nice experience

- I really appreciate your understanding and cooperation
- Please feel free to contact me if I can be of any help

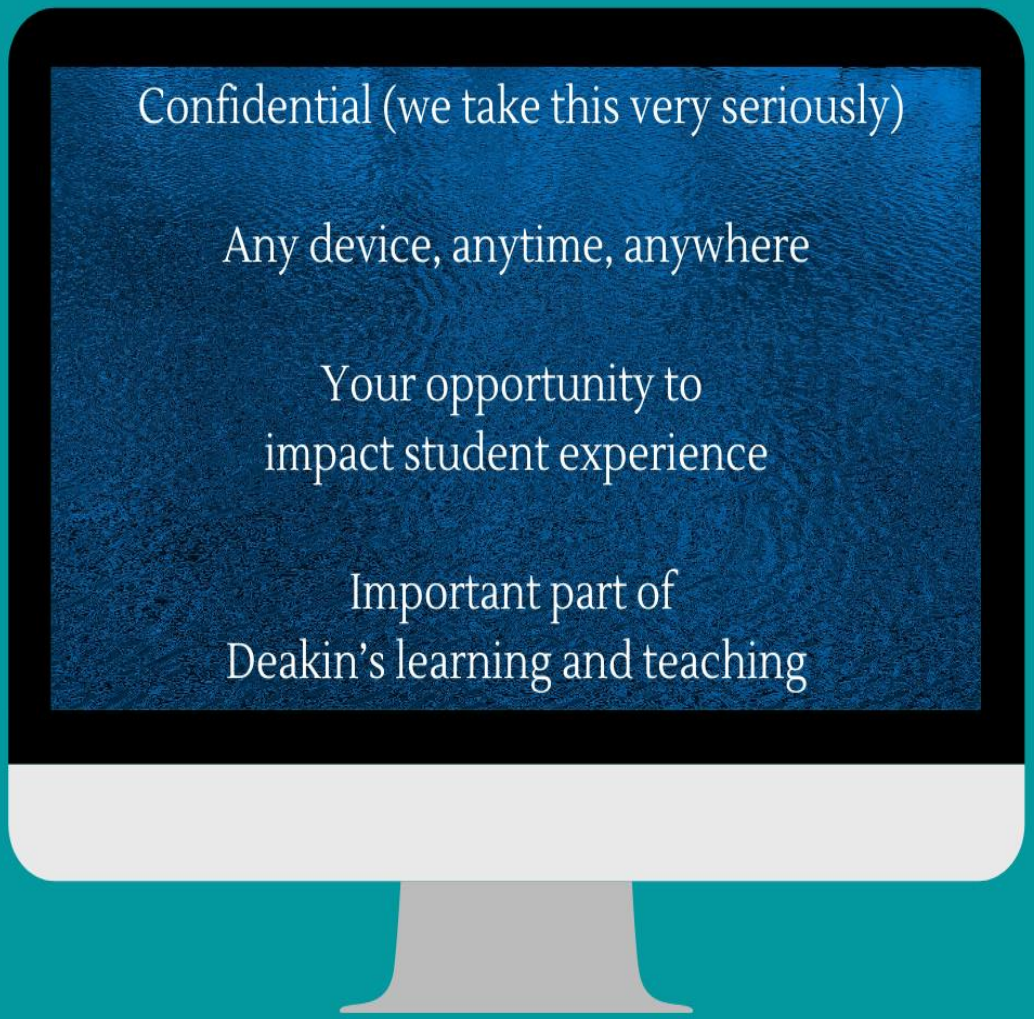
  - academic reference to apply for jobs, internships or further studies

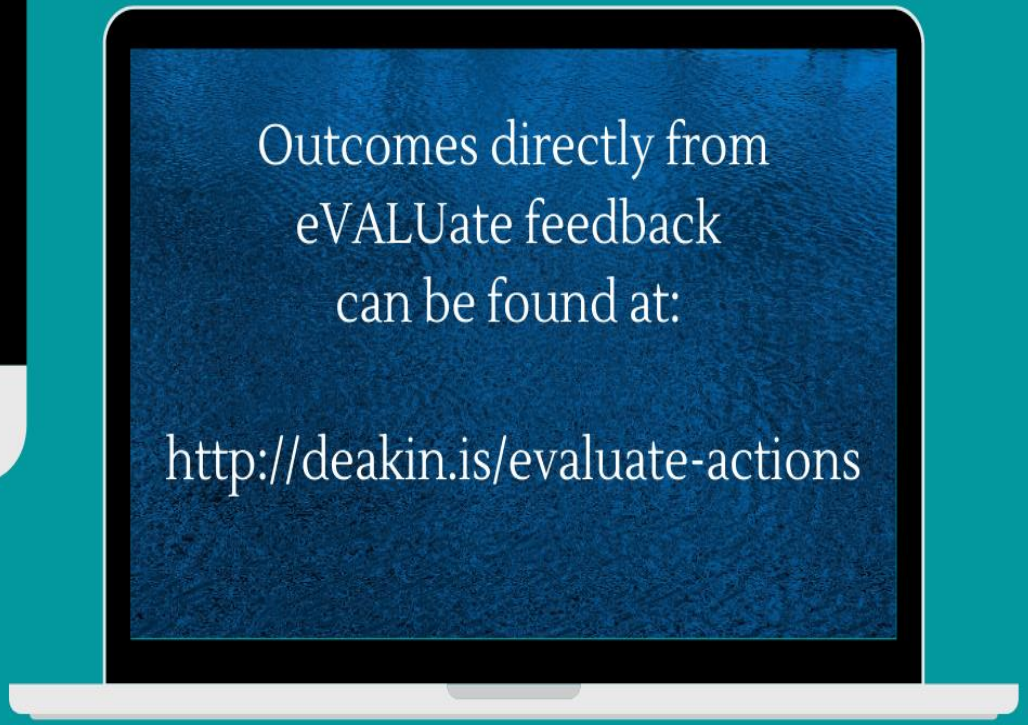
  - if you are interested to do Honour's research or Coursework Major/Minor thesis with me in Health Machine Learning or AI

Wish you all the best for rest of your study and whatever you do after graduation!

eVALUate is now open

This is your chance to give feedback





Giving feedback on eVALUate