ACF2400 notes

What's included?

- Comprehensive notes on all examinable chapters
- Diagrams and tables to summarise key information

Table of Contents

Ethical decision making 5
  Stakeholder Analysis Framework 5
Fraud 6
  The fraud triangle 6
  Preventing and detecting fraud 6
System documentation 8
  Data flow diagrams (DFD) 8
    Context diagrams 8
    Level-0 DFD 8
    Level-1 DFD 9
    Errors in DFDs 9
  Flowcharts 9
    Types of flowcharts 10
  Business process diagrams (BPD) 10
Control and AIS 11
  Internal control 11
  Sarbanes Oxley Act (SOX) 11
  COBIT 11
  COSO-ERM 11
    Internal environment 12
    Objective setting and event identification 12
    Risk assessment and risk response 12
    Control activities 13
    Communication information and monitoring 13
Processing integrity and availability controls 15
  Input controls 15
    Data entry controls 16
  Processing controls 16

  - Output controls 17
  - Availability 17
    - Minimise system downtime 17
    - Backup and recovery 17
- The revenue cycle 19
    - General threats 19
  - Sales order entry 19
    - Take customer order 20
    - Credit approval 20
    - Inventory availability 20
    - Customer inquiries 20
  - Shipping 21
    - Picking and packing 21
    - Shipping the order 21
  - Billing 21
    - Invoicing 22
    - Accounts receivable 22
  - Cash collection 22
  - Summary of duties and personnel 23
- The expenditure cycle 24
  - Ordering 24
  - Receiving 24
  - Approving supplier invoice 25
  - Cash disbursement 25
  - Summary of duties and personnel 25

System documentation

System documentation is used for showing how processed in a business work, and depicting the flow of information between different systems.

Data flow diagrams (DFD)

Data flow diagrams have five main elements:

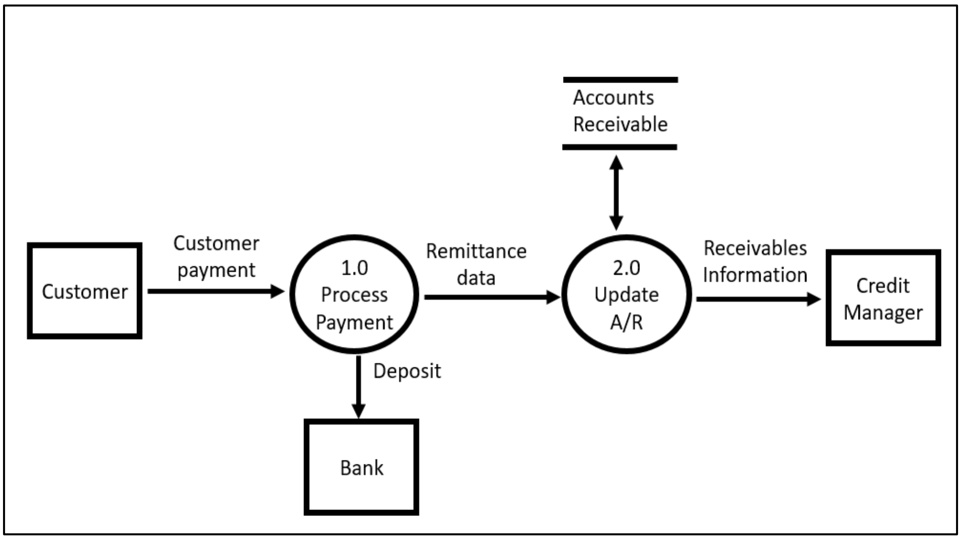
1. Squares, which represent external entities or data sources/destinations
2. Arrows, which represent data flow
3. Circles, which represent actions or transformations
4. Double horizontal lines, which represent data storage
5. Yellow triangles, which represent internal controls

Context diagrams

Context diagrams are the highest level DFD. They only show data sources/destinations, and all data flows connect to **one** process (circle). They are used to depict the inputs and outputs of a system.

Level-0 DFD

These are one step down from context diagrams. They show major steps within the system, each of which are labelled 1.0, 2.0, 3.0, and so on (hence "level-0"). The circles are also labelled with an active form of a verb, such as "**Update** ledger" or "**Process** payment". Since level-0 DFDs show the steps within a context diagram, they should have the same amount of external entities.


Accounts Receivable
Customer
Customer payment
1.0 Process Payment
Remittance data
2.0 Update A/R
Receivables Information
Credit Manager
Deposit
Bank

Control and AIS

Internal control

Internal controls are processed implemented to provide reasonable assurance that important objectives are met, such as safeguarding assets, operational efficiency, providing accurate and reliable information, and more.

- **Preventative controls** are put in place to prevent problems from arising in the first place
    - Segregation of duties
    - High quality staff
    - Controlling access to assets and information
- **Detective controls** discover the problems that have not been prevented
    - Double checking calculations
    - Bank reconciliation
    - Monthly trial balances
- **Corrective controls** correct and fix errors that have occurred
    - File backups
    - Data entry validation

Sarbanes Oxley Act (SOX)

The Sarbanes Oxley Act was implemented into legislation in the early 2000s as a general means of guidance and governance to ensure internal controls existed in US public companies. It covers areas such as management reporting, board governance, and more, and it outlines certain rules for auditing, such as auditor independence, IT security, and so on. It greatly changed rules about auditing committees. Particularly who can be appointed to them, in an effort to increase independence and integrity.

COBIT

COBIT stands for **C**ontrol **Ob**jectives for **I**nformation & **R**elated **T**echnology. It provides a framework for IT governance and management.

COSO-ERM

COSO-ERM is another control framework widely implemented, with its main advantage being its focus on risk assessment and risk management.

Data entry controls

Control	Explanation	Example
Field check	Ensures the type of data is correct	Permits 150 but not "one hundred fifty"
Sign check	Ensures the number is either positive or negative	Permits 200 but not -200
Limit check	Ensures data falls above or below a limit	Maximum hours worked per week is 40
Range check	Ensures data falls within a given range	Days worked in the week must be between 0 and 5
Size check	Ensures data is of a specific length	Employee ID must be eight digits
Completeness check	Ensures all fields are filled in	Will not continue unless all three fields have correct data
Validity check	Ensures entered data exists in master file	Only permits employee IDs already in the system
Reasonableness test	Ensures data entered makes sense logically	Overtime hours must be 0 if an employee has worked below the minimum hours
Check-digit verification	Uses a check-digit to ensure entered data is correct	Credit cards have a check digit at the end

Processing controls

- Data matching: two or more pieces of data must match before continuing
- File label checking: ensures most up to date file version is used
- Recalculating batch totals: compare computer totals to manual totals
- Cross-footing balance test: compares alternative ways of calculating the same thing to identify discrepancies
- Zero-balance test: controlling certain accounts that should maintain a zero balance
- Overwrite protection mechanisms: protect against overwriting or erasing data
- Concurrent update control: prevent users from updating/deleting the same record simultaneously

The revenue cycle

The primary objective of the revenue cycle is to provide the right product to the right place at the right time for the right price.

The four basic activities involved in the revenue cycle are:

1. Sales order entry
2. Shipping
3. Billing
4. Cash collection

General threats

There are general threats that apply to the information within the revenue cycle, and each step also has its specific threats, along with controls that can be implemented to mitigate these threats.

1. Inaccurate or invalid master data
    - Data processing integrity controls
    - Restrict access to master data
    - Review all changes to master data
2. Unauthorised disclosure of master data
    - Access controls
    - Encryption
    - Tokenisation
3. Loss or destruction of master data
    - Backups
    - Disaster Recovery Plan
4. Poor performance
    - Managerial reports

Sales order entry

The steps within sales order entry are:

1. Take the customer's order
2. Approve their credit
3. Check if there is available inventory for sale
4. Respond to customer inquiries (may be done by separate customer service team)

Take customer order

Customers request sales through a document known as a sales order. These can be entered via Electronic Data Interchange, where the customer enters the data directly to the business. A customer's sales history can be used to customise solicitations.

Threats	Controls
Incomplete or inaccurate customer orders Invalid orders	Data entry controls

Credit approval

Sales orders should be approved before the order is processed. For existing customers who are purchasing under their limit and have no outstanding balances, a sales clerk could do this, but for new customers, or ones over their limit or with outstanding balances, a credit manager should approve them (segregation of duties).

Threats	Controls
Uncollectible accounts	Credit limits Authorisation by a credit manager Aged receivables report

Inventory availability

If there is sufficient inventory, the order should be processed and a picking ticket should be sent to the shipping department to authorise release of goods. An acknowledgement of the successful sales order should be sent to the customer.

If there is insufficient inventory, a back order should be placed for the required goods (for manufacturing companies, this is the production team; for retail companies, this is the purchasing team).

Threats	Controls
Stockouts Excess inventory	Perpetual inventory system Bar codes or RFID for inventory tracking Sales forecasts and activity reports

Customer inquiries

Threats	Controls

The expenditure cycle

The four steps in the expenditure cycle are:

1. Ordering
2. Receiving
3. Approving supplier invoices
4. Cash disbursement

Ordering

Decide what to order, when, and for how much. Inventory control systems typically include EOQ (economic order quantity) and JIT (just in time).

Then decide of suppliers that will provide high quality goods at a fair price, and are dependable. Then place a purchase order.

Threats	**Controls**
Purchasing inferior quality goods	Purchase from approved suppliers Track and monitor product quality per supplier Hold purchase managers responsible
Purchasing from unauthorised suppliers	Maintain list of approved suppliers Configure system to only permit approved suppliers Review and approve purchases from new suppliers
Kickbacks	Prohibit receiving gifts from suppliers to purchasing personnel Require purchasing agents to disclose interest in suppliers Job rotations and mandatory vacations

Receiving

The receiving department decides whether to accept goods and verifies quantity and quality of the delivery. This includes checking purchase order numbers on received package against purchase order sent. If goods are damaged, a debit memo will be sent to supplier, who then returns a debit memo, which is passed onto the accounts payable team to update the accounts.