Global Information Assurance Certification Paper

Jamie Rossato

Submitted 23 Dec 2004

G7799 Practical

Abstract

This Practical covers the implementation of an ISMS for the Regulatory Compliance Unit (RCU) within ACME Parcels, an Australian international parcel distribution (courier) company.

The RCU's mission is to provide accurate, timely and relevant information to Law Enforcement and Customs Services, in accordance with documented RCU processes under each respective nation's law. IT services for the RCU are provided by ACME Parcels' IT Services Unit (ITSU) which provide support from their main datacentre.

ACME Parcels has a Security Committee, headed by the CEO. An issue already identified by the Committee is their lack of involvement in IT Security. The committees intention in implementing 7799 is to address that vulnerability and strengthen IT security by ensuring a continuous process of Plan-Do-Check-Act is followed. The RCU, for its part, has been selected as the pilot site for 7799 implementation.

This paper will detail how the ISMS for the RCU was implemented under a Prince 2 project methodology and a FMECA analysis, providing examples at each stage.

Part One: Define the System

ACME Parcels is a privately owned international parcel distribution (courier) company with its headquarters in Australia.

The company forms part of the communications sector of the Australian economy, an industry group that encompasses postal, courier and telecommunication services. In 2002-03 this sector of the Australian economy generated revenues of $41.6 billion, and industry gross product of $20.9 billion.[1]

Over the last five years courier services haven grown weakly, at 1.8% per annum (p.a), compared to Telecommunications which grew at 6.2% p.a over the same period. '*This is due mainly to a result of the growth in telecommunications services providing a substitute service through electronic communications'*. [2]

According to IBISWorld's *Review of Communication Services in Australia*, courier services, of which ACME Parcels is a part, are expected to experience average real growth of 2.5 percent p.a. However competition is also expected from advancements in communication technology and advancements in e-commerce will in particular affect the messenger and small document market. Offsetting this trend is that communications improvements will allow businesses greater freedom of location and lead to an increased volume of parcel and small consignment traffic away from the Central Business District. '*The increase in e-commerce is also expected to impact positively as it provides fulfilment services'.* [3]

ACME Parcels industry profile is inline with the IBISWorld Review. While 60% of its parcel distribution (by volume) is within Australia, profit margins in this segment are small and over the last five years revenue growth has been flat. International distribution by comparison has grown steadily in volume and revenue, generating the lion's share of operating profits. Furthermore, while distribution between Australia and New Zealand constitutes the majority of work (currently 75% of all international distribution is between Australia and New Zealand), ACME Parcel's board has recently adopted a strategy of growing international distribution in under-represented countries in Asia, Europe and South America.

ACME Parcels has approximately 500 employees, supplemented by a large number of delivery contractors. The majority of employees are located in Australia, followed by 50 based in New Zealand. At its branch offices in Oceania, the Americas, Asia and Europe there are between 5 and 20 employees. There are a total of 22 offices located worldwide. An organisation chart is attached at Appendix A.

---

[1] All statistical data courtesy of *Communication Services in Australia*, IBISWorld Pty Ltd, 16 Mar 2004
[2] ibid
[3] ibid

Within the ACME Parcels business is the *Regulation Compliance Unit* (RCU). This organisation is responsible for ensuring all international parcel distribution conducted by the business complies with the laws of all countries ACME Parcels has dealings with. As well as liaising with each countries Customs or Border Control Offices the RCU coordinates assistance to national law enforcement agencies in accordance with that country's law. Assistance includes handling search warrants or court subpoenas and coordinating parcel tracking, intercepts or diversions.
The RCU reports directly to Chief Legal Counsel. The RCU has 12 employees, the majority of personnel of which (11) are collocated at ACME's head office. The only other permanent RCU presence outside Australia is an employee based in an Asian country at the branch office. RCU staff visit branch offices at least annually and on an as required basis where their presence can facilitate better service or assistance to government agencies.

IT services for ACME Parcels are managed centrally through the *IT Services Unit* (ITSU). ITSU has a total staffing of 25 employees; 22 are employed in Australia and the remaining three in New Zealand. The majority of personnel are located at the company's datacentre in Brisbane, Australia. The other main ITSU locations are in ACME Parcels main distribution centres in New Zealand and Asia. ACME Parcels Head Office, located in Sydney Australia is supported through the company's virtual service desk run out of the Brisbane Datacentre.

Where the ITSU believes incident resolution requires onsite technical expertise beyond the capabilities of the local staff, a contractor will be dispatched. There is a company-wide agreement with an international IT company to provide this service.

The ITSU provides 1st and 2nd line support to all ACME Parcel IT systems. Where further, specialised knowledge is required, the ITSU has maintenance agreements with key vendors.

Within the RCU, which is where my Information Security Management System (ISMS) shall focus; there are two information systems used only by the RCU:

- Package and Service History (PASH)
- Investigation Management System (IMS)

PASH is an Oracle database containing information on all parcels handled by the business. It is used to answer requests from law enforcement agencies against a range of criteria. PASH is not connected to the ACME Parcels core operational information system – the Parcel Tracking System (PAT).[4]

Every two hours, PAT runs a routine that produces a data file containing information on the status of all parcels in the system and writes it to a

[4] The Parcel Tracking System (PAT) operates from the Brisbane Datacentre. There is another PAT server farm, located in Asia, that provides continuously availability and forms part of the overall business continuity plan.

dedicated folder on one of the PAT servers. An FTP service, operating from the RCU polls the folder for new files and when a new file is detected, downloads it from the PAT server to the RCU FTP server. The file on the PAT server is deleted as part of the process.

PASH polls the FTP server and when a new file is detected, uploads it into the PASH database. Fields are validated and if any errors in the upload process are detected, the ITSU and RCU manager are alerted via email. A successful upload is logged and an email sent to the RCU email account. The PAT files on the FTP server are deleted automatically as part of a weekly run job.

The PASH database contains information on all parcels in the system as well as the history of each parcel's status going back six months. When a law enforcement or border protection agency make a request to ACME Parcels for information regarding a parcel, a sender, or recipient, the RCU is responsible for processing the request. The RCU, once satisfied the request is within the relevant agencies statutory authority and properly executed, will conduct a search on PASH to obtain the information requested. The results of the search are produced as a text file that can be emailed, or printed to be faxed or couriered, to the requesting agency. Files emailed to agencies are encrypted using PGP where those agencies have a public key, however these are very few of these (under 5% of all requests) and the majority (90%) are faxed.

Whenever a member of the RCU receives a request from a law enforcement or border protection agency, the details of the request are entered into the Investigation Management System (IMS). IMS is a SQL database with a customised front-end that is used to track active requests as well as serve as a record of completed requests / investigations. RCU staff enter information pertinent to each request and its progress in order to ensure that the relevant information can be produced in a court (should such information be subpoenaed) as well as meet Australian privacy principles.

Other systems used in the RCU are workstation applications (Microsoft Office) used in the preparation of reports, correspondence and budgets. The RCU is connected to the corporate network (TCP/IP) and email system (Microsoft Exchange) through a Cisco PIX firewall. (see Appendix B).

The ITSU are responsible for the management of the RCU systems and firewall. The ITSU Help Desk monitor system generated emails that are sent to an RCU email account. Remote access to the ITSU PASH and IMS systems is possible from the ITSU datacentre through a single, dedicated terminal. This terminal can be physically accessed by any ITSU personnel. RCU workstations can be accessed remotely via the ITSU help desk staff. Internal firewalls within ACME Parcels are managed centrally through a dedicated management terminal, also password protected. The passwords to the PASH / IMS terminal as well as the Firewall management terminal are restricted to the ITSU shift leaders (4) and the changed every 90 days.

Security within ACME Parcels is taken seriously. The critical nature of the PAT system has ensured that IT security is taken equally seriously. Company security is the responsibility of the Manager, Security and Loss Prevention who reports to the General Manager, Operational Services. There is strong physical security at ACME Parcels distribution sites and at the main datacentre. The Corporate Office, where the RCU is part of an office 'park' which is near, but not located with, the Sydney distribution centre.

The Manager Security and Loss Prevention, has established strong physical and personnel security measures at ACME Parcel sites. Physical controls in place at the distribution sites include:

- Chain link fences around the facility
- Main access point controlled by security staff during working hours
- Regular perimeter patrols day and night
- Employee car park inside the site (and vehicles subject to search on exit)
- Building access controlled by locks or key card (depending on size of site)
- All buildings alarmed and monitored, either to onsite security, or remotely monitored.

Personnel security controls on sites include:

- All personnel must wear ACME Parcels ID card onsite
- All visitors must be accompanied anywhere, particularly where client parcels are held or sorted.
- Delivery contractors are restricted to the pick up / drop off area(s)
- As part of their contract, Delivery contractors permit ACME Parcels to conduct a police check on them. This is at ACME's expense and normally only occurs where ACME have repeated issues with late or non-delivery of parcels.

At ACME Head Office, three floors (1-3) of a modern office block are leased. The RCU as part of Finance and Legal, are located on the second floor. The floor is a mix of open plan in the centre, with offices around the outside. Day to day access is via two elevators which open into a small (unmanned) foyer. Glass doors fitted with electronic "swipe" card locks open onto the office space. The RCU is configured with two groups of four desks and one group of two in the open plan, with the RCU manager having a lockable office. The RCU have their own networked printer and can secure material in a four drawer safe which is located next to the printer.

The PASH, IMS, FTP Server and Firewall are all located in the Head Office Server Room. The room is located next to reception on the first floor and access to the Server Room is controlled by the same "swipe" card used elsewhere. Inside the room the RCU equipment is located in its own rack, which is lockable, but not locked. There is a single UPS (650 VA) for all RCU systems. If access is required into the server room, there are several "power users" from Finance who have access. Contractors who require access have to see one of these power users. No RCU personnel have access to the room.

Personnel at Head Office are issued, but rarely display, ACME Parcel ID cards. All personnel in Finance and Legal are required to sign non-disclosure agreements as a condition of employment.

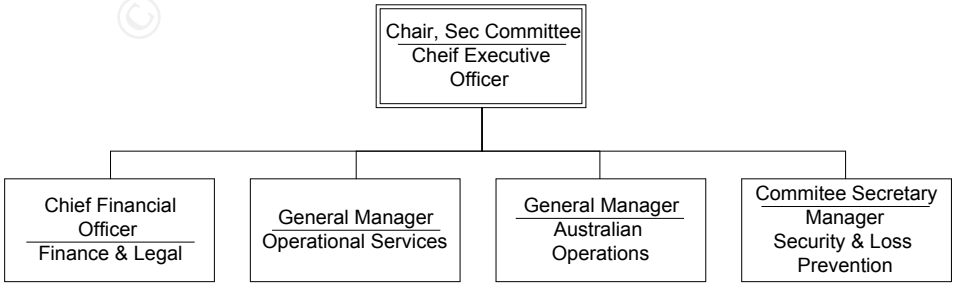
The Brisbane Datacentre, is co-located with the Brisbane site, but is separated from the main facility by a chain wire fence and has a separate entrance. It is a one story brick building that was refurbished specifically as a datacentre. Access controlled by electronic "swipe" card locks. There is one lock on the main entrance which opens onto the ITSU office space and another for access onto the server floor. The emergency exit is secured and alarms on opening. There are cameras in the datacentre monitored by ACME Security next door and all alarming is connected into the Brisbane site. The datacentre maintains a battery bank and diesel generator to provide continuous power to the IT systems in the event mains power is lost. ITSU staff wear ACME Parcels ID card onsite are sign non-disclosure agreements as a condition of employment.

IT Security is primarily the responsibility of the ITSU Unit Leader who operates as the de facto Information Security Officer (ISO). The ITSU Unit Leader has had a number of company wide IT policies endorsed by the CEO. These relate to:

- Email and internet access (focussing on acceptable use)
- Terminal and workstation security (focussing on use and security of passwords)
- System configuration and change management
- Virus Protection (anti-virus measures)
- Physical security of IT equipment

All of these policies are based on the security principles of *Confidentiality*, *Integrity* and *Availability*. Supporting these policies is a number of ITSU procedures and guidelines to assist the ITSU in providing operational support to the rest of ACME Parcels.

There is a Security Committee, headed by the CEO. An issue already identified by the Committee is their lack of involvement in IT Security. The committees intention in implementing 7799 is to address that vulnerability and strengthen IT security by ensuring a continuous process of Plan-Do-Check-Act is followed. The RCU, for its part, has been selected as the pilot site for 7799 implementation.



ACME Parcels Security Committee

Scope: The ISMS shall be restricted to those systems used within the RCU and encompass PASH, IMS, office applications and email. It includes the

personnel and processes employing these information systems within the RCU.
The reasons for selecting the RCU is that the security of the organisation's systems is of critical importance to the ACME Parcels, particularly as it seeks to grow its international distribution. There are significant risks (legal, financial and reputational) associated with the compromise of RCU security. As such, there is a need for strong, effective, security and audit controls that are not only documented, but known and practiced.

Part Two: Plan

There are a number of steps to be undertaken before successfully delivery of an ISMS for the RCU. To achieve that, ACME Parcels intends to follow the Prince 2 Project Process to prepare, implement and improve on the existing IT security for the RCU system. Briefly, Prince 2 was selected for project management for the ISMS implementation, partly because it is already used by ACME Parcels, but also what it provides relates to some of the key requirements meeting 7799 controls:

- *'Controlled management of change, in terms of investment and return on investment* [e.g. Controls A.10.5.1 and A.10.5.2]*;*
- *Active involvement of users and stakeholders throughout the project to ensure that the product(s) will meet the business, functional, environmental, service and management requirements* [e.g. Controls A.4.1.1, A.4.1.2 and A.4.1.3]*; and*
- *An approach which distinguishes the management of the project from the development of the product(s), so that the management approach is the same whether the project is to build a ship or implement new working practices'* [i.e. Control A.8.1.5].[5]

Important components of the project plan include the Business Case, Project Organisation, Project Plans, Controls, Risk Management, Quality Assurance, Configuration and Change Management. One of the benefits of using Prince 2 is it provides controls throughout the project and ensures regular reviews are conducted. This is important in ensuring senior management (in ACME Parcels case, the CEO and CFO) are involved throughout the project's life, at appropriate times.

The Project Start Up which include creating the RCU ISMS Steering Committee, preparation of the project brief, approach and likely stages. It is here that the ISMS scope would be confirmed, along with a charter and mission statement for senior management approval (the ACME Parcels Security Committee).

The Project Direction process would be initiated to ensure authorisation and ad-hoc direction would be provided by senior management to the project. The signoff of the CEO would be a critical milestone early on in the project as such signoff ensures there is high level commitment to the project. Existing ACME

[5] *Managing Successful Projects with PRINCE 2*; Office of Government Commerce; Norwich, United Kingdom; 2001; p.1.2

Parcels policies would also provide guidance to the project team throughout the project.

Controlling each project stage would be undertaken by the Project Manager. Hand in hand with stage control is management of stage boundaries, where the Project Manager ensures the project remains focussed on delivering the ISMS to the RCU. Likely project stages include:

- A review of existing ACME Parcel Security Policy and development of a high level RCU Security Policy. This is aided by the existence already of RCU business objectives which are:
    - Provide accurate, timely information to Law Enforcement and Customs Services in accordance with national and international laws in order for ACME to meet its obligations under each respective nation's law.
    - Disclose only the information requested in the search warrant or court subpoena in order to protect the privacy of ACME clients.
    - Protect the security of Law Enforcement and Customs Service requests in order to prevent the compromise of enforcement operations.
- Establishment of the RCU Security Organisation. In addition to work already undertaken with charter and mission, the project may identify internal security teams and committees (of which more detail later).
- Undertake asset identification within the RCU. This is likely to include asset categories such as Information (classification of data), Software, Personnel and Physical assets.
- Undertake risk assessment on identified assets using the FMECA methodology.
- Undertake Risk Mitigation by defining both security controls and audit controls.
- Write up the policy with statement of applicability. This must include statements on controls that do not apply, as well as those that do.
- Develop the RCU Security Awareness Program and conduct training of RCU personnel in accordance with it. This training will assist in overcoming possible objections, as well as demonstrate the benefits of introducing controls.

No project is complete without supporting documentation. Some documents that will be required to be developed and maintained during the project include:

- Business Case and Project Approach
- An Approval document (from the CEO endorsing and authorising the project)
- Communications Plan (particularly important for managing approvals)
- Project Initiation Document (which defines the ISMS scope, its deliverables and exclusions)
- The Project Plan (including the overall timeline, pre requisites, dependencies, planning assumptions, stage breakdown, budget and resource requirements)
- Stage Plans and related acceptance criteria, for each stage.
- End of Stage reports

- Supporting documents such as Project Issue Log, Project Risk Log, Project Quality Log and Exception reports
- Post Project, Post Implementation Report which would include any lessons learnt.

The project would also maintain a library with relevant ACME Parcel policies, guidelines, standards and procedures. These would include the existing IS Policies (Email and internet access; Terminal and workstation security; System configuration and change management; Virus Protection; and Physical security of IT equipment). There would also be reference to existing RCU standards and procedures for handling Law Enforcement warrants as well as legal and audit policies and procedures.

Asset Identification

An asset is '*anything valuable and useful'*.[6] Within the RCU, identification of assets will require the project to firstly determine what it is that is valuable and useful. This is critical so time or effort is not wasted by over classifying or classifying every item within the RCU as an asset (i.e. a pencil). Assets can then be placed into an inventory and assigned into categories to assist in determining how to determine the risk associated with each asset.

Asset identification should start with the ISMS Committee who should define the asset categories. RCU staff should then be interviewed, including the overseas member by phone. ITSU staff who support the RCU should also be interviewed to identify any other assets. Other ACME Parcel personnel, such as Finance and Legal may also be interviewed.

Broad categories likely to be identified within the RCU Asset Inventory could include:

- Physical assets
- Software
- Information
- Personnel
- Network and Telecommunications links

Each asset category could then be broken down further:

RCU Asset Category

Asset: Information		
Sub-Category	**Asset Example**	**Importance**
General (public)	Building addresses of ACME Headquarters	Least important
ACME	PAT Data, Employee details, PCs	Some importance
RCU	PASH Database	
Law Enforcement	Certain Data Fields within IMS	Most important

Risk Identification and Management

To identify risks within the RCU, the FMECA process will be employed. FMECA is a US Military Standard for Risk Assessment (MIL-STD-1629A). Because this process looks at points of failure, rather than arbitrary or emotive

[6] Collins English Dictionary, 4th Australian Ed, Harpers Collin, 1998

decisions on "what could go wrong" it is well suited to the RCU's requirement of ensuring that worst case events do not occur. As the Standard sets out in the foreword:

'*While the objective of an FMECA is to identify all modes of failure within a system design, its first purpose is the early identification of all catastrophic and critical failure possibilities so they can be eliminated or minimized through design correction at the earliest possible time*'[7]. Employing the eight step FMECA approach, an example of how the RCU would employ FMECA is provided below.

Step One: **Define the System**

To start the process, the system to be analysed must first be defined. For this project, the RCU itself is the system. It would include the physical location of the RCU offices, its personnel, its hardware, software and the information it processes. At this part of the process, the system's mission is also defined. As well as defining the system, interfaces to other systems would be explored. For the RCU there are several system levels. The highest level would be the RCU itself, with lower 'local' levels consisting of hardware, software, existing policies and any other entity that provides a means for the RCU to achieve its mission.

RCU System Definition

System	ACME Parcels Regulatory Compliance Unit (RCU)
Mission	To provide accurate, timely and relevant information to Law Enforcement and Customs Services, in accordance with documented RCU processes, in order for ACME Parcels to meet its obligations under each respective nation's law
Interfaces	• Law Enforcement Agencies • IMS System • PASH System • ITSU and other ACME Parcels Personnel • RCU Personnel (Asia) • Office computer systems (word processing) • Email and Secure Email • Printer and Fax equipment • RCU Firewall
Performance Criteria	**Mission Time**: Extended Business Hours in Australia and Asia. • Acknowledgement of request / warrant within two hours • Respond to request / warrant within two business days • No unauthorised disclosure of Law Enforcement information • No compromise of ACME Parcel or Law enforcement data • Compliance with Australian and relevant overseas law

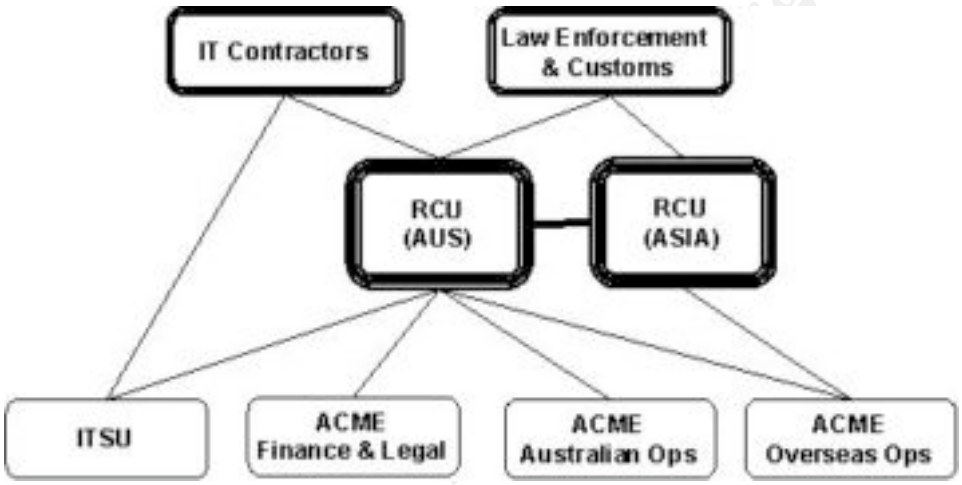
[7] MIL-STD 1629A, *Military Standard Procedures for Performing a Failure Mode, Effects and Criticality Analysis;* USA Department of Defence; Washington, USA; 1980, p.1

Step Two: **Create Block Diagram**

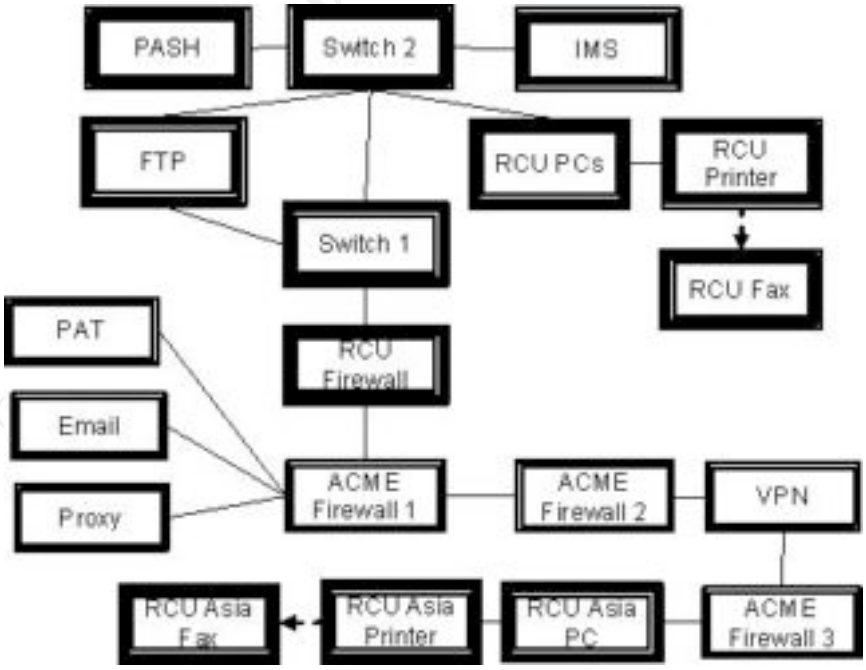
The Block Diagram is an '*illustration of the operations, interrelationships and interdependencies of the functional entities of a system*'[8]. By creating the Diagram all interfaces can be viewed simultaneously. Critical interfaces and information pathways may therefore become more evident.

Because this has not been undertaken before, the first Block Diagram for the RCU will be at a fairly high level. High level Block Diagrams can subsequently be broken down into smaller sub-systems with more detail for further analysis.

Some High Level Block Diagrams are illustrated below.



Block Diagram 1: RCU Functional Entity Relationships (High Level)



Block Diagram 2: RCU System Entity Relationships (High Level)

[8] ibid; Section 4.1.4

An essential part of Block Diagram creation is ensuring that all stakeholders (process owners) are consulted. For the RCU this would involve the ITSU, who have a far greater understanding of many of the technical interfaces than RCU personnel, as well as other key personnel in ACME Parcels (such as Finance and Legal). It is desirable that once created the Block Diagram is maintained by the stakeholder.

Step Three: Identify Module, System and Interface Failures

The Block Diagrams are now ready to be analysed. Failure can occur either within the 'block' or along the 'line'. Each block and line should be assessed to determine what failures could occur.

In the Military Standard, the probability of occurrence that could result in a failure (likelihood of failure) is divided into five categories, from Frequent to Extremely Unlikely. Each occurrence is assessed against a defined operating period. For the RCU, a realistic period of time could be per annum, as per the example below.

Likelihood Rating

Category	Occasion	Definition	Example
Level A	**Frequent**	A high probability of occurrence during the year	The second floor access door at ACME Headquarters will be left propped open by an employee
Level B	**Reasonably probable**	A moderate probability of occurrence during the year	An RCU employee will leave their desk without locking the terminal (Ctl-Alt-Del)
Level C	**Occasional**	An occasional probability of occurrence during the year	RCU will leave the safe open and unattended
Level D	**Remote**	An unlikely probability of occurrence during the year	Mains power will be lost at ACME Headquarters for more than 30 minutes
Level E	**Extremely Unlikely**	A failure whose probability of occurrence is essentially zero during the year	Fire will destroy the RCU office in Australia

With the Level C example, it is assessed; perhaps due to a quantifiable number of times this has previously occurred, or a qualitative assessment; that the RCU will leave their four drawer safe open while the RCU area is unattended (or perhaps event overnight). While this 'failure' may not prevent the RCU performing its mission, it may mean a performance criteria is not achieved. Of course the analysis does not stop here, and as such failures are further worked through the FMECA process, issues such as severity, preventative and detective controls are raised.

Step Four: Determine Severity

Step Four analyses the severity of each failure. Severity classifications are assigned '*to provide a qualitative measure of the worst potential consequences resulting from design error or item failure*'[9]. These failures are assessed first at the 'local' level, i.e. what the consequence of that failure is at the lowest level. The failure should be described and assigned a severity.

Severity Rating

Category	Descriptor	Definition	Example
IV	**Minor**	Some impact on fulfilling requests in timely fashion. Total time lost less than one business day	Power outage at ACME Headquarters under 10 minutes
III	**Marginal**	Some impact on fulfilling requests in a timely fashion. Total time lost more than one business day, but less than three business days	Unscheduled PASH Server outage during business hours
II	**Critical**	RCU operations curtailed for more than three business days; may be unable to meet legal or statutory requirements	PASH data lost due to Server crash, but recoverable and not compromised
I	**Catastrophic**	RCU to stop operations until resolved, possible impact on ACME's ability to operate in a country; adverse Media attention likely; legal charges possible	Law Enforcement Agency data compromised

Each local failure may also have an effect on a higher level system or operation. With FMECA, the effect of each local failure is considered at each higher level until an end effect that may consist of a number of separate, cascading local failures is determined.

As an example, the RCU safe may be left open, unattended and is categorised as a Level C Likelihood, with a Level III Severity. At the same time, the second floor access door at ACME Headquarters is left propped open by an employee (Level A, III) and a non-ACME employee stops on the second floor (Level B, IV). Taken together these two local failures combined with what otherwise would be a relatively benign event, could have an end effect rated Remote (D) and Catastrophic (I). End effects therefore must take into consideration cascading local failures where two (or more) separate local failures lead to a critical or catastrophic failure.

Severity and Likelihood can be combined to assist in evaluation and prioritising further assessment. This is important where there are numerous systems and interfaces and a limited time to conduct a detailed analysis on every one. In the table below, Failures assessed as both Frequent (A) and Catastrophic (I) should be given first priority. Those assessed to occur less frequently, or with less impact should be evaluated later (those 2 through 8).

[9] ibid; Section 4.4.3

Priority

Likelihood	Severity			
	IV	III	II	I
A	4	2	1	1
B	5	4	2	1
C	6	5	3	2
D	8	6	4	3
E	8	7	5	4

As an example, one such failure may be RCU FTP server failing to connect properly to the PASH Server. The failure was due to the FTP service not being manually restarted after a scheduled reboot of the machine. As a result, updates from PAT are not received by PASH. This is assessed as Reasonably Probable (Level B) with a Severity rating of Critical (Category II). The priority for further analysis should therefore be second, behind those rated Priority 1.

Step Five: Failure Detection Method

For some failures, it may be impossible, or near impossible to detect failure before it occurs. For others, controls may either exist, or be capable of being introduced. This step examines existing failure detection controls and their adequacy. It identifies the current detection control (or mechanism) and how that control compensates for the failure.

Failure Detection

Failure: FTP service fails to be restarted following reboot	
Severity Rating	(II) Critical / (B) Reasonably Probable → Priority 2
Current Detecting Mechanisms	RCU does not receive the usual "success" email from PASH
Current Compensating Controls	RCU personnel notice that they have not received any "success" email, possibly only after several days
Adequacy of Current Controls	Poor. • The administrator may not correctly check all necessary services are running before leaving the server. • The system should alert to failure as well as success. • The ITSU should be alerted to a technical failure, not just the RCU.

Step Six: Describe Actions to Prevent or Eliminate Failure

This step examines and defines any additional compensating controls required to prevent or detect failure. To reduce the severity of a failure, redundancy is a commonly employed control, as are the implementation of alternatives such as backups or standby systems.

In many cases the actions of individuals becomes an important part of managing or mitigating the failure. Termed 'Operator Actions' in FMECA, such actions are considered not just in a positive, corrective fashion, but also '*the consequences of any probable incorrect action(s) by the operator in response to an abnormal indication should be considered and the effects recorded*'[10].

[10] ibid; Section 5.8.2

Actions to Prevent or Eliminate Failure

Failure: RCU Safe left open overnight	
Incident Handling	On detection the next morning of an open safe: • Notify RCU Manager • Commence 100% audit of material • Have entry / exit logs checked • Raise incident report for Manager, Security and Loss Prevention
Preventative Controls	Have individual allocated responsibility for closing safe (Controls A.4.1.3, A.6.1.1, A.6.1.4, A.7.1.4) Regular training and notices reminding people to close safes (A.6.2.1) Have safe moved into an office which self locks (Control A.7.2.1) Have information handling procedures that follows a "you open, you close" rule (Control A.8.6.3)
Detective Controls	Have others report any failures of people to close safes (A.6.3.1) Link safe to alarm system that will generate alarm if left open for either a certain period or after a certain time (Control A.9.7.2)
Compensating Controls	Have individual allocated responsibility for checking the safe is closed (Controls A.4.1.3, A.6.1.1, A.6.1.4, A.7.1.4) Have disciplinary procedures for breaches (Control A.6.3.5) Have documented incident handling procedure (Control A.8.1.3)
Consequence of Incorrect Handling	Incorrect Handling, which may include an individual simply closing the safe without notifying anyone or conducting an audit of the contents, could possibly result the compromise of data going undetected

Step Seven: Consequence of Additional Controls

In Step Seven, the introduction of each control is evaluated to determine if it has any other consequences on the system. This is an important step as the introduction of a new control must have some effect. The impact of the additional control can be rated from Very Positive through to Positive, Neutral, Negative or Very Negative.

This rating can be determined either qualitatively, quantitatively, or a combination of the two. Two common criteria to measure consequence are cost and complexity. Cost can be measured in dollars – both to implement and also to maintain; while complexity can either be simple to implement and / or maintain, or be a labour and /or process intensive process.

Clearly those controls that rate either Very Positive or Positive should be adopted, while those that are negative should not, or at least be re-evaluated. Neutral controls may be implemented according to these or other business priorities.

Consequence

Failure: RCU person leaves desk without manually locking terminal.	
Compensating Control(s)	Terminal to lock automatically after 5 minutes of inactivity, user unable to modify (Control A.9.3.2)
Consequence(s)	Users may find terminal locks out while they are still at desk. Other individuals have reduced window in which to access the unlocked terminal
Impact	The impact of the compensating control is assessed as Positive. The complexity cost is low The financial cost to implement is low (under $5,000) The financial cost to maintain is low (under $5,000 p.a)

Step Eight: Analysis Documentation

The final step is documenting the results of the analysis and preparing a report for the ISMS management committee. The Report should include the Inventory of Assets, threats, vulnerabilities, the problems detected and possible solutions. It will need to comment on the risk of not implementing a solution, and those solutions that may not be feasible either due to cost or impact on other parts of ACME Parcels.

The FMECA Report to the ISMS Committee will provide:

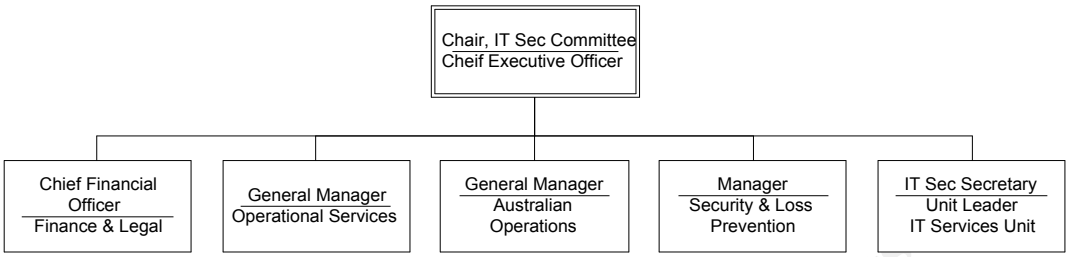
- Identified the system and its constituent parts (RCU assets)
- The relationship between RCU assets and other areas as well as RCU local asset relationships
- Sources of failure - either within the asset itself or as a result of the interface between it and other areas
- The likelihood of failure (either as the result of a threat or vulnerability)
- The severity of the failure and the consequence of the failure
- A prioritised list of risks to be examined
- An assessment of existing controls that are in place to manage or mitigate the identified risks
- Additional controls that can be put in place to manage or mitigate risk, the consequence (including likely cost) of the additional control
- Recommended controls to be implemented

The ISMS Management Structure

The ISMS structure for the system will consist of the overall (ACME Parcels) security policy continuing to be governed by the existing Security Committee. The RCU shall be represented on this committee by the Chief Financial Officer. However the ITSU Team Leader will join the committee in the role of ISO and act as secretary. This group will form the permanent Information System Security Steering Committee. The reasons for this are to utilise the existing Security Committee and ensure that for information security "*A management forum to ensure that there is clear direction and visible management support for security initiatives shall be in place. The management forum shall promote security through appropriate commitment and adequate resourcing*"[11].

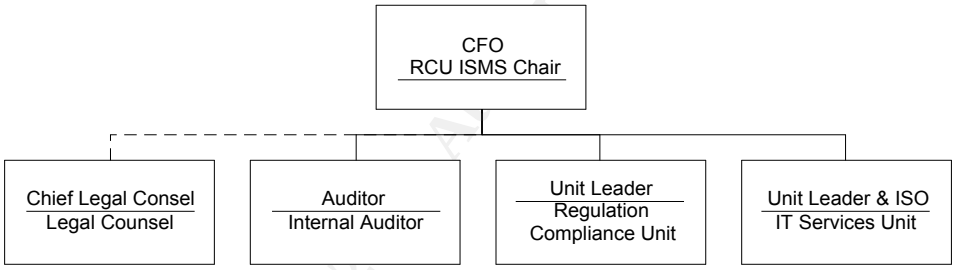
[11] ASNZ 7799:2:2003 *Information Security Management – Part 2: Specification for information management systems;* Second Edition*,* Standards Australia; Sydney Australia; 2001; p.16

Having the ITSU Manager on the committee also ensures that IT staff (all within the ITSU) will have buy-in through their manager as well as provide a level of technical expertise that was previously missing from the committee.



Revised ACME Parcels Security Committee

However, this committee does not have sufficient knowledge of the RCU processes, nor would they have the time to be sufficiently involved with the development of the ISMS. Therefore a smaller, security team consisting of the CFO as chair, the ITSU Manager (in the ISO role), the RCU Team Leader and Auditor will be established to ensure that RCU business objectives, security principles and risk management strategy are defined. Chief Legal Counsel will be a member of the committee, but will be involved primarily as a subject matter expert on matters of law.



RCU ISMS Security Committee

This committee structure benefits from having a senior manager, who reports directly to the CEO, involved. It has process owners (the Manager of the RCU and ITSU) and the Auditor, who as well as having a good understanding of the RCU processes, can bring sound risk management practices to the committee. The Chief Legal Counsel will be involved as required to ensure all the legal business risks are covered, but without bogging the committee down with large amounts of legalese.

Policies Identified for Development and Implementation

Having identified those assets (systems) most at risk and prioritised them, the RCU project will be required to undertake development and implementation of policies to address them.

The rationale for this is to ensure that controls that are already in place, or proposed to be put into place cannot be enforced unless there is a documented policy or procedure behind it.

For the RCU, the ISMS should address the following areas:

- Personnel Security Policy
- User Access Policy
- Incident Management Policy
- Physical Security Policy
- Data Classification Policy
- Electronic Mail Security Policy
- Legal Compliance Policy

RCU Policy:	Personnel Security Policy
Purpose:	Control objective: To reduce the risks of human error, theft, fraud or misuse of facilities. This policy should cover who is responsible for security and what that role entails. For the RCU this policy should include security responsibilities for each individual and for Human Resources, cover what needs to be in job descriptions, terms and conditions of employment, verification checks (Police checks) to be conducted and any formal disciplinary measures. User training and security incident responses would also be detailed at a high level.
Audience:	RCU Personnel ACME Parcels, Human Resources
AS/NZ 7799.2	A.6.1 Security in job definition and resourcing

RCU Policy:	User Access Policy
Purpose:	Control objective: To control access to information, ensure access to systems are authorised, allocated and maintained and that users prevent unauthorised access through good security practices. This policy would define what RCU systems were for use by which personnel (defined by role / job description). Password management, the role of the RCU Manager in reviewing access rights and user responsibilities for logging in, out and locking screens would be covered.
Audience:	RCU Personnel ITSU Personnel
AS/NZ 7799.2:	A.9.1 Business requirement for access control A.9.2 User access management A.9.3 User responsibilities

RCU Policy:	Incident Management Policy
Purpose:	Control objective: To ensure the correct and secure operation of information processing facilities. This policy would cover the requirements for documenting operating procedures, how change to systems was to occur, incident management responsibilities and procedures and the use of logs in collecting data. At a high level it should provide guidance on what information needs to be logged (to enable collection of incident data). Segregation of responsibilities, particularly for some ITSU personnel would be covered.
Audience:	RCU Personnel ITSU Personnel
AS/NZ 7799.2:	A.8.1 Operational procedures and responsibilities

RCU Policy:	Physical Security Policy
Purpose:	Control objective: To prevent unauthorized physical access, damage and interference to business premises and information. This policy would identify the controls to be taken to be taken to physically secure the RCU and its systems. The principle of “defence in depth” would be applied so that there was more than one barrier between non-authorised and authorised personnel. Perimeter and entry controls to the RCU would be covered. Policy for working in the ACME Parcel Server Room would also be included.
Audience:	RCU Personnel ACME Headquarter personnel, including visitors
AS/NZ 7799.2:	A.7.1 Secure areas

RCU Policy:	Data Classification Policy
Purpose:	Control objective: To ensure that information assets receive an appropriate level of protection as well as prevent damage to assets and interruptions to business activities. Policies for classifying, labelling, handling, storing and disposal of RCU data (in all media formats) would be covered.
Audience:	RCU Personnel ITSU Personnel
AS/NZ 7799.2:	A.5.2 Information classification A.8.6 Media handling and security A.8.7.4 Security of electronic mail

RCU Policy:	Electronic Mail Security Policy
Purpose:	Control objective: To prevent loss, modification or misuse of information exchanged between organisations as well as protect the confidentiality, authenticity or integrity of information. This policy would be to ensure that RCU personnel protected any classified data to be emailed before it is sent. This would cover cryptographic controls to be followed for encrypt / decrypt of classified data.
Audience:	RCU Personnel
AS/NZ 7799.2:	A.8.7.4 Security of electronic mail A.10.3 Cryptographic controls

RCU Policy:	Legal Compliance Policy
Purpose:	Control objective: To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements. The policy would detail explicitly, the statutory and regulatory requirements that the RCU is required to fulfil. The frequency of how often a review of legislation and regulations is to be conducted would be included. Safeguarding of evidentiary material, warrant s and other important RCU records along with the controls to ensure personal privacy is not breached would also be covered.
Audience:	RCU Personnel Chief Legal Council
AS/NZ 7799.2:	A.12.1 Compliance with legal requirements

The Process to Identify Risks to the System

The methodology employed to identify the risks to the RCU system will be the FMECA model, as previously described. Looking at the broad categories within the RCU Asset Inventory and the interfaces previously detailed in FMECA Step One, a number of risks can be identified.

Following the FMECA process, once risks are identified (source, likelihood, severity) a plan to control the risk (Step Six) can be developed. Under Step 4, the risks have already been prioritised based on assessed likelihood and severity. The table overleaf provides a sample of some of the main risks (one for each of the asset categories) identified and details:

- The nature of the threat
- The specific vulnerability
- The Likelihood of its occurrence
- The Severity of impact of the occurrence
- The Risk level (Priority for Treatment)
- A description of the control(s) selected (against ASNZ 7799)
- The reason for selecting the control; and
- The residual risk level after implementing the control

It should be noted that this table does not contain all risks identified within the RCU, for example, other risks to physical assets include:

- Theft of RCU workstations
- Damage to RCU workstations
- Damage to the PASH / IMS Server

For these, the same process as outlined in the table would be undertaken.

Risk Identification Table

Asset	Threat	Existing Vulnerabilit(ies)	Likelihood	Severity	Risk Level & Priority for treatment	Controls Selected (ASNZ 7799)	Rationale for Control	Residual Risk & ot consequences c controls
Physical	PASH or IMS Server failure	• Equipment located in office environment, not dedicated data centre • No backup power at ACME Parcel Headquarters • Under powered UPS • Poor air cooling system in Server Room	Occasional (C)	Critical (II)	High Risk (Priority 3)	A.7.1.1 A.7.2.1, A.7.2.2, A.7.2.4 A.8.1.3 A.8.2.1, A.8.2.2 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5	The controls selected are to ensure that the vulnerabilities identified in the current server environment at ACME Parcel Headquarters can be mitigated to ensure there is not a loss of these systems availability for the RCU.	If all the controls identifie and implemented, the likelihood is reduced. Th residual risk is recalcula Medium Risk. Consequences of these controls would be the co implement and maintain them.
Information	Law Enforcement Agency operations data compromised (loss of confidentiality)	• RCU Environment open plan • No controls on safe • Workstations unlocked • Material left on desks during breaks, lunch, etc	Remote (D)	Catastrophic (I)	High Risk (Priority 3)	A.5.2.1, A.5.2.2 A.6.1.1, A.6.1.2, A.6.1.3, A.6.1.4 A.6.2.1 A.6.3.1, A.6.3.2 A.6.3.3, A.6.3.4 A.7.1.3, A.7.1.4 A.7.2.6 A.7.3.1 A.8.7.1, A.8.7.5 A.8.7.7 A.9.3.1 A.9.5.7, A.9.5.8 A.9.7.2	The controls selected are to ensure that information relating to law enforcement operations is classified appropriately and treated separate from ACME Parcel business information; that RCU staff are aware of their responsibilities and the risk of error or misuse is reduced. The controls will also establish controls for working in the RCU as well as the procedures to be followed for information exchange.	If all the controls identifie and implemented, the likelihood and the impac (severity) is reduced. Th residual risk is recalcula as a Medium Risk. Consequences of these controls would be the co implement and maintain them; more formal proce for some activities and a greater degree of loggin auditing of system and u activity.
Software	Malicious software downloaded or installed onto RCU workstations	• Controls on workstations • RCU users are local administrators	Remote (D)	Critical (II)	Medium Risk (Priority 4)	A.8.3.1 A.8.4.1 A.8.5.1 A.9.2.2 A.9.5.5	The controls selected are to ensure that the RCU systems are protected from software that may impact on the integrity of the RCU systems; prevent possible loss of information, compromise of information or loss of productivity.	If all the controls identifie and implemented, the likelihood is reduced. Th residual risk is recalcula still as a Medium Risk. Consequences of these controls would be the co implement and maintain

Asset	Threat	Existing Vulnerabilit(ies)	Likelihood	Severity	Risk Level & Priority for treatment	Controls Selected (ASNZ 7799)	Rationale for Control	Residual Risk & ot consequences c controls
								implement and maintain them; user training and greater involvement of I personnel in RCU syste
Personnel	RCU Personnel make an inappropriate disclosure to a Law Enforcement Agency	• Poor controls on dispatch of information • Changes in law not circulated	Occasional (C)	Catastrophic (I)	High Risk (Priority 2)	A.4.1.6 A.6.2.1 A.7.3.1 A.8.6.2, A.8.6.3 A.8.7.2, A.8.7.4 A.12.1.1, A.12.1.3 A.12.1.4	The controls selected are to ensure that the likelihood of inappropriate disclosure is made as unlikely as can be managed. Controls on the infrastructure, environment, media handling are introduced as are processes to ensure RCU personnel are regularly trained on pertinent legislation and regulations.	If all the controls identifie and implemented, the likelihood is reduced. Th residual risk is recalcula as Medium Risk. Consequences of these controls would be the co implement and maintain them.
Network / Telco links	Loss of WAN connection between RCU and Australian Data centre	• Single data link • No redundant or standby link in place • Under powered UPS	Remote (D)	Marginal (III)	Low Risk (Priority 6)	A.6.3.4 A.7.2.4 A.8.2.1 A.11.1.1, A.11.1.2 A.11.1.3, A.11.1.4 A.11.1.5	The controls selected are to ensure that the RCU has a business continuity plan in place to deal with the impact of a network outage.	If all the controls identifie and implemented, the likelihood and the impac (severity) is reduced. Th residual risk is recalcula Very Low Risk. Consequences of these controls would be the requirement for cost to implement and maintain a training liability to ensu RCU and ITSU staff resp correctly.

Part Three: Do

'*The Do activity within the PDCA cycle is designed to implement selected controls and promote the action necessary to manage the information security risks in line with the decisions that have been taken in the Plan phase'*.[12]

In Part Two several policies were identified for development and implementation. They are presented as the problem (the threat or vulnerability), the action to be undertaken to remediate the problem, which part of 7799 this action addresses and the steps that it would be necessary to undertake to implement the action plan.

Problem:	There is no reference to security in any RCU job definitions, which presents a risk to information assets
Action:	This problem should be addressed by having the security responsibilities for each role within the RCU defined
7799 Criteria:	A.6.1 Security in job definition and resourcing.
Steps Taken:	1. Define & develop security responsibilities for each role in the RCU 2. Issue new responsibilities to Human Resources for inclusion in existing work agreements and as part of the terms and conditions for any new RCU staff 3. Establish verification procedures for Human Resources to follow for any hiring of new RCU staff 4. Educate RCU staff on new requirements in employment terms and conditions 5. RCU staff to sign confidentiality agreements & acceptance of the security responsibilities

Problem:	Access controls to information within the RCU are not well developed, which presents a risk to information assets
Action:	This problem should be addressed through establishing procedures or guidelines for RCU staff to following when accessing sensitive information, either electronically, or from other sources (such as the fax or from the safe)
7799 Criteria:	A.9.1 Business requirement for access control A.9.2 User access management A.9.3 User responsibilities
Steps Taken:	1. Define and document the controls required a. Registration & Deregistration controls b. Technical access controls c. Staff procedures to be followed 2. Establish technical controls for RCU systems a. Login & logout times b. Passwords c. Screen (terminal) lockouts d. Fax & printer controls 3. Educate ITSU staff on access controls applicable for the RCU 4. Educate RCU staff on access control policy and procedures

[12] ibid, p.45

Problem:	The RCU has no established procedures for dealing with system outages or security incidents
Action:	This problem should be addressed through establishing incident management procedures or guidelines to 'ensure a quick, efficient and orderly response'[13] to events that disrupt the functioning of the RCU
7799 Criteria:	A.8.1.3 Incident Management Procedures
Steps Taken:	1. Define and document the RCU policy for managing incidents 2. Develop incident procedures for the RCU a. Workshop draft procedures with RCU and other stakeholders such as ITSU and ACME Parcels personnel 3. Educate RCU staff on the incident procedures 4. Conduct training and rehearsals of the documented procedures

Problem:	The physical environment in which the RCU operates is not separated from the rest of the ACME staff on the second floor
Action:	To remedy this, the RCU can either relocate, have the other staff relocate, have physical barriers between themselves and the rest of the floor installed, have the other staff on the floor follow the same security requirements as the RCU and / or implement additional controls for the RCU staff
7799 Criteria:	A.7.1 Secure areas
Steps Taken:	1. Review feasibility of relocating the RCU staff to another part of the building where a secure facility can be located 2. Review feasibility of partitioning the RCU from the remainder of personnel located on the floor 3. Review and establish procedures for RCU staff to follow while operating with sensitive data 4. Present findings to ISMS Management for decision on relocation / rebuilding

Problem:	Data (information) handled within the RCU is does not currently have any documented controls on how sensitive information should identified or be handled differently to other types of data
Action:	Ensure RCU staff are educated in that identification and handling data that requires classification. Also ensure procedures for checking classification handling is occurring properly are in place
7799 Criteria:	A.5.2 Information classification A.8.6 Media handling and security A.8.7.4 Security of electronic mail
Steps Taken:	1. Establish classification criteria for RCU information relating to law enforcement investigations 2. Establish protocols for the handling of classified information 3. Establish protocols for the dispatch of classified information via email 4. Establish technical controls (with ITSU) for ensuring classified information are accessible only to those personnel who require it. This may require clearance from the ISMS Management Committee. 5. Educate RCU staff

[13] ibid, p.20

Problem:	Any email that the RCU dispatch to Law Enforcement / Custom agencies containing sensitive (classified) information must be secured appropriately using the PGP software provided, otherwise there is a risk of unauthorised disclosure of information
Action:	Establish controls for use of the PGP software and monitoring of outbound emails from the RCU
7799 Criteria:	A.8.7.4 Security of electronic mail A.10.3 Cryptographic controls
Steps Taken:	1. Define and document the RCU policy and procedures for use of the encryption software 2. Establish technical controls (with ITSU) a. Logging and auditing of encrypted emails 3. Training of ITSU & RCU staff on use of encryption software 4. Develop training package for Law Enforcement Agencies (who may request the material in electronic format in the future)

Problem:	There is a risk that RCU staff Legal Compliance Policy
Action:	Processes to ensure RCU personnel are regularly trained on pertinent legislation and regulations need to be introduced
7799 Criteria:	A.12.1 Compliance with legal requirements
Steps Taken:	1. Define and document the RCU procedures for undertaking disclosure of information to law enforcement and custom agencies 2. Establish liaison with Legal Consul a. Register of relevant legislation (per country) b. Procedures for updating the legislation register 3. Training of RCU staff on regulatory / statutory changes

Statement of Applicability

The statement of applicability is a "*document describing the control objectives and controls that are relevant and applicable to the organisation's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes.*"[14]

Three examples of a Statement of Applicability for the RCU ISMS are provided below, two of which are applicable and one that is not.

Part 9: ACCESS CONTROL			
A.9.5: Operating System Access Control			
Control objective: To prevent unauthorised computer access			
Controls		**Applicable?**	**ASNZS 7799:2001**
Terminal Time-out	Inactive terminals in the RCU shall shut down after a defined period of inactivity to prevent access by unauthorised persons.	YES	9.5.7
Rationale	This control ensures that in the event a RCU staff member leaves their computer terminal without logging off, or locking it, that the system will automatically lock and then shut down the terminal to prevent other, possibly unauthorised individuals accessing the RCU systems.		

[14] ibid, p.15

Part 12: COMPLIANCE			
A.12.1 Compliance with Legal Requirements			
Control objective: To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.			
Controls		**Applicable?**	**ASNZS 7799:2001**
Identification of applicable legislation	All relevant statutory, regulatory and contractual requirements shall be defined explicitly and documented for each information system.	YES	12.1.1
Rationale	This control is crucial to the operation of the RCU. RCU personnel are required to ensure ACME Parcels comply with the statutory requirements of various countries, each with their own statutes and legal system. There are significant trans-national issues that require close coordination. As an Australian company, the RCU is also responsible for ensuring that in comply with one nation's laws, it is not in breach of Australian or a third country's laws.		

An example of a Statement of Applicability for the RCU ISMS for control that is not applicable is as follows:

Part 8: COMMUNICATIONS AND OPERATIONS MANAGEMENT			
A.8.7 Exchanges of information and software			
Control objective: To prevent loss, modification or misuse of information exchanged between organisations.			
Controls		**Applicable?**	**ASNZS 7799:2001**
Electronic Commerce Security	Electronic commerce shall be protected against fraudulent activity, contract dispute and disclosure or modification of information.	NO	8.7.3
Rationale	This control is not applicable to the RCU as it has no electronic commerce systems.		

Part Four: Check

'*The Check activity is designed to ensure that the controls are working effectively and as intended, and that the ISMS remains effective*'[15]. With the project having completed the 'Do', the RCU ISMS now requires a checklist to be developed against which the selected system controls detailed earlier can be audited.

The table below provides a non exhaustive example of the audit controls expected to be put in place at the RCU.

RCU Audit Controls

ASNZS 7799:2001	Control Objective	Rationale	Audit Conduct
A.4.2.2	Security requirements in third-party contracts	Arrangements involving third-party access to the RCU shall be based on a formal contract containing all necessary security requirements	1. Obtain details of all third-party contracts that relate either directly to the RCU or ACME Parcels (such as the cleaning contract for the second floor or IT services through the ITSU 2. Verify that security requirements are part of each contract
A.5.2.1	Classification guidelines	Classifications and associated protective controls for information shall take account of business needs for sharing or restricting information, and the business impacts associated with such needs	1. Confirm existence of classification guideline & procedures document 2. Interview RCU staff to verify they are aware of the documents and how to follow them 3. Check a sample (10%) of classified documents to verify that meet the documented guidelines 4. Search RCU directories (using a tool such as NGrep) on the computer system to see if any sensitive information is locatable on a non-classified part of the network
A.6.1.2	Personnel screening and policy	Verification checks on permanent staff, contractors, and temporary staff to the RCU shall be carried out at the time of job applications	1. Confirm existence of RCU Employment Policy 2. Confirm existence of procedures for screening staff with Human Resources and these are in alignment with the Policy 3. Verify that procedures have been undertaken such as evidence of Police checks
A.6.1.4	Terms and conditions of employment	The terms and conditions of employment shall state the employee's responsibility for information security	1. Confirm existence of RCU Employment Policy 2. Confirm existence of procedures for screening staff with Human Resources and these are in alignment with the Policy 3. Verify that RCU staff have acknowledged acceptance of the terms and conditions of their employment 4. Interview RCU staff to verify they are aware of their responsibility for information security
A.6.3.2	Reporting of security weaknesses	Users of information services in the RCU shall be required to note and report any observed or suspected security weaknesses in, or threats to, systems or services	1. Verify incidents are registered in an incident log 2. Check log for reports made 3. Interview RCU staff to determine if they are aware of the log and if any reports have not been made
A.7.3.1	Clear desk and clear screen policy	The RCU shall have a clear desk and a clear screen policy to reduce the risks of unauthorized access, loss of,	1. Conduct walk through of the RCU without notice and verify that terminals are locked and there is no sensitive material on desks at:

[15] ibid, p.42

ASNZS 7799:2001	Control Objective	Rationale	Audit Conduct
		and damage to information	a. Lunch time b. After hours 2. Interview RCU staff to verify they are aware of what is required under the clear screen policy
A.8.6.3	Information handling procedures	Procedures for the handling and storage of information shall be established in order to protect such information from unauthorized disclosure or misuse	1. Confirm existence of procedures document 2. Interview RCU staff to verify they are aware of the procedures and that they are followed correctly
A.8.7.4	Security of electronic mail	Electronic mail shall be controlled to reduce security risks created by electronic mail, particularly the dispatch of any sensitive information	1. Access outbound email logs of RCU staff 2. Review details of emails sent to Law Enforcement agencies 3. Check a sample (20%) to confirm if sensitive material was encrypted
A.9.3.1	Password use	Users shall be required to follow good security practices in the selection and use of passwords	1. Confirm existence of Password policy and procedures documents 2. Check ITSU have established technical controls as per documented controls 3. Check RCU that no passwords are written down in: a. On or near the computer b. In desk drawers
A.9.5.7	Terminal time-out	Inactive terminals serving high risk systems shall shut down after a defined period of inactivity to prevent access by unauthorized persons	1. Confirm existence of policy and procedure documents 2. Check ITSU have established technical controls as per documented controls

Audit Timings

The timing of these audits should occur with sufficient frequency so that weaknesses in the existing controls do not remain undetected for a period of time that is greater than the likelihood of a risk occurring. Too regular auditing however may be an inefficient use of resources and interfere with normal operations. The following table details the proposed timings for the audit of controls previously listed.

Timings

ASNZS 7799:2001	Control Objective	Timing
A.4.2.2	Security requirements in third-party contracts	Annual
A.5.2.1	Classification guidelines	Bi annual
A.6.1.2	Personnel screening and policy	Annual
A.6.1.4	Terms and conditions of employment	Annual
A.6.3.2	Reporting of security weaknesses	Bi annual
A.7.3.1	Clear desk and clear screen policy	Monthly
A.8.6.3	Information handling procedures	Annual
A.8.7.4	Security of electronic mail	Monthly
A.9.3.1	Password use	Bi Annual
A.9.5.7	Terminal time-out	Bi Annual

Audit Benefits

The benefits of having an audit and checklist is that it will assist the RCU in improving its system security. It achieves this by providing a foundation on which the performance of their ISMS can be evaluated. Each time the audit is conducted it will identify new vulnerabilities that existing controls do not cover, or existing vulnerabilities where existing controls are not working.

It will generate information that can be quantified and used to support trend analysis so that systems (for example) that consistently have issues can be identified and addressed. It also ensures that the security of the RCU will keep pace with changes in the way both ACME Parcels conducts business, as well as changes in technology.

Regular audits, conducted properly, will also improve the awareness of RCU personnel to security issues. This in turn will make the RCU more self policing, where issues are identified prior to the audit proactively resolved.

Part Five: Act

Finally, an important part of implementing the ISMS is to ensure continual improvement – *'The organisation shall continually improve the effectiveness of the ISMS through the use of the information security policy, security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review'*.[16]

Following the initial implementation of the ISMS and conduct of the first audit, a number of issues with controls may be identified. How will the ISMS be maintained and improved?

Maintenance and Improvement

The FMECA model permits further analysis of the system. While the initial project has focussed on the RCU as a system, a study of lower "indenture" levels could be undertaken. This could involve, for example, assessing the processing of information between various groups (or individuals) within the RCU or analysing technical components in more detail.

The Block Diagrams initially developed do not identify all external influences that may impact on the RCU. One example was a legislative change that was subsequently identified. In Australia the Privacy Act was extended to encompass the private sector in Dec 2001. One area that required immediate assessment and evaluation was that information relating to National Privacy Principle 9 – "*An organisation can only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection*".[17] As an interface into the RCU, a failure in this system

[16] ibid, p.25
[17] The Privacy Act 1998 and The Privacy Amendment (Private Sector) Act 2000; both Commonwealth of Australia.

could result in prosecution of ACME Parcels. While it was not included in the initial high level Block Diagram, a process that saw the ISMS Committee review the last FMECA would ensure other changes would be identified.

Maintenance of the ISMS will be conducted by ongoing data collection and statistical analysis to enable the RCU to move to a more quantitative analysis of risk. Critical to the success in maintaining the ISMS is to ensure it remains relevant and it is adhered to by the RCU staff. Ongoing management commitment, the training and education of staff, together with regular reporting of incidents (either actual or potential) will ensure this occurs.

Improvements to the ISMS will be managed through the RCU ISMS Committee. For issues that may require changes to other areas of ACME Parcels, the Committee will refer the requests onto the ACME Parcels Security Committee.

Internal and External Audits

For the RCU, there is a possibility that an external party (such as a Law Enforcement Agency) may wish to confirm that there is sufficient security in place. As such an audit may occur with little notice, internal auditing should occur at the frequency detailed in the previous section.

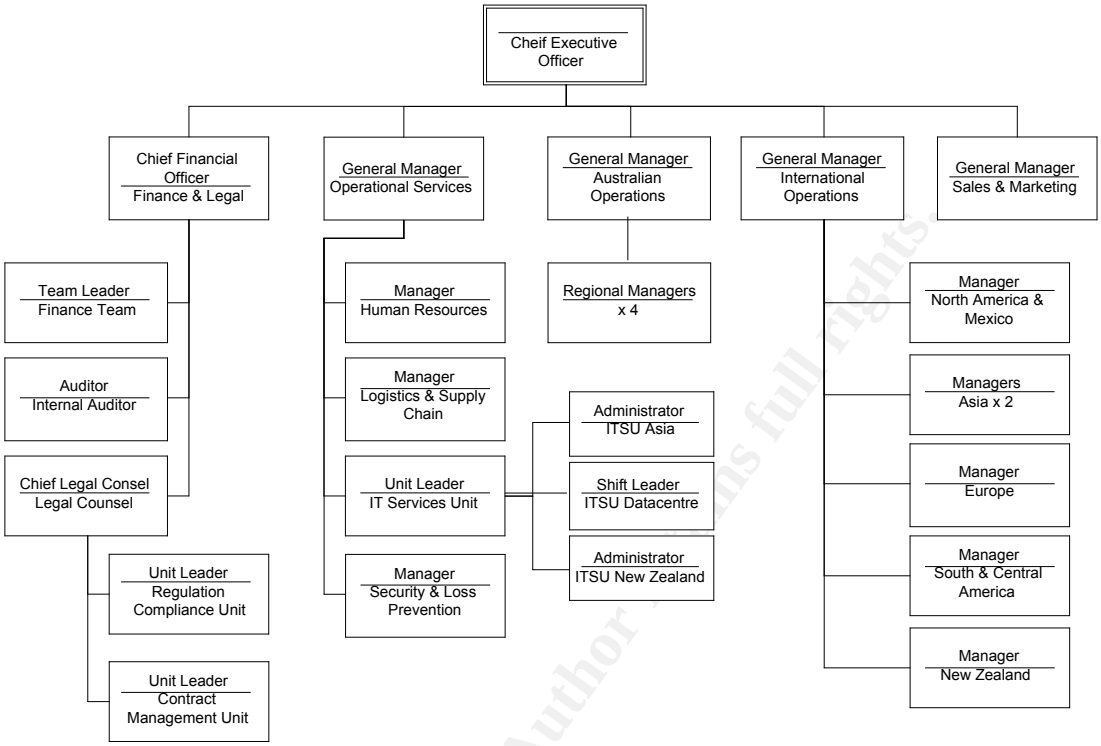
The ACME Parcels Auditor should also be involved to ensure the results of all audits are properly documented and recorded.

The RCU ISMS Committee should accept an external audit to be conducted every second year and it is desirable that this is undertaken in conjunction with any audit ACME Parcels Security Committee wish to conduct. This ensures that the audit covers areas that interact with the RCU (i.e. the ITSU) but which may have not been as comprehensively audited if it was only the RCU being audited. For technical controls (such as those undertaken by the ITSU) the use of an external auditor is often invaluable in identifying weaknesses in technological controls.

Conclusion

In conclusion, the implementation of an ISMS within the RCU ensures that the significant risks (legal, financial and reputational) associated with the compromise of RCU security are mitigated and controlled. Other parts of ACME Parcels will be able to commence their own implementation. With the successful implementation of ISMS, ACME Parcels strategy of growing international distribution in under-represented countries in Asia, Europe and South America can continue.

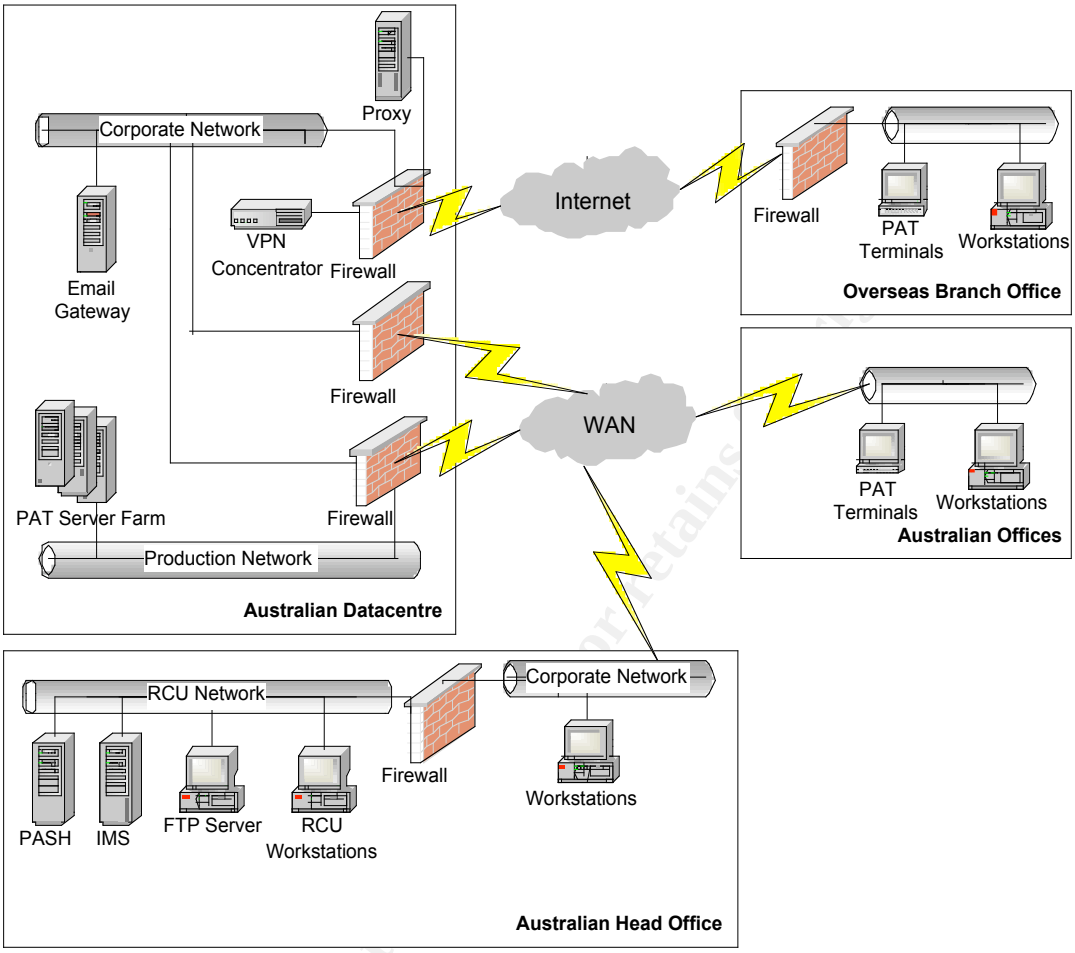
APPENDIX A: ACME PARCELS ORGANISATION CHART



ACME PARCELS

Organisation Chart

APPENDIX B: ACME PARCELS SYSTEM DIAGRAM



BIBLIOGRAPHY

Standards Australia; ASNZ 17799:2001 Information Technology – Code of practice for information Security Management; Sydney Australia; 2001

Standards Australia; ASNZ 4360:1999 Risk Management; Sydney Australia; 1999

Standards Australia; ASNZ 7799:2:2003 Information Security Management – Part 2: Specification for information management systems; Second Edition; Sydney Australia; 2001

IBISWorld Pty Ltd; Communication Services in Australia,; Australia; 2004 <http://www.ibisworld.com.au/> (subscriber access only)

Office of Government Commerce; Managing Successful Projects with PRINCE 2; Norwich, United Kingdom; 2001

USA Department of Defence; MIL-STD 1629A, Military Standard Procedures for Performing a Failure Mode, Effects and Criticality Analysis; Washington, USA; 1980 <http://jcs.mil/htdocs/teinfo/software/ms18.html>

Commonwealth of Australia; The Privacy Act 1998; Canberra, Australia; 1998 <http://www.privacy.gov.au/act/privacyact/index.html>

Commonwealth of Australia; The Privacy Amendment (Private Sector) Act 2000; Canberra, Australia; 2000 <http://www.privacy.gov.au/act/privacyact/index.html>