CHAPTER 9

Implementation (Delivery) Options

LEARNING OUTCOMES

By the end of this chapter, you should be able to:

1. Define the meaning of security technology;
2. Identify the tool and it usage for security;
3. Explain the assurance and trust in relation to confidence mechanism;
4. Identify the usage WRMS in protecting information; and
5. Identify the step to overcome the compliance issue.

INTRODUCTION

Before we begin, let us observe the video below.

Source: http://www.youtube.com/watch?v=oYniDSGzvTE

Based from the video above, can you identify the points highlighted by IBM Express Advantage. State your opinion on the higlighted points and share your thoughts on the matter.

For the past few years, IT and security professionals have talked about information technology and particularly information security as a "business enabler." Today, it might also be called a "compliance enabler." IT and security organisations have both been on the front lines for compliance efforts and are now being asked to play two pivotal roles in implementation:

- First is to provide a secure, well-controlled IT environment to improve business performance; and
- Second, to assist the organisation in strategically and tactically addressing its governance, risk and compliance requirements.

9.1 SECURITY TECHNOLOGY AND TOOLS

With the rapid growth of interest in the Internet, computer security has become a major concern to companies throughout the world. The fact that the information and tools needed to penetrate the security of corporate networks are widely available has increased that concern.

Because of this increased focus on computer security, administrators often spend more effort protecting their networks than on actual network setup and administration. Tools that probe for system vulnerabilities, such as the Security Administrator Tool for Analysing Networks (SATAN), and some of the newly available scanning and intrusion detection packages and appliances, assist in these efforts, but these tools only point out areas of weakness and may not provide a means to protect networks from all possible attacks. Thus, as an administrator, you must constantly try to keep abreast of the large number of security issues confronting you in today's world. Some of the security technology issues that should be taken into consideration are:

Ensuring the security of the network: Due to the network security is critical issue; the infrastructure should be diligently and continuously protected. Alert for software vulnerabilities is should be constantly monitored and software patches is applied promptly.

Anti-virus protection: Network security is monitored for viruses and both proactive and reactive is taken, measures to prevent, detect and eliminate them.

Providing a secure environment for users' communications: Communications should take place within a controlled environment, and are facilitated over highly secure data transit network.

Preventing denial of service attacks or other intrusions: Integrating denial of service mitigation protection at all levels of network system, which can helps administrator to protect against attempted attacks. If the administrator aware of potential vulnerabilities to their systems, they can quickly address these issues and prevent any disruptions to network service.

Safeguarding access users data: Administrator should commit to the security and privacy of our users' personal data. A privacy protection control system is designed to ensure the security. Passwords should be strictly confidential. Numerous safeguards should be implemented in order to allow access to user data. We understand that a sound security system is the result of not only tools such as firewalls, intrusion detection systems, and anti-virus software, but that the internal employees play an integral role in protecting security. To this end, security access to user data is granted on a need-to-know basis and employees are extensively screened prior to being granting access privileges. Periodic internal auditing of network records of data access

to detect and promptly address suspicious activity.

In order to implement the tools for securing your network, it is advisable to develop your security design. The design of the perimeter network and security policies requires the following subjects as shown in Figure 9.1 to be addressed.

Figure 9.1: The subjects required in the design of the perimeter network and security policies

From the diagram above, let's look into details each of the subjects.

1. Know Your Enemy

Knowing your enemy means knowing attackers or intruders. Consider who might want to circumvent your security measures, and identify their motivations. Determine what they might want to do and the damage that they could cause to your network. Security measures can never make it impossible for a user to perform unauthorised tasks with a computer system; they can only make it harder. The goal is to make sure that the network security controls are beyond the attacker's ability or motivation.

2. Count the Cost

Security measures usually reduce convenience, especially for sophisticated users. Security can delay work and can create expensive administrative and educational overhead. Security can use significant computing resources and require dedicated hardware. When you design your security measures, understand their costs and weigh those costs against the potential benefits. To do that, you must understand the costs of the measures themselves and the costs and likelihood of security breaches. If you incur security costs out of proportion to the actual dangers, you have done yourself a disservice.

3. Identify Any Assumptions

Every security system has underlying assumptions. For example, you might assume that your network is not tapped, that attackers know less than you do, that they are using standard software, or that a locked room is safe. Be sure to examine and justify your assumptions. Any hidden assumption is a potential security hole.

4. Control Your Secrets

Most security is based on secrets. Passwords and encryption keys, for example, are secrets. Too often, though, the secrets are not all that secret. The most important part of keeping secrets is in knowing the areas that you need to protect. What knowledge would enable someone to circumvent your system? You should guard that knowledge and assume that everything else is known to your adversaries. The more secrets you have, the harder it will be to keep them all. Security systems should be designed so that only a limited number of secrets need to be kept.

5. Human Factors

Many security procedures fail because their designers do not consider how users will react to them. For example, because they can be difficult to remember, automatically generated nonsense passwords often are written on the undersides of keyboards. For convenience, a secure door that leads to the system's only tape drive is sometimes propped open. For expediency, unauthorised modems are often connected to a network to avoid onerous dial-in security measures.

If your security measures interfere with essential use of the system, those measures will be resisted and perhaps circumvented. To get compliance, you must make sure that users can get their work done, and you must sell your security measures to users. Users must understand and accept the need for security. Any user can compromise system security, at least to some degree.

For instance, passwords can often be found simply by calling legitimate users on the telephone, claiming to be a system administrator, and asking for them. If your users understand security issues, and if they understand the reasons for your security measures, they are far less likely to make an intruder's life easier.

At a minimum, users should be taught never to release passwords or other secrets over unsecured telephone lines (especially cellular telephones) or e-mail. Users should be wary of people who call them on the telephone and ask questions. Some companies have implemented formalised network security training so that employees are not allowed access to the Internet until they have completed a formal training program.

6. Know Your Weaknesses

Every security system has vulnerabilities. You should understand your system's weak points and know how they could be exploited. You should also know the areas that present the greatest danger and should prevent access to them immediately. Understanding the weak points is the first step toward turning them into secure areas.

7. Limit the Scope of Access

You should create appropriate barriers in your system so that if intruders access one part of the system, they do not automatically have access to the rest of the system. The security of a system is only as good as the weakest security level of any single host in the system.

8. Understand Your Environment

Understanding how your system normally functions, knowing what is expected and what is unexpected, and being familiar with how devices are usually used will help you detect security problems. Noticing unusual events can help you catch intruders before they can damage the system. Auditing tools can help you detect those unusual events.

9. Limit Your Trust

You should know exactly which software you rely on, and your security system should not have to rely on the assumption that all software is bug-free.

10. Remember Physical Security

Physical access to a computer (or a router) usually gives a sufficiently sophisticated user total control over that computer. Physical access to a network link usually allows a person to tap that link, jam it, or inject traffic into it. It makes no sense to install

complicated software security measures when access to the hardware is not controlled.

11. Make Security Pervasive

Almost any change that you make in your system may have security effects. This is especially true when new services are created. Administrators, programmers, and users should consider the security implications of every change they make. Understanding the security implications of a change takes practice; it requires lateral thinking and a willingness to explore every way that a service could potentially be manipulated.

9.2 SECURITY TECHNOLOGY AND TOOLS

Trustworthy entity has sufficient credible evidence leading one to believe that the system will meet a set of requirements. **Trust** is a measure of trustworthiness relying on the evidence. To determine the trustworthiness, we focus on methodologies and metrics that allow us to measure the degree of confidence that we can place in the entity under consideration.

Assurance is confidence that an entity meets its security requirements based on evidence provided by applying assurance techniques.

Example of assurance techniques includes the use of a development methodology, formal methods for design analysis, and testing. Assurance is to indicate "how much" to trust a system and is achieved by ensuring that the need in Figure 9.2 is fulfill.

- The required functionality is present and correctly implemented.
- There is sufficient protection against unintentional errors.
- There is sufficient resistance to intentional penetration or by-pass.

Figure 9.2: Assurance needs

Security assurance is acquired by applying a variety of assurance techniques that provide justification and evidence that the mechanism, as implemented and operated, meets the security requirements described in the security policy for the mechanism. Security assurances focus on the correctness, consistency, completeness of the requirements and

implementations of those mechanisms. The security assurance process is as illustrated in Figure 9.3.

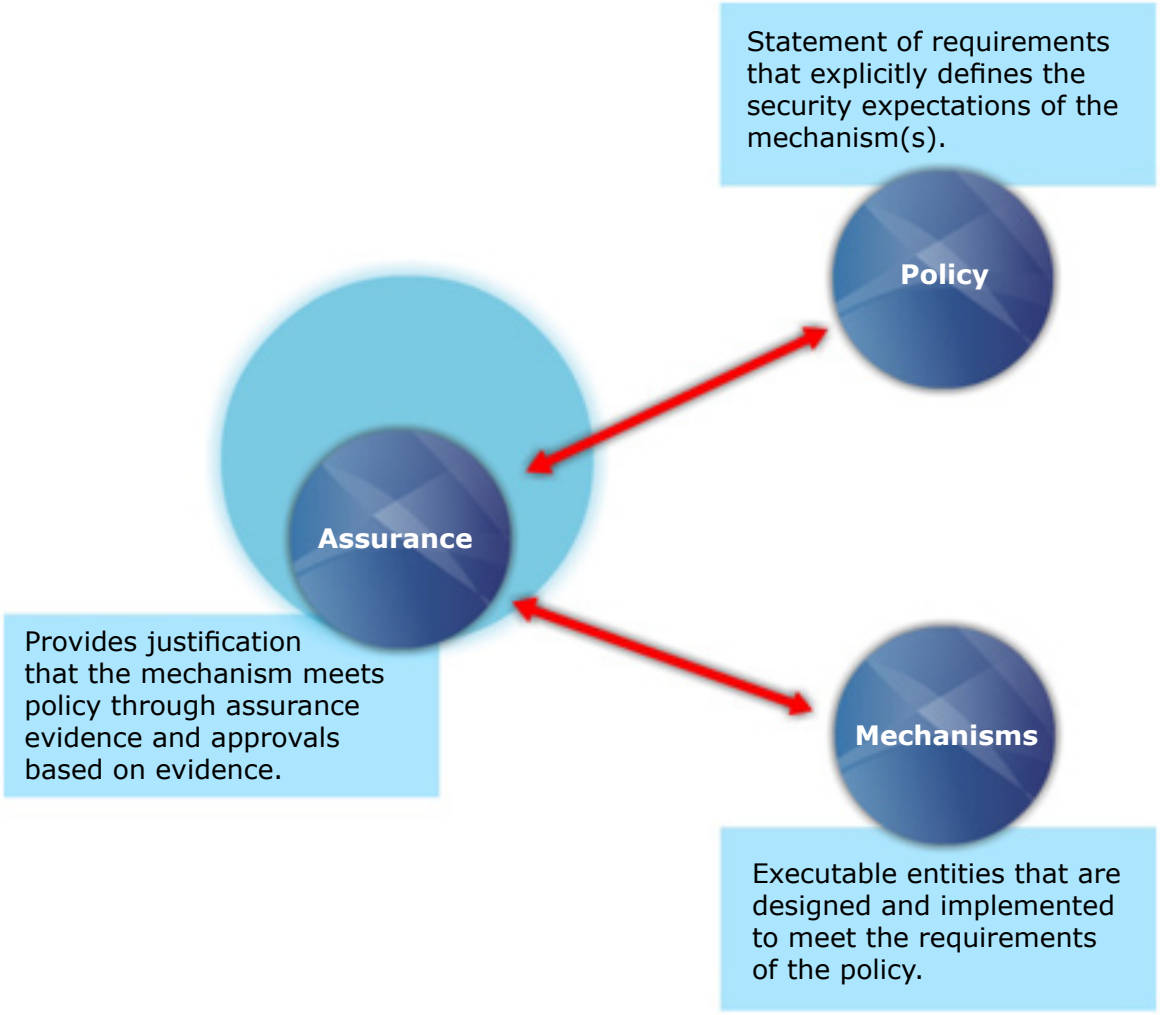

Figure 9.3: Relationships of assurance, policy and mechanisms

The basis for determining this aspect of trust should be done according to the Specification, Design and Implementation. Specific methodologies aggregate evidence of assurance and results are interpreted to assign levels of trustworthiness. Two standards that have been replaced by the Common Criteria are The Trusted Computer System Evaluation Criteria and the Information Technology Security Evaluation Criteria. These two standards provide increasing level of trust.

9.2.1 Source of Assurance Problems

Applying assurance techniques is time-consuming and expensive. Accidental or unintentional failures of computer systems, as well as intentional compromises of security mechanism can lead to security failures. There are nine types of problem sources in computer systems as shown in Figure 9.4.

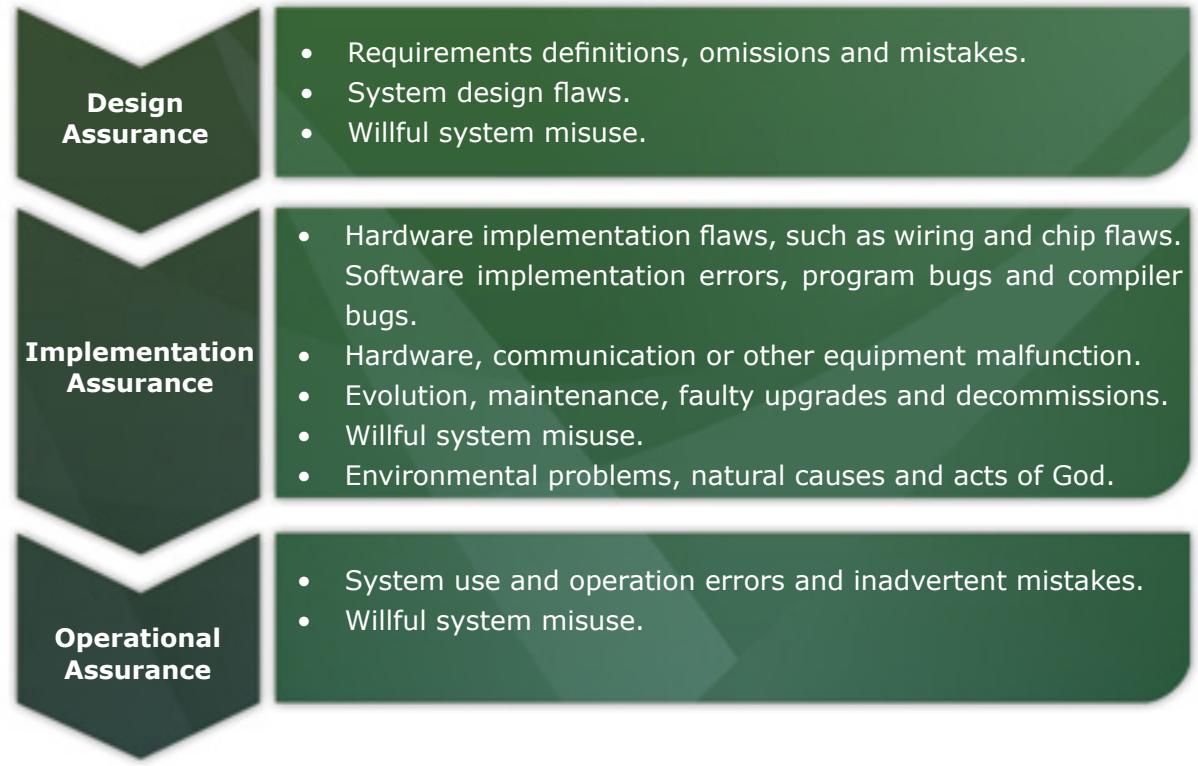

Figure 9.4: Assurance problem sources

This is not mainly deal with security problem, as it wills also addresses risks to safety, reliability and privacy. The examples of assurance risk as shown below (see Table 9.1).

Table 9.1: Examples of Assurance Risk

Assurance Risk	Details
Challenger explosion	It is due to sensors has been removed from booster rockets to meet accelerated launch schedule.
Deaths from faulty radiation therapy system	It is due to hardware safety interlock removed cause by flaws in software design.
Bell V22 Osprey crashes	Failure to correct for malfunctioning components; two faulty ones could outvote a third.
Intel 486 chip	Bug in trigonometric functions. Intel's public reputation was damaged, and replacing the chips cost Intel time and money. As a result, Intel using high-assurance methods to verify the correctness of requirements in their chip design.

9.2.2 Types of Assurance

The goal of assurance is to show that an implemented and operational system meets its security requirements throughout its life cycle. Due to the difference in the levels of abstraction between high-level security requirements and low-level implementation details, the demonstration is usually done in stages. Different assurance techniques apply to different stages of system development. Therefore, assurance is classified into policy assurance, design assurance, implementation assurance and operational assurance which as shown in Table 9.2.

Table 9.2: Assurance Type

Assurance Type	Description
Policy assurance	It is the evidence establishing security requirements in the policy is complete, consistent and technically sound.
Design assurance	It is the evidence establishing that a design is sufficient to meet requirements of the security policy.
Implementation assurance	It is the evidence establishing that the implementation is consistent with security requirements of security policy.
Operational assurance (Administrative Assurance)	It is the evidence establishing that the system sustains the security policy requirements during installation, configuration and day-to-day operation.

In Figure 9.5 shows that if assurance step 4 indicates a flaw in the implementation, the implementation will be adjusted and step 4 has to be redone.

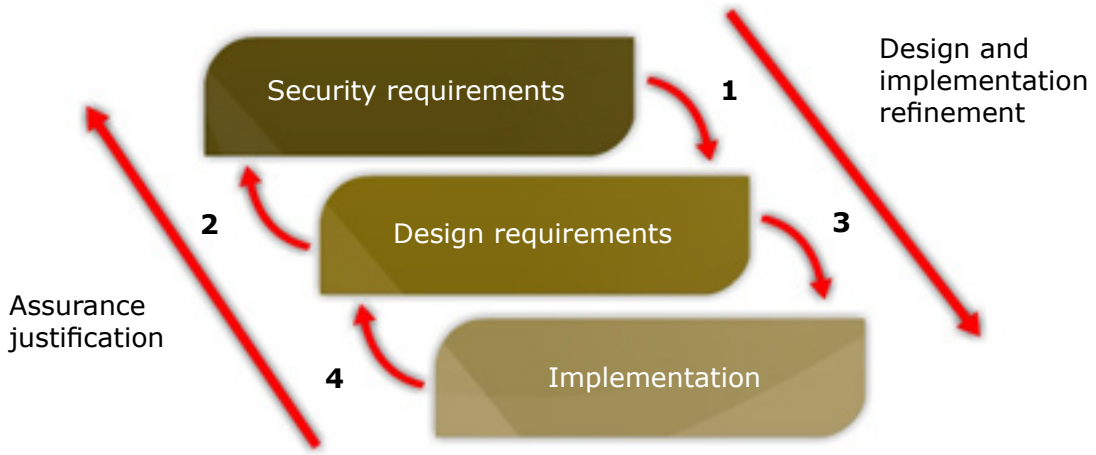

Figure 9.5: Development of a trusted system. There may be multiple levels of design and implementation.

If a flaw happens in implementation, thus indicates flaw in the design, causing step 1, 2, 3 and 4 to be revisited. A flaw in implementation or design is related to a flaw in the requirement.

9.2.3 Life Cycle and Assurance

To build secure and trusted systems will depend on standard software engineering techniques augmented with specific technologies and methodologies. To illustrate this concept, a metamodel that addresses the need of any business application has incorporates the four stages of life cycle which are conception, manufacture, deployment and fielded product life. The life cycle stages are shown in Table 9.3.

Table 9.3: Life Cycle Stages

Life Cycle Stage	Description

Conception	• Decisions to pursue it.
	• It needs proof of concept and identify if idea has merit.
	• High-level requirements analysis.
	  • What does "secure" mean for this concept?
	  • Is it possible for this concept to meet this meaning of security?
	  • Is the organisation willing to support the additional resources required to make this concept meet this meaning of security?

Manufacture	• Develop detailed plans for each group involved.
	  • May depend on use; internal product but requires no sales.
	• Implement the plans to create entity.
	  • Includes decisions whether to proceed, for example due to market needs.

Deployment	• Delivery.
	  • Assure that correct masters are delivered to production and protected.
	  • Distribute to customers, sales organisations.
	• Installation and configuration.
	  • Ensure product works appropriately for specific environment into which it is installed.
	  • Service people know security procedures.

Fielded Product Life	• Routine maintenance, patching.
	  • Responsibility of engineering in small organisations.
	  • Responsibility may be in different group than one that manufactures product.
	• Customer service, support organisations.
	• Retirement or decommission of product.

Related to this lifecycle stage, Waterfall Lifecycle Model is the most common model to be used. However this model is not the only technique for building secure and trusted systems. This lifecycle model consists of five stages which Requirements Definition and Analysis, System and Software Design, Implementation and Unit Testing, Integration and System Testing and Operation and Maintenance as shown in Figure 9.6.

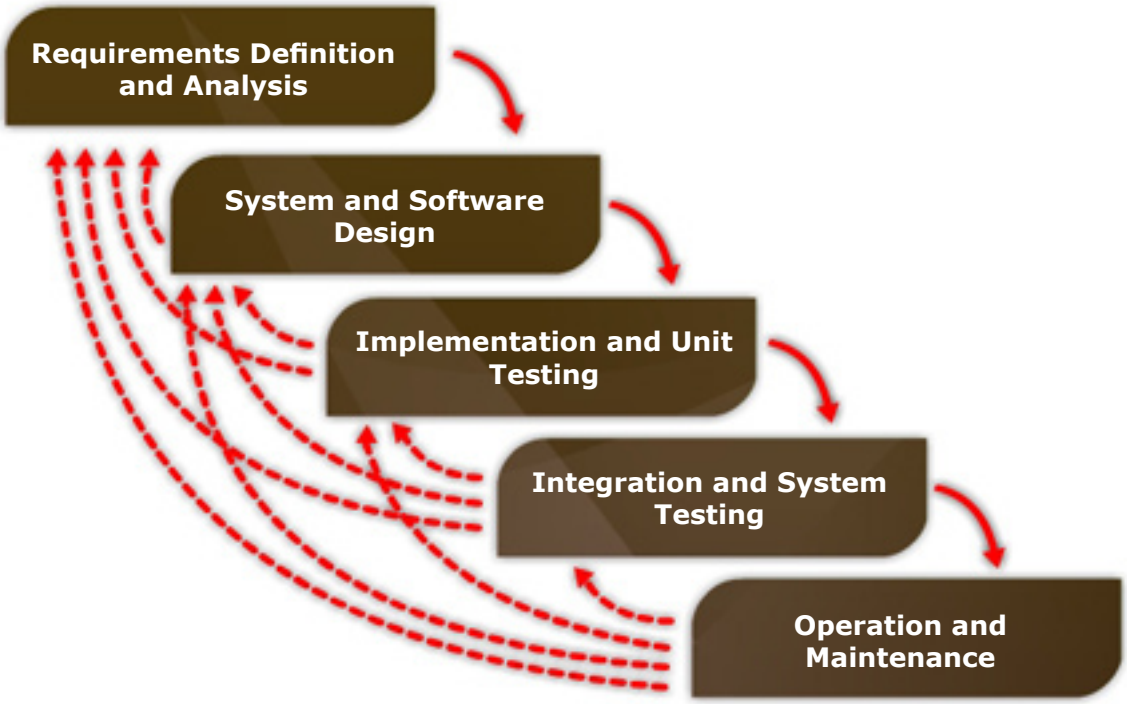

Figure 9.6: Waterfall Lifecycle Model

The solid arrows show the flow of development in the model, while the dash arrows show the paths along which information about errors may be sent. Other example life cycle model can be Exploratory Programming, Prototyping, Formal transformation and Extreme Programming.

Security is an integral part of a computer system. It should be integrated from beginning rather than added later.

9.3 INFORMATION PROTECTION MANAGEMENT SERVICES

In previous day, administrator will placed a firewall on the network perimeter to keep unauthorised traffic out, and their security jobs were done. Presently, organisations are struggled to fight viruses and worms became a daily threat, enterprises require deploying antivirus software and keeping it updated.

Currently, most of organisations focus on risk management issues on how to protect their private and confidential information such as:

- Trade secrets;
- Intellectual property;
- Business strategy; and
- Financial data in order to ensure unauthorised users are not able to access or read this data.

Several commercial services are offered to keep this information locked down with technology. However, organisations need to thoroughly identify the most suitable information protection services that can fit their business process.

Examples of information protection management services are:

- *Email Management Express* by IBM;
- *EDS Information Security Management Services* by EDS.com; and
- *Microsoft's Windows Rights Management Services (WRMS)* by Microsoft.

9.3.1 Overview of WRMS

WRMS is an example of information protection management services that using client-server architecture. It provides similar data protection capabilities and restrictions for administrators or data owners provided by the digital rights management (DRM) technologies employed by the music and movie industries.

DRM attempts to control how and where copyrighted media are used. WRMS used WRMS-based client software to protect data and define access rights by encrypting the content and embedded policy within the data that describes the access permissions. The WRMS-server provides RMS licenses that can be used to manage authentication and authorisation functionality.

9.3.2 How to Protect Data with WRMS

WRMS can be used to control the permission of the file. The permission can be given either Read or Change authority. The Read permission will allow users to view the

file only. However, Change permission will allow users to view, edit and save changes to the file, but cannot print the content.

WRMS also allows several options of customised document access as in Figure 9.7.

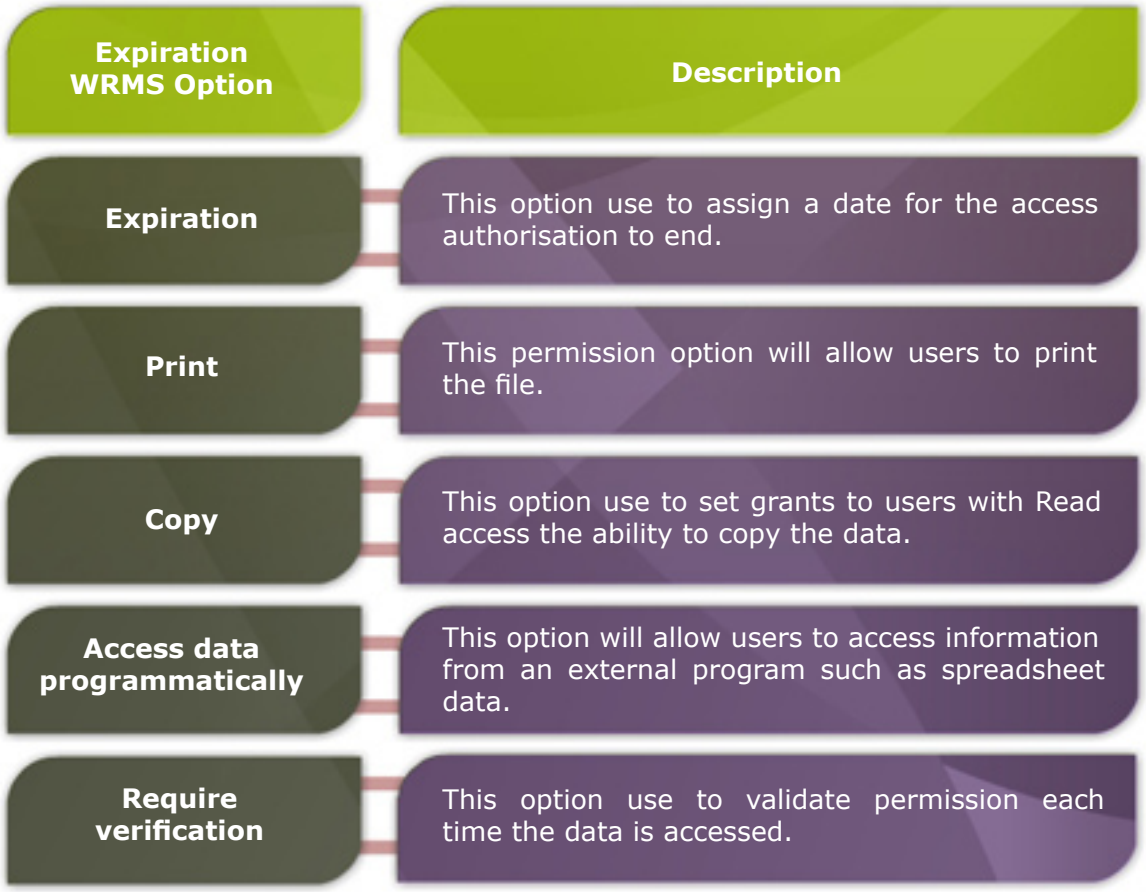

Figure 9.7: WRMS Options for customised document

WRMS provides protection for email services that can restrict email recipients from forwarding, printing, or copying email messages. There is an additional option offered by WRMS by supplying an email address for users to request additional permissions to increase the access capability. One of the disadvantages of WRMS is that the client-side applications must be enabled for rights management in order to protect or access data.

Intellectual property and sensitive company information are invaluable data. Therefore, organisations need to ensure that confidential information is not compromised or leaked either by ignorant employees or through corporate espionage. Hence, by using one of information protection management servies such as WRMS, data owners and network administrators can control all the activities done to the data that accessed by users.

9.4 COMPLIANCE ISSUES

For critical IT infrastructure, there must be the central starting point for risk assessment and regulatory compliance. Complying with regulations such as FISMA and DITSCAP/ DIACAP (for US federal agencies) requires thorough analysis of the systems on which government agencies runs with:

- Precise;
- Consistent;
- Actionable metrics;
- The necessary information to understand their levels of software risk;
- Identify next steps to remediate those threats; and
- Demonstrate improvement over time.

Some of the compliance categories are shown in Figure 9.8.

Figure 9.8: Examples of compliance categories

To secure the IT system/network is more than simply protecting it from viruses and hackers. Many companies have to implement strict security measures required by their business partners and the government in order to adhere to the security compliance. Securing business network may seem daunting, but with careful planning and a little research, steps can be taken to safeguard company.

Here are a few strategies (see Figure 9.9) to help ensure that business can run smoothly and data remains secure.

Figure 9.9: Few strategies to help ensure that business can run smoothly and data remains secure

1. Getting Started

- **Build in-depth protection.**
  To fully safeguard your business, your security must intercept all communication between applications and the network. You should determine:
  - Who is allowed access to the network and data.
  - Which areas of the network they are allowed to reach.
  - What operations each person is allowed to conduct.
  - What information they can access and use.

Install firewalls and intrusion prevention systems to help you control who uses the network. You can also add content security to prevent viruses, spam, and spyware and provide control over Web browsing.

- **Create security event logs.**
  Tracking the behavior of an application and collecting and reporting network events can help you adapt to changing threats. Tracking helps you protect network endpoints such as PCs and servers with the latest security software, to keep malicious code from spreading across your business.

2. Set Up a Response Plan

- **Build a response plan.**
  This plan will help you determine whether an alert represents a serious incident or false alarm, and create reports on current threats.

- **Work with your networking staff.**
  Train your networking staff, as well as business, financial, and legal employees, to participate in a team that puts the response plan into action.

- **Consider outside help.**
  Outsourcing security monitoring and compliance can be more cost-effective than trying to recruit a security expert and provide nonstop network security. Companies often outsource tasks like user and system-activity logging, intrusion detection and prevention, and firewall management.

- **Get educated on incident response.**
  Start with the National Institute of Standards and Technology's Computer Security Resource Center, which publishes a range of security policy guidelines. In addition, the SANS Institute offers the Security Consensus Operational Readiness Evaluation, which seeks to provide a minimum standard for information security procedures. ISO standard 17799 also offers guidelines for security management and incident management.

3. Find the Source

- **Assess the damage, and find the source of the attack.**
  Security analysis tools can help you catch the perpetrator, identify what data or resources the attacker gained access to, and close security gaps. A threat mitigation tool and security information management (SIM) can help you locate the source of an attack.

- **Keep watch over your network.**
  Use configuration management to keep software on your network consistent, track

network changes, and provide up-to-date network visibility. Keeping track of your network configuration can help you be more aware of what's happening on your network and prevent an attack before it happens.

4. Meet Your Company's Needs

- **Establish company guidelines.**
  You can build and customise security response guidelines to suit your company's unique business needs. Keep lines of communications with managers and other employees open, to involve them in your efforts to protect the business.

- **Regularly review and update the security policy.**
  Be sure that your security policy lists behaviors that are allowed and those that are not allowed. Educate employees so they are aware of the importance of keeping the network safe.

- **Assess risk.**
  Understand the level of risk if a security breach occurs. You may want to change your security policy or business practices to reduce risk.

- **Plan ahead with vendors.**
  Make sure your business partners such as contractors and service providers understand and comply with your security policy. Prenegotiate security contracts and rates with service providers before an incident occurs.

5. Learn from Experience and Mistakes

- **Host a post-incident meeting.**
  If a security incident occurs, meet with your teams to discuss what went wrong, how to prevent it from occurring again, and lessons learned. Convert these findings into training and education programs for employees. Use e-mail and intranet sites to keep employees up to date on security threats.

- **Stop threats before they occur.**
  Run network vulnerability scans with security software to help ensure that your network remains secure. A good security application can help you discover gaps in your network before a hacker does.

SUMMARY

1. Security Assurance is critical for determining trustworthiness of systems.
2. Different levels of assurance arise, from informal evidence to rigorous mathematical evidence.
3. Assurance needed at all stages of system life cycle and building security in is more effective than adding it later.
4. WRMS provides similar data protection capabilities and restrictions for administrators or data owners.
5. Content protected by WRMS is encrypted and a usage policy is embedded within the data that describes the access permissions.
6. Some of the compliance categories are Identification and Authentication, Risk Assessment, Vulnerability Management, Outsourced Information System Services, Security Testing and Vulnerability Remediation.
7. Few survival guidelines should be implemented to overcome the compliance issue such as build in depth protection, setup response plan and so on.

GLOSSARY

DITSCAP/DIACAP	Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), number 5200.40, December 30, 1997.
Espionage	**Spying** involves an individual obtaining information that is considered secret or confidential without the permission of the holder of the information.
FISMA	Federal Information Security Management Act of 2002, Public Law No. 107-347, December 17, 2002.
WRMS	Windows Rights Management Services.

DISCUSSION QUESTIONS

1. Why is the Waterfall Model of software engineering the most commonly used method for development of trusted system?
2. A computer security expert contends that most break-ins to computer system today are attributable to flawed programming or incorrect configuration of systems and products. If this claim is true, do you think design assurance is as important as implementation and operational assurance? Why or why not?
3. Requirements are often difficult to derive, especially when the environment in which the system will function, and the specific tasks it will perform, are unknown. Explain the problems that this causes during development of assurance.

REFERENCES

Cisco System Inc. (2009). *Security Compliance: A Survival Guide*. http://www.cisco.com/web/solutions/smb/need_to/securitycompliance_a_survival_guide.html

Matt Bishop (2004). *Introduction to Computer Security*. Boston: Addison-Wesley Massachusetts: Jones and Bartlett Publishers.

OUNCE Labs (2007). *Know where your software is vulnerable*. http://www.ouncelabs.com/writable/resources/file/complianceguidefed.pdf

Tony Bradley (2008). *Network Security Tactics*. http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1287738,00.html