4. INFORMATION ON THE GROUP

4.1 BACKGROUND

4.1.1 History and Business

SCAN Associates was incorporated in Malaysia under the Companies Act, 1965 on 9 September 2000 as a private limited company under the name of Secure Computing & Networking Associates Sdn Bhd. Subsequently, on 27 August 2002, it changed its name to SCAN Associates Sdn Bhd. On 15 June 2005, it was converted to a public limited company and has since assumed its present name.

The SCAN Group is principally involved in providing ICT Security Services and Solutions. Currently the main focus of the Group is on data. With convergence of technologies, ICT Security for voice is starting to gain momentum. SCAN Group has future plans to venture into ICT Security for voice, especially for mobile communications.

The history of SCAN Group can be traced back to 1996, prior to its formation. Dato' Dr. Norbik Bashah bin Idris and Dato' Nasri bin Nasrun, the two main founders, together with another eight co-founders were involved in R&D in ICT security in general including the development of a Cryptoengine. The Cryptoengine was later capitalised at RM3.0 million during the incorporation of SCAN Group. Today, the Cryptoengine plays a pivotal role in the provision of ICT Security Services and Solutions by SCAN Group.

SCAN Group officially started with the incorporation of SCAN Associates in September 2000. The initial business activities of SCAN Group were in the provision of ICT security and general ICT solutions. In October 2000, one month after its incorporation, SCAN Group successfully landed its first major job providing Managed Security Services (MSS) to the Institut Diplomasi dan Hubungan Luar (IDHL). In February 2001, Mayban Venture Capital Company Sdn Bhd became the first venture capital investor in SCAN Associates.

In December 2000, SCAN Group won a major project with MAMPU to provide ICT security consulting and training services. In line with the Malaysian Government's emphasis to address opportunities in the ICT Industry, SCAN Group, through SCAN Associates, applied and was awarded MSC status in 2002.

In October 2002, SCAN Group won a contract from the Malaysian Government to provide monitoring and MSS over four-year period covering 500 units of ICT security devices for various government agencies. In the same year, Malaysian Debt Ventures Berhad provided funding amounting to RM26.3 million for the Government MSS Project. The contract was set-up from scratch and to operate an on-site Security Operation Centre in MAMPU to provide monitoring and Managed Security Services for its entire in-house ICT facilities.

In November 2003, SCAN Group built its own Security Operation Centre in its premises to provide Managed Security Services focusing on the private sector. To-date the success of its Security Operation Centre is reflected in its client base, which includes Affin Bank Berhad, Malaysia National Insurance Berhad, IDHL, Mayban Venture Capital Company Sdn Bhd and UTM's CASE.

In April 2004, SCAN Group won a contract for the development, integration and deployment of Application Security System from the Government.

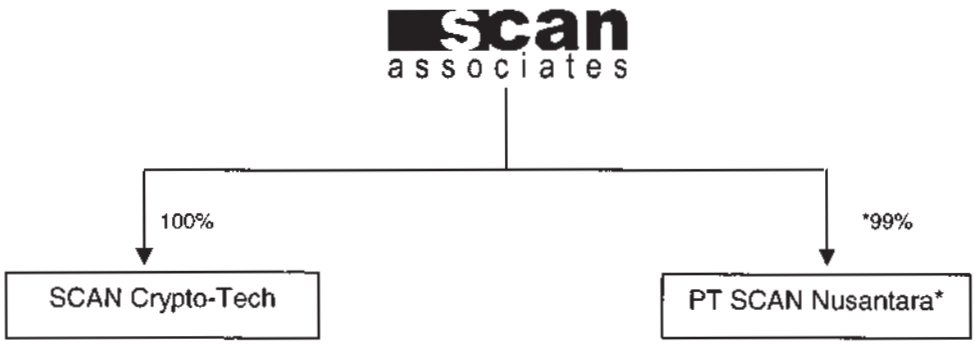
4. INFORMATION ON THE GROUP

In August 2004, CAV controlled approximately 56% equity interest in SCAN Associates by acquiring shares from Mayban Venture Capital Company Sdn Bhd and Dato' Nasri bin Nasrun.

Presently, the Group is principally involved in the provision of ICT security services and solutions.

4.1.2 Group Structure

An overview of the Group's structure is set out below: -



Details of the subsidiary corporations of the Company are summarised below: -

Company	Date/Place of Incorporation	Issued and Paid-up Share Capital (RM)	Effective Equity Interest (%)	Principal Activities
Subsidiaries of SCAN Associates				
SCAN Crypto-Tech	6 September 2002 / Malaysia	2	100	Intended for provision of crypto solution and secure mobile communications products and services
PT SCAN Nusantara*	27 September 2004 / Indonesia	USD100,000	99	Provision of ICT Solutions

Note:-

* Hazmi bin Hussain is entitled to purchase a further 39% of the share capital in PT SCAN Nusantara upon the fulfilment of the terms and conditions of the Shareholders Agreement dated 27 May 2005 between SCAN Associates and Hazmi bin Hussain.

4. INFORMATION ON THE GROUP *(Cont'd)*

4.1.3 Location of Business

The location of principal place of business of the Group is as follows:

		Location of Business	Approximate Built-up Area (sq. ft.)
Corporate Head-Office and Operations Premises	:	Level 8 Menara Naluri 161-B Jalan Ampang 50450 Kuala Lumpur	24,902
Research And Development Premises (MSC)	:	Block M-1 UPM-MTDC Incubation Center 1 Lebuh Silikon Universiti Putra Malaysia 43400 Serdang	2,400
SCAN Crypto-Tech	:	Level 7 Menara Naluri 161-B Jalan Ampang 50450 Kuala Lumpur	490
PT SCAN Nusantara	:	Park View Plaza Lantai 2 Jl. Taman Kemang No. 27 Jakarta Selatan 12730 Indonesia	2,368

4.1.4 Key Achievements/ Milestones/ Awards

Over the years in operations, the Group's key achievements and milestones are as follows: -

DATE	ACHIEVEMENTS AND MILESTONES
September 2000	SCAN Group started with the incorporation of SCAN Associates
October 2000	Capitalisation of intellectual property Cryptoengine and its related applications at RM3.0 million
October 2000	First job for Institut Diplomasi dan Hubungan Luar
December 2000	Major project with MAMPU for ICT Security Consultancy and ICT Security Training valued at RM2.7 million
February 2001	Mayban Venture Capital Company Sdn Bhd became the first venture capital investor in SCAN Associates
May 2002	Champion for the local hacking competition "Hack In The Box 2002"
September 2002	Champion for the local hacking competition "Info Security 2002"
October 2002	Project financing loan facility from Malaysian Debt Ventures Berhad of RM26.3 million for the Government MSS project
December 2002	Secured major contract from Government of Malaysia to develop monitoring and Managed Security Services, valued at RM65.7 million over a period of four years
December 2002	Received MSC status
December 2002	Extension of ICT Security Consultancy and ICT Security Training for MAMPU

4. INFORMATION ON THE GROUP *(Cont'd)*

DATE	ACHIEVEMENTS AND MILESTONES
January 2003	Appointed as consultant to provide security auditing for the Ministry of Defence
November 2003	Built a ICT Security Operations Centre (SOC) to provide managed security services
December 2003	Awarded contract for Managed Security Services by a major government agency
December 2003	Participated and won the international hacking competition held at the "Black Hat Asia 2003 Conference"
April 2004	Contract to develop, integrate and deploy Application Security System for the Government valued at RM6.3 million
April 2004	Secured Letter of Award from Malaysia National Insurance Berhad for IT Managed Security Services for three years
June 2004	Awarded contract by Affin Bank Berhad to provide Managed Security Services
August 2004	Commerce Asset Ventures Sdn Bhd acquired approximately 56% ownership of SCAN Associates
July 2005	Signed a Commercial Agency Agreement with GulfSCAN
July 2005	Awarded a Contract to provide 24 x 7 monitoring and surveillance services to the Government of Malaysia
August 2005	Renewal of the MSS Contract by a local bank for an additional year
October 2005	Certified by Mastercard International as Site Data Protection (SDP) Compliant Vendor. SCAN can now evaluate the security of online merchant's websites which store MasterCard account data and help them achieve compliance with the *Payment Card Industry (PCI) Data Security Standard* scanning requirement
December 2005	Awarded the Information Security Management System (ISMS) certification or better known as the BS 7799-2:2002 certificate, by SIRIM QAS International Sdn Bhd, for Software Product Development
January 2006	Signed a Contract with Central Information Technology Commission (CITC) of Saudi Arabia to provide ICT security consultancy services
February 2006	SCAN's subsidiary, PT SCAN Nusantara, signed an agreement with one of Indonesia's largest banks, for the provision of MSS
May 2006	Awarded the Frost & Sullivan 2006 Telecoms Award for Managed Security Service Provider of the Year

4.1.5 Share Capital And Changes In Share Capital

The present authorised share capital of SCAN Associates is RM25,000,000 comprising 250,000,000 ordinary shares of RM0.10 each. The issued and paid-up share capital of SCAN Associates is RM14,950,000 comprising 149,500,000 ordinary shares of RM0.10 each.

Details of the changes in the issued and paid-up share capital of the Company since its incorporation are as follows:

4. INFORMATION ON THE GROUP *(Cont'd)*

Date of Allotment	No. Of Ordinary Shares Allotted	Par Value (RM)	Consideration	Total Issued And Paid-up Share Capital (RM)
Ordinary Share				
09.09.2000	2	1.00	Cash	2
24.10.2000	2,999,998	1.00	Other than cash (capitalisation of development expenditure)	3,000,000
02.07.2001	1,285,000	1.00	Cash	4,285,000
09.05.2006	8,570,000	1.00	Other than cash (Bonus issue)	12,855,000
19.05.2006	2,095,000	1.00	Cash (Rights issue)	^14,950,000
19.05.2006	149,500,000	0.10	Sub-division of shares	14,950,000
Redeemable Preference Shares* ("RPS")				
12.08.2002	5,000	1.00	Cash	5,000
31.12.2003	(5,000)	1.00	Redeemed out of profits	-

Notes:
^ Fully paid on 9 August 2006
* 5,000 RPS of RM1.00 each were issued at a premium of RM99.00 each

4.1.6 Listing Scheme

In conjunction with, and as an integral part of the listing and quotation for the entire issued and paid-up share capital of SCAN Associates on the MESDAQ Market of Bursa Securities, the Company undertook a listing scheme which involved the following: -

(i) Bonus Issue

SCAN Associates undertook a bonus issue of 8,570,000 new ordinary shares of RM1.00 each to the existing shareholders of SCAN Associates on the basis of two (2) new ordinary shares for one (1) existing ordinary share held in SCAN Associates effected via capitalisation of the retained profits and capital redemption reserve. All the bonus issue shares rank pari passu in all respects with the existing ordinary shares of SCAN Associates.

Upon completion of the Bonus Issue, the issued and paid-up capital of SCAN Associates increased from RM4,285,000 to RM12,855,000 comprising 12,855,000 ordinary shares of RM1.00 each. The Bonus Issue was completed on 9 May 2006 and this has been reflected in the SCAN Group's latest audited accounts for the financial period ended 30 June 2006 in Sections 1.4 and 9.10.

(ii) Rights Issue

Upon completion of the Bonus Issue, SCAN Associates undertook a Rights Issue of 2,095,000 new ordinary shares of RM1.00 each at RM1.00 each per share to all the existing shareholders of SCAN Associates. The Rights Issue was undertaken on the basis of approximately point one six (0.16) new ordinary share for every existing one (1) ordinary share in SCAN Associates. The Rights Issue was allotted on 19 May 2006 and fully paid on 9 August 2006. This has been reflected in the SCAN Group's latest audited accounts for the financial period ended 30 June 2006 in Sections 1.4 and 9.10.

(iii) Sub-division

The par value of RM1.00 per ordinary share of SCAN Associates was sub-divided into ten (10) ordinary shares of RM0.10 each. Consequently, the number of issued and paid-up share capital of SCAN Associates increased from 14,950,000 ordinary shares of RM1.00 each to 149,500,000 ordinary shares of RM0.10 each.

The sub-division was completed on 19 May 2006 and this has been reflected in the SCAN Group's latest audited accounts for the financial period ended 30 June 2006 in Sections 1.4 and 9.10.

(iv) Public Issue

The Public Issue of 50,500,000 new ordinary shares at an issue price of RM0.50 are payable in full on application upon such terms and conditions as set out in this Prospectus and will be allocated and allotted in the following manner: -

(a) Malaysian Public

10,000,000 Public Issue Shares will be made available for application by Malaysian citizens, companies, societies, co-operatives and institutions, of which at least 30% is to be set aside strictly for Bumiputera individuals, companies, societies, co-operatives and institutions.

(b) Eligible Employees, Directors and Business Associates of the Group

20,000,000 Public Issue Shares will be reserved for the eligible employees, Directors and the business associates (which include the suppliers, sales agents and customers) of the Group.

13,500,000 Public Issue Shares have been allocated to 171 eligible employees and Directors of the Group based on the following criteria as approved by the Company's Board of Directors: -

(a) At least eighteen (18) years old;
(b) Job position;
(c) Length of service; and
(d) Performance.

THE REST OF THIS PAGE IS INTENTIONALLY LEFT BLANK

4. INFORMATION ON THE GROUP *(Cont'd)*

Details of the Directors' pink form allocation are as follows: -

Name of Directors	Designation	Pink Form Allocation
Datuk Ir. Mohamed Al Amin Abdul Majid	Chairman / Independent Director	125,000
Lt. Gen (R) Raja Dato' Abdul Rashid bin Raja Badiozaman	Deputy Chairman / Independent Director	125,000
Aminuddin Baki @ Sabtu bin Esa	CEO / Executive Director	-
Dato' Dr. Norbik Bashah bin Idris	Technical Director/ Executive Director	-
Dato' Nasri bin Nasrun	Non-Executive Non-Independent Director	-
Raja Shamsul Kamal bin Raja Shahruzzaman	Non-Executive Non-Independent Director	125,000
Mohd Jafni bin Mohd Alias	Alternate Director to Raja Shamsul Kamal bin Raja Shahruzzaman	125,000
Shaharil bin Abdul Malek	Alternate Director to Dato' Dr. Norbik Bashah bin Idris	-
Total		**500,000**

6,500,000 Public Issue Shares have also been allocated to 200 eligible business associates of the Group based on the following criteria as approved by the Group's Board of Directors: -

(a) Contribution to the Group's current and future business operations and opportunities; and
(b) Length of business relationship.

(c) Placees

20,500,000 Public Issue Shares are reserved for private placement to selected investors, which have been identified.

In summary, the IPO Shares will be allocated and allotted in the following manner: -

	Public Issue Shares	% of Enlarged Share Capital (%)
Public	10,000,000	5%
Eligible Employees, Directors and Business Associates of the Group	20,000,000	10%
Placement – Selected Investors	20,500,000	10.25%
Total	**50,500,000**	**25.25%**

4. INFORMATION ON THE GROUP *(Cont'd)*

All the Public Issue Shares available for application by the Malaysian public and the eligible employees, Directors and business associates of the Group have been fully underwritten. The Public Issue Shares available for application by the selected investors are not underwritten. The Placement Agent has received irrevocable undertakings from the selected investors to take up the Public Issue Shares available for application under the private placement.

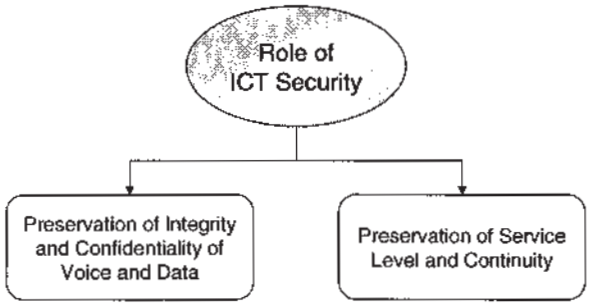
Any Public Issue Shares which are not taken up by eligible employees, Directors and the business associates of the Group will be made available for application by Malaysian Public via ballotting and the selected investors via private placement. Any Public Issue Shares not taken up by Malaysian Public will be made available to selected investors via private placement if the private placement is oversubscribed and vice versa. Any further Public Issue Shares not subscribed for will be made available for subscription by the Underwriters in the proportion specified in the Underwriting Agreement dated 1 June 2006.

THE REST OF THIS PAGE IS INTENTIONALLY LEFT BLANK

4. INFORMATION ON THE GROUP *(Cont'd)*

4.2 BUSINESS

SCAN Group's business is focussed on providing ICT Security Services and Solutions. The main role of ICT Security in an organisation is as follows: -

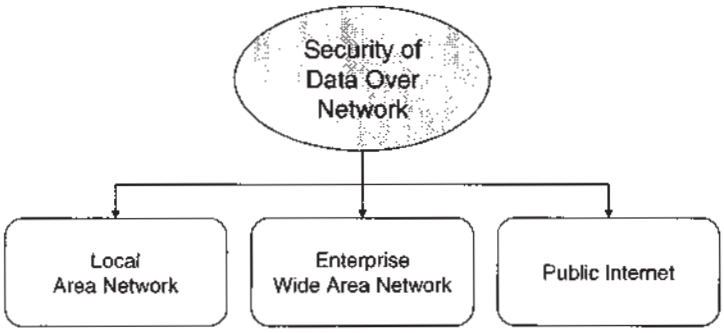


Currently the main focus of the Group is on data rather than voice or sound. However, with convergence of technologies, ICT Security for voice is starting to gain momentum. SCAN Group has future plans to venture into ICT Security for voice, especially for mobile communications.

Currently SCAN Group's ICT Security services are focused in the following areas:-

- Preservation of Integrity and Confidentiality of Data; and
- Preservation of Service Level and Continuity.

SCAN Group's ICT Security services are focused on network-based security as follows: -



Network-Based Security

The SCAN Group is not involved with ICT Security of stand-alone processors and devices. Instead, the SCAN Group's ICT Security is focused on end-to-end ICT Security for networks. This enables the SCAN Group to provide ICT Security for data in transit and at all ends or nodes of the enterprise network together with all the devices attached to the network.

For data in transit, SCAN Group uses two methods to provide ICT Security: -

- Cryptography where data in transit is securely encrypted; and
- Virtual Private Network (VPN) gateway to create a controlled private communication channel using Secured Socket Layer (SSL) protocol to secure data transmission through tunnelling over a private or public network.

For data in storage, the SCAN Group's employs Cryptography method to ensure confidentiality. The focus of SCAN Group's ICT Security Products, Services and Solutions are as follows: -

- **Cryptography**: It involves the application of encryption and decryption technologies to preserve the confidentiality of data in transit and storage. It also involves the methodology of operating an encryption and decryption system effectively and efficiently.

- **Managed Security Services:** It is an outsourcing function where clients may outsource all or some of their ICT Security requirements to be managed by SCAN Group. Some of these services include:

  - Prevention of unauthorised access and intrusion into systems and data depositories; and

  - Monitoring of network traffic for abnormality, diagnostics and reporting.

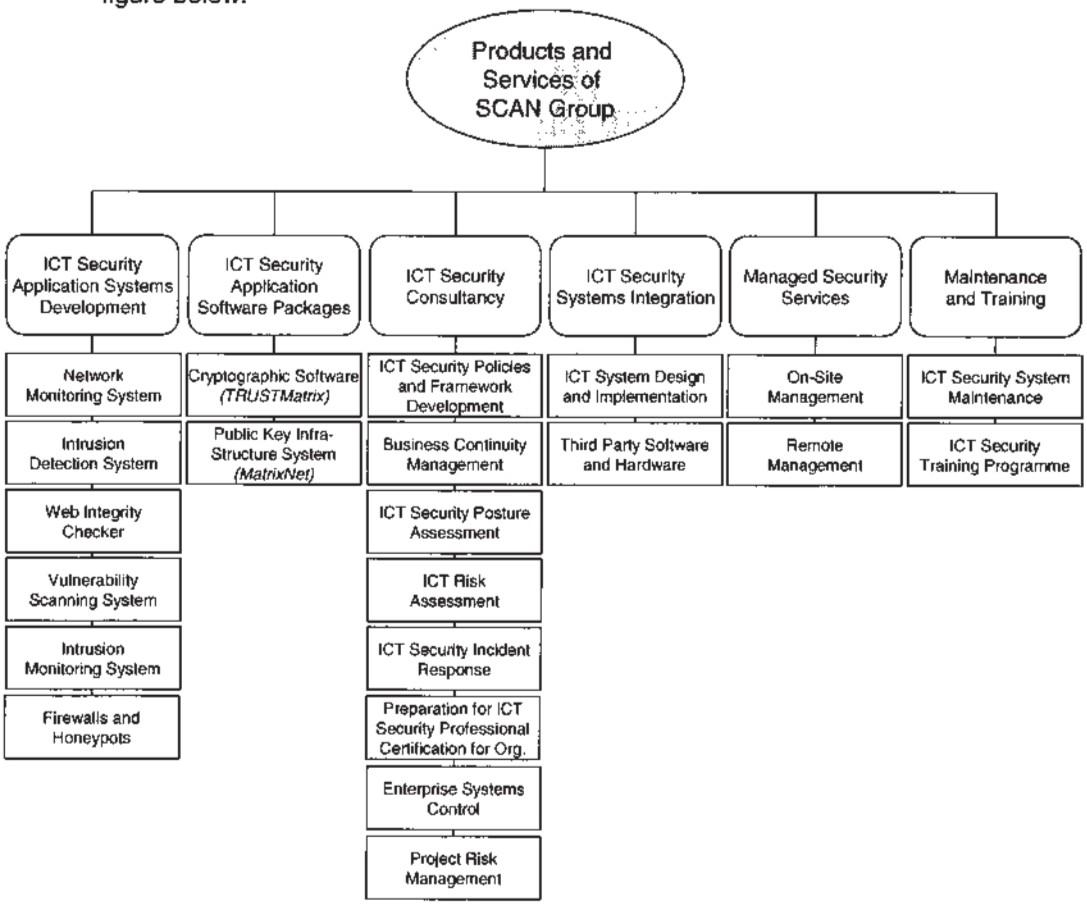
- **ICT Security Application Software Development:** It involves the development and customisation of ICT Security applications.

- **Consultancy**: It covers consultancy services on ICT Security risk and advisory.

The SCAN Group's business is mainly project based and therefore is not subject to any seasonal effects or trends.

4.2.1 Types of Products and/or Services

The current principal business activities of the SCAN Group are depicted in the figure below:



Principal Business Activities of SCAN Group

As an ICT Security Service and Solutions provider, the principal activities of SCAN Group are focused on the following areas:

- ICT Security Application Systems Development;
- ICT Security Application Software Packages;
- ICT Security Consultancy;
- ICT Security Systems Integration;
- Provision of Managed Security Services; and
- Provision of Maintenance and Training Services.

4.2.1.1 ICT Security Application Systems Development

One of the core competencies of SCAN Group is the in-house development of customised software solutions for ICT Security. This involves the creation of application software specific to clients' needs. One of the primary functions of this activity is coding (writing) of computer programs based on specific operating systems (for example Unix) using selected computer programming languages (for example C++). This business activity also incorporates systems testing to ensure that the ICT Security Application Software runs accurately and smoothly.

The ICT Security Application Software may be reused for other customers. SCAN Group is able to select the modules that meet the client's requirements and undertake some customisation and integration to the customers' systems. The reusability of this ICT Security Application Software provides SCAN Group with high profit margin due to the low cost of customisation and integration works. Some of the ICT Security Application Software are discussed below: -

ICT Security Application Systems Development		Descriptions
Network Monitoring System	:	Networking monitoring system monitors the entire enterprise network and checks on the networking devices and the service level of the network. This application provides information about status and problems of the network as well as the traffic flow. Log files and performance charts of the network can be generated from this system.
Intrusion Detection System	:	This is an application system that detects unauthorised access or attempts to enter the system through improper channels or means.
Web Integrity Checker	:	This is an automatic recovery system whereby it is able to recover a website back to its original condition after it has been attacked or defaced.
Vulnerability Scanning System	:	A system to scan for vulnerabilities by matching against a database containing known vulnerabilities. As at end of 15 May 2006, (being the latest practicable date prior to the issuance of the Prospectus), SCAN Group's vulnerability database has approximately 6,000 known vulnerabilities. This database is collected based on SCAN Group's own experiences combined with the standard Common Vulnerabilities and Exposures database maintained by Mitre Corporation of the US, a non-profitable organisation funded by the US Government. The objective of the system is to highlight vulnerabilities to enable management to take remedial actions to eliminate or minimise the impact of the vulnerabilities. It scans the system periodically or based on a timetable.

ICT Security Application Systems Development		Descriptions
Intrusion Monitoring System	:	This is a Java-based system that monitors cyber attacks. It is correlated with SANS ("System Administration, Audit, Network, Security") Institute's Internet Storm Center (ISC) that reports on global cyber attacks. The Intrusion Monitoring System enables the SCAN Group to analyse trends and methods of attacks to develop effective and efficient responses.
Firewalls	:	Firewall is a system or a group of systems that enforces an access control policy between two or more networks. This system works in a pair of mechanisms as follow:- - Block Traffic; and - Permit Traffic. This pair of mechanisms prevents unsolicited activities from occurring in the protected enterprise network from external parties. Firewall can be configured according to some set network policies determined by management. Firewall also generates log files on the type and volume of traffic passing through its network, and the number of attempts in breaking into the system.
Honeypots	:	Honeypot, also known as hacker decoy, is a decoy designed to act like a server to attract attacks and unauthorised access. Generally, Honeypots are used for prevention, detection, or information gathering of attacks or unauthorised access. It can distract hackers away from valuable machines on a network by luring the hackers to the honeypot itself. Honeypots are closely monitored to study the behaviour of intruders and the means of their attack. As such, Honeypots sometime act as advance warning of impending attacks and prepares the company in mounting a counter attack.

4.2.1.2 ICT Security Application Software Packages

SCAN Group has developed two ICT Application Software Packages that are generic in nature and may be installed on clients' systems without need for major customisation or integration. These are described below.

4.2.1.2.1 Cryptographic Software – TRUSTMatrix®

TRUSTMatrix® is a cryptographic software package that enables data to be encrypted for transmission and storage, and subsequently decrypted as and when required. TRUSTMatrix® is an indigenous cryptographic solution developed in-house by SCAN Group and it holds the intellectual property rights.

For data in transit, while being transmitted from one point to another, encrypted data is one of the most effective ways to prevent unauthorised tapping or access to data. This is particularly pertinent for wireless communications where there are devices that can easily tap data while being transmitted through microwaves, radio frequencies or infrared. For data in storage, encryption represents another line of defence to undermine unauthorised data access.

4. INFORMATION ON THE GROUP *(Cont'd)*

TRUSTMatrix® uses its own in-house developed industrial strength Cryptoengine for encryption and decryption. It provides minimum encryption strength of 128-bit, choice of algorithms and authentication with a minimum of 1024-bit public key size.

SCAN Group's Cryptographic Software package is designed for the enterprise level or a close-user group. This means that all users must be registered with the organisation that is running TRUSTMatrix®. SCAN Group's Cryptographic Software package is not designed for public use and does not require a PKI-based solution. However, it is possible to integrate PKI into SCAN Group's Cryptographic Software package, if required.

TRUSTMatrix® comes with seven applications in which five are for the client side and two for the server side. The five applications for the client side are as follows:

(i) Encryption Explorer

This application is used to protect contents of folders against unauthorised user by encrypting the folders. The application is integrated with Microsoft Windows Explorer and Microsoft Word, and supports MS-Office 97 and Windows 2000 and their higher versions.

(ii) Email Encryption Plug-in

This application is use for encrypting and decrypting e-mail messages and attachments. It also provides digital signatures for authentication and is integrated with the Public Key Management System. The application is integrated with Microsoft Windows Explorer and supports MS-Office 97 and Windows 2000 and their higher versions.

(iii) Secure Delivery

This is an application that allows TRUSTMatrix® users to deliver content securely to third-party recipients regardless of the platform.

(iv) Key Manager

This is an automatic management tool for tracking, managing and distributing public-key cryptography.

The application supports various tokens such as USB and smart card. It complies with international standard such as OpenPGP protocol format and Public Key Cryptography Standards (PKCS).

(v) Hotkeys

A simple application used to encrypt or decrypt text content of any Windows-based applications. The two applications for the server side are as follows:-

Key Server
A public key repository for all registered users.

KeyAdmin Console
It is one of the main applications in TRUSTMatrix® where it has the capability to control the whole system of authentication, encryption and decryption. This is an application whereby the authorised server administrator has the authority to manage corporate signing key, enforcing encryption policy and provides message recovery facility.

4.2.1.2.2 Public Key Infrastructure System - MatrixNet

MatrixNet is a PKI solution whereby it enables users to use unsecured public network such as the Internet to securely and privately exchange data by using Digital Signature that is obtained and shared through a Trusted Authority or commonly called Certificate Authorities.

MatrixNet is an indigenous solution developed in-house by SCAN Group and it holds the intellectual property rights. The whole of PKI technology depends on the Cryptoengine. SCAN Group developed the Cryptoengine, which is called SCAN Cryptoengine.

A PKI system is normally extended to the public. Each sender or recipient of encrypted items must be registered with the central organisation that is using and administrating the PKI solution for its specific purpose.

Digital Certificates are designed to authenticate the identity of a person who sends a message across the network and also provide an encryption key to send encrypted and secured message. The Certified Authorities are the organisations that can issue digital certificates and make public keys available to intended recipient. Certified Authorities can revoke Digital Certificates if someone uses or obtains the certificate illegally. Currently there are only two Certified Authorities that are allowed to issue Digital Signature in Malaysia:-

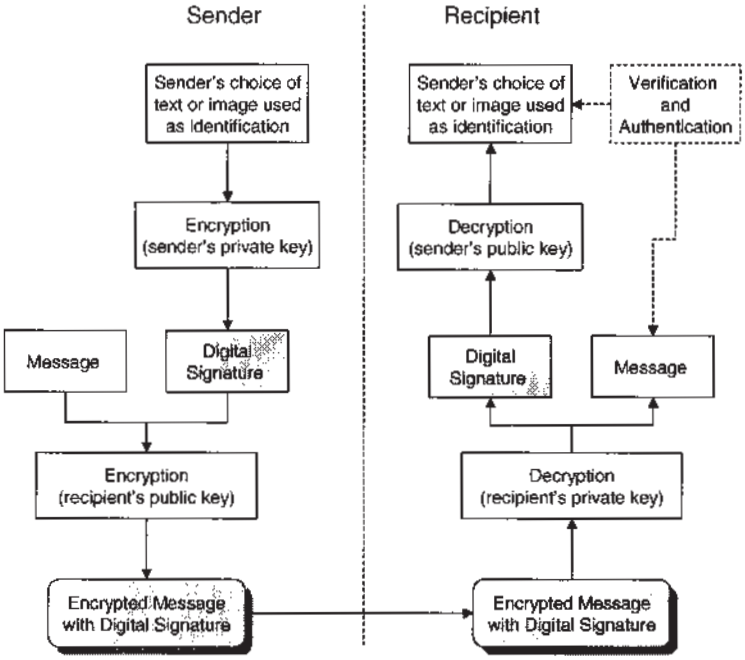
- Digicert Sdn Bhd; and
- MSC Trustgate.Com Sdn Bhd.

Digital Certificates contain vital information such as the following:-

- Sender's name;
- Certificate's serial number;
- Expiration date;
- Copy of sender's public key;
- Certificate issuer's public key; and
- Digital Signature for verification purpose

Digital Certificate issued to the users is installed on user's computer to identify user's identity.

4. INFORMATION ON THE GROUP *(Cont'd)*



Public Key Infrastructure Solution

In PKI solution, Digital Signature is vital for verification purpose. A sender can create a Digital Signature related to the message that it is sending. A Digital Signature may start of as any text or image selected by the sender to be the signature. The sender will then use his own private key issued by a Certified Authority to encrypt the signature and hence it becomes a Digital Signature.

The message to be sent can be in text or image. It is then encrypted using the intended recipient's public key. The Digital Signature is attached to the message, which are then encrypted together. The sender will send the encrypted message and Digital Signature to the recipient. It is not possible to separate the message and Digital Signature without the recipient's private key. Any one can receive the encrypted message but only the intended recipient will be able to decrypt and read the message because the intended recipient's private key is the only one that can decrypt the message.

At the same time the recipient will also decrypt the Digital Signature using the sender's public key to verify and authenticate the sender of the message.

It is possible for a PKI solution to exclude the Digital Signature function. However, businesses and contractual matters would more likely incorporate the added Digital Signature function.

There are two modes of Encryption/Decryption process:-

- Symmetric, whereby only one key is used for both encryption and decryption; and
- Asymmetric, whereby one key is used for encryption and a different key is used for decryption, which is more secure.

4.2.1.3 ICT Security Consultancy

ICT Security Consultancy represents a core component of SCAN Group's revenue stream. It includes the following:-

- ICT Security Policies and Framework Development;
- Business Continuity Management;
- ICT Security Posture Assessment;
- ICT Risk Assessment;
- ICT Security Incident Response;
- Preparation for ICT Security Professional Certification for Organisations;
- Enterprise Systems Control; and
- Project Risk Management.

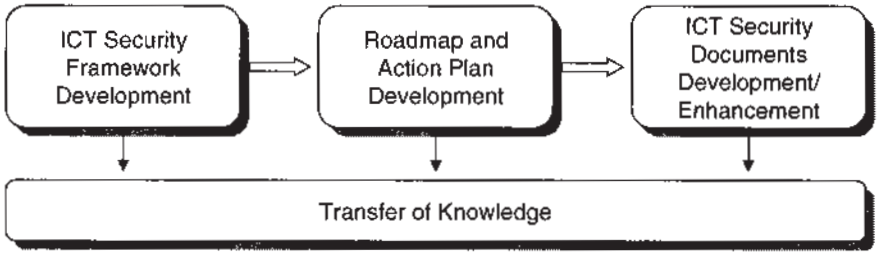
These services are critical to organisations, especially larger organisations that need to implement a robust enterprise-wide ICT Security system. Although these services may be undertaken in-house, more often than not, most organisations would not have in-house expertise to do them. As such, most of these works are done by external ICT Security Consultants like the SCAN Group.

4.2.1.3.1 ICT Security Policies and Framework Development

ICT Security Policies and Framework Development is to establish the standards and policies pertaining to a company's data security, security framework, processes as well as security solution technologies. SCAN Group's ICT Security Policies and Framework Development is also in accordance to best practices as well as in compliance to local regulatory requirements and international standards.

There are two components in this service, namely Security Framework and Security Policy. The Security Framework sets out to define the optimum framework for ICT Security for the company. It establishes the objectives, targets and processes to meet the company's needs.

The cycle of ICT Security Policies and Framework Development goes through a number of stages as depicted in the diagram below:-

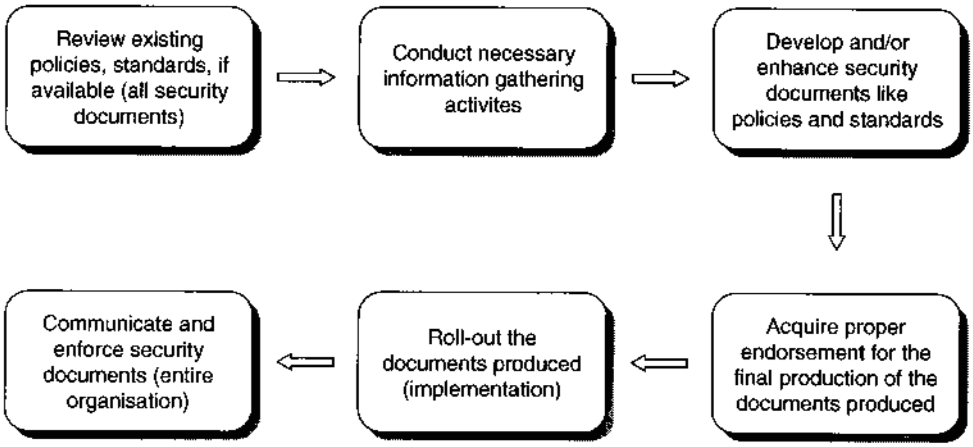


Transfer of Knowledge in ICT Security Policies and Framework Development

4. INFORMATION ON THE GROUP *(Cont'd)*

The ICT Security Policies and Framework Development is a consultancy service to devise a custom ICT Security policy to comply with management's guidelines and principles. It is designed to protect information confidentiality, integrity and availability in processing, storage and in transition, based on clearly defined policy statement, safeguard selections and effective implementation.

A series of stages are required to develop a set of ICT Security Documents as below:-

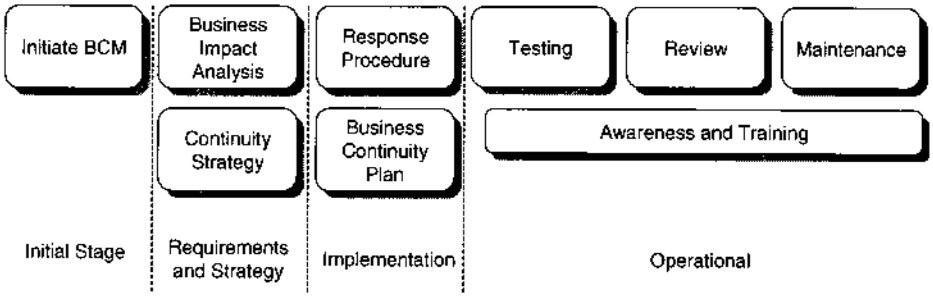


SCAN Group Approach in ICT Security Policies and Framework Development

4.2.1.3.2 Business Continuity Management

SCAN Group provides Business Continuity Management consultancy to ensure continuous business processes especially during and after a major disruption.

The Business Continuity Management (BCM) service goes through a series of stages:



SCAN Group Approach to Business Continuity Management

- **Initiate BCM:** Establish the scope and limitations of the BCM. An initiation checklist is used to collect and analyse information and data.

- **Business Impact Analysis:** Undertake studies to identify, quantify and qualify the impact of disruption. Assess the impact in terms of time, compliance and legal requirements.

- **Continuity Strategy**: Identify strategies for recovery based on a "worst possible post-disaster situation".

- **Response Procedures**: Develop and implement procedures for responding and stabilising the situation after an incident. Potential types of emergency and responses needed are identified and response procedures, established. A salvage policy and plan are also developed.

- **Business Continuity Plan**: A detailed and structured plan is developed to cover all aspects of responses in case of an incident. This includes mobilising of staff into teams, identifying their roles and responsibilities, and prioritisation of actions.

- **Testing**: The plan undergoes thorough testing which includes a simulation test.

- **Review and Maintain**: The plan is reviewed and maintained periodically to ensure relevance and effectiveness.

- **Awareness and Training**: Staff who is involved in the daily operation of the company are made aware and trained on the plan.

4.2.1.3.3 ICT Security Posture Assessment

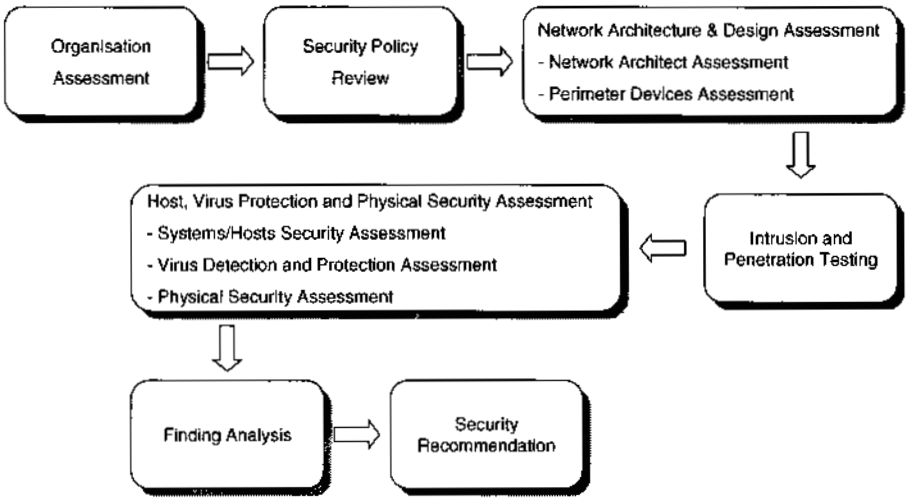
ICT Security Posture Assessment (SPA) is a comprehensive examination and review of a company's current ICT network and systems security. It identifies weaknesses and vulnerabilities within the network and systems security that could put the organisation at risk. Specific recommendations are then provided or introduced to enhance security against internal and external threats.

Some of the features of SPA consist of a number of assessments and reviews, which are as follows:-

- Organisation security review;
- ICT Security policy review;
- Network architecture review and security assessment;
- Penetration testing;
- Physical security review;
- Systems/hosts review and security assessment;
- Virus detection and protection assessment; and
- Data analysis, findings and recommendations.

4. INFORMATION ON THE GROUP *(Cont'd)*

Details of the company's SPA procedures and processes are depicted below:-



SCAN Group Approach in ICT Security Posture Assessment Process

- A team of consultants studies and analyses the company's ICT network set-up, architecture and policy based on information provided by the company. Another team conducts investigations on the actual 'ground-level' situation. Data collected is then compared and contrasted to uncover discrepancies in perceived and existing security. This policy review and audit is an essential initial step in SPA.

- Consultants perform penetration testing or 'ethical hacking' whereby they 'hack' into the company's network using advanced security tools to gain access to systems and hosts. This is to simulate how external hackers penetrate systems. The consultants will also attempt to penetrate the company's security from within the company using an internal LAN connection to simulate an informed hacking within the company.

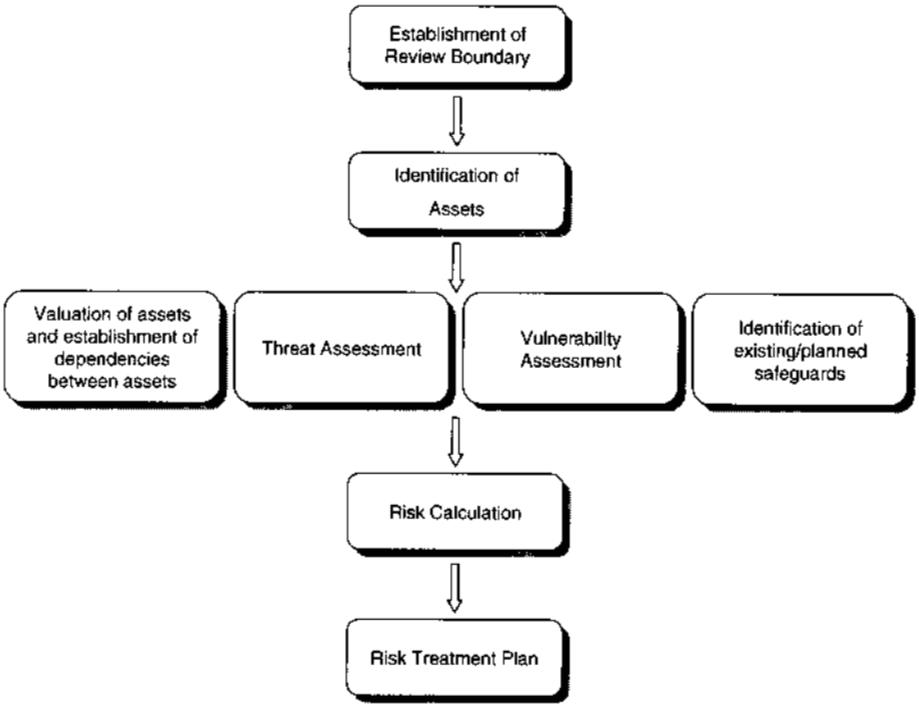
- Host security assessment refers to the problems that involve individual user authentication and file permissions, the file system of the host, system start-up files, system configuration files, and bugs and vulnerabilities that could be exploited by intruders who are actually logged onto the host.

  This is to reduce the exposure of internal hacking by insider such as staff or vendor. In most cases, correcting the setup or configuration of the host can solve these problems.

- Reports are then submitted outlining the company's security posture. The reports will also provide recommendations and customised solutions for long-term security measures.

4.2.1.3.4 ICT Risk Assessment

ICT Risk Assessment is the assessment of a company's ICT infrastructure and applications in terms of risks under threat. This knowledge of risks is a key element when the company undertakes targeted cost-conscious measures to manage and handle risks.



SCAN Group ICT Risk Assessment Plan

SCAN Group's approach to ICT Risk Assessment utilises its proprietary methodology to assess risks and develop recommendations to mitigate and minimise risks. The company's ICT Risk Assessment covers the following tasks:-

- **Establishment of review boundary.** This is where the scope of the activity is defined. Risk assessment of all assets in the company is done in stages, whereby critical business functions are given priority over the less critical ones.

- **Identification and valuation of assets.** This involves identification of business functions and processes as well as physical and information assets associated with the functions and processes. Assets include hardware, software, people, network and informational data. Once assets are valued, a quantitative and qualitative value is assigned to them and to establish the dependence between assets.

- **Threat assessment.** Using well-known threat databases as guidelines to identify threat categories such as non-compliance that are also identified to be later rectified.

- **Vulnerability assessment.** SCAN Group uses the Common Vulnerabilities and Exposure Guidelines to analyse the vulnerabilities associated with each asset identified.

- **Identification of existing and planned safeguards.** For accurate assessment, existing as well as planned safeguards are identified before the level of risk for each asset is qualified.

- **Risk calculation**. A business impact analysis is performed as well as a likelihood analysis to calculate risks. The impact analysis identifies assets that ought to be adequately protected to prevent business interruptions in case of security breach. The likelihood of the assets being compromised is analysed as well. Based on the information derived, a risk matrix is created.

- **Risk treatment plan**. Once risks associated with each asset are identified, corrective actions can be taken. This comes in the form of reduced, accepted, transferred or avoided risks. Appropriate controls are identified as treatment.

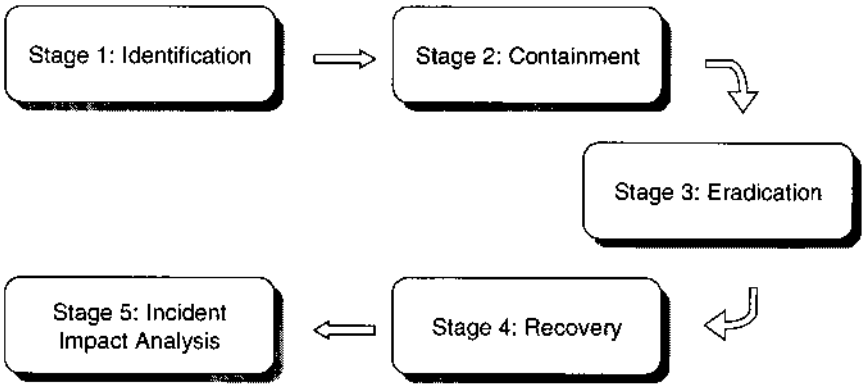
4.2.1.3.5 ICT Security Incident Response

An ICT security incident is a deliberate attempt to gain unauthorised access to a company's system or data in order to disrupt the service or change the system's characteristics without the owner's knowledge. Unauthorised access to a company's data or system can come in many forms as follows:-

- *Malicious Codes* such as viruses, worms, Trojan horses, and time bombs.

- *Intrusions* or *Breaking* whereby an intruder may bypass a system's authentication process to engineer unauthorised activities.

- *Insider Attack* includes industrial or commercial espionage by someone working inside the organisation.



Stages of ICT Security Incident Response Handling

4. INFORMATION ON THE GROUP *(Cont'd)*

In Incident Response Handling, SCAN Group performs two responses.

The main one is to respond and minimise damage and ensure continuity of operations when incidents occur. This initiative occurs in five stages:-

- *Identification* and determining the exact problem using sophisticated detection software as well as audit information to investigate the identity, nature and extent of the network attack;

- *Containment* by limiting the extend of the attack. This may involve shutting down the system temporarily if the system is classified or sensitive data is at risk. Another alternative is to keep the system up and risk some minimal damage in order to identify the intruder.

- *Eradication* of the system once the incident is contained using specialised software for such procedures and ensuring all backups are also free of viruses. Systems can become periodically re-infected with viruses because viruses are not periodically cleaned from the backup source.

- *Recovery* of the system to its normal working state after eradication. If the incident attack is network-based, it is important to install patches to all vulnerable holes in the operating system, which were exploited during the attack.

- *Incident Impact Analysis* of the system. This is a crucial follow-up stage and is post-mortem analysis providing very valuable information such as the following:-

  . to create a set of 'lessons learnt' as reference to improve future performance in similar situations;

  . justifying all security measures and efforts to management;

  . yielding information including a formal chronology of events, which may be essential in legal proceedings; and

  . to provide report, which includes estimates in monetary terms, the amount of damage, caused by the incident. This refers to loss of software, data, hardware damage, manpower costs and other restoration and reconfiguration costs.

The second response, which is a proactive initiative, is to promote proactive contingency action to tighten a company's ICT security against future incidents.

4.2.1.3.6 Preparation for ICT Security Professional Certification for Organisations

An example of preparation for ICT Security professional certification offered by SCAN Group is the ISO/IEC 27001 for Information Security Management System (ISMS) which is part of a company's information security management programme. It is a means by which a company monitors and controls its security and minimises risk to ensure that it fulfils the requirements of clients, users and partners to deliver products and services in a secure and protected environment.

The ISMS establishes a management framework that covers personnel, ICT systems and processes within a company. Changes are regularly monitored and reviewed and appropriate action taken to improve the security management system. The ISMS ensures that assets, which include sensitive and highly classified information, and the infrastructure around the information are adequately protected against threats. It ensures a system of implementing, operating and monitoring security that covers policy, procedures and guidelines.

The ISMS addresses following control areas:-

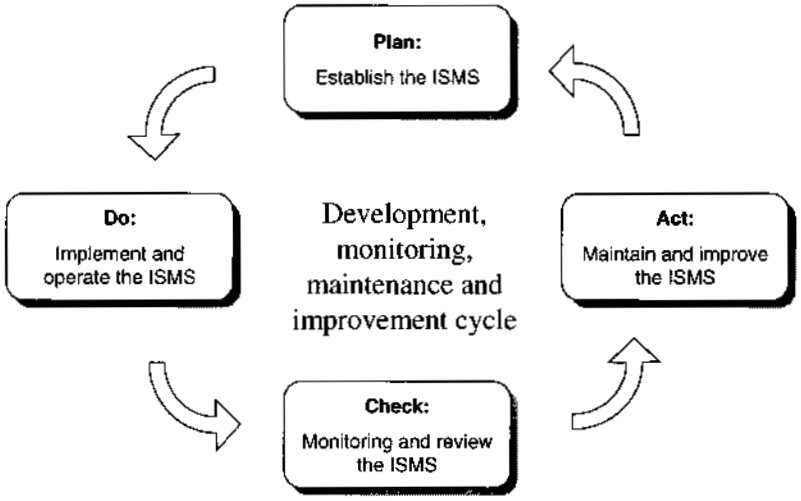
- Security policy;
- Security organisation;
- Asset classification and control;
- Personnel security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Systems development and maintenance;
- Business continuity management; and
- Compliance.

The ISO/IEC 27001 certification is an internationally recognised British Standard for ISMS specification and framework. The ISO/IEC 27001 certification recognises that a company has established and maintained documented ISMS that revolves around the build, operate, maintain and improve information security principle.

ISO/IEC 27001 certification ensures that an organisation complies with the industry's best practices for security. It makes for good marketing as it encourages trust among present and potential clients. With compliance, a better work practice and ethics in security is established. It creates credibility and confidence in an organisation company, especially if the organisation is dealing with government agencies or parties knowledgeable about ISO/IEC 27001 certification.

4. INFORMATION ON THE GROUP *(Cont'd)*

The figure below depicts components of an ISMS:



Plan-Do-Check-Act (PDCA) Model Applied to ISMS

The components of the PDCA Model applied to ISMS are as follows:-

- **Plan**: Establish the ISMS
  Establish scope, security policy, objectives, targets, processes and procedures to manage risk and improve information security to deliver results in accordance with the company's policies and objectives.

- **Do**: Implement & operate
  Operate the security policy, controls and procedures. Understanding of procedure is essential to ensure prompt detection and response to incidents. All staffs are appropriately trained and competent.

- **Check**: Monitor & review
  Assess and measure where applicable: process performance against security policy and objectives against practical experience and report to management for review.

- **Act**: Maintain & improve
  Take corrective action, preventive action and make improvements based on the management review.

4.2.1.3.7 Enterprise Systems Control

SCAN Group provides Enterprise Systems Control services, which are modular suites of services as part of Risk Management for enterprise solution such as ERP (Enterprise Resource Planning). The Enterprise Systems Control provides the following benefits to clients:-

- Proactive design and implementation of efficient operational and financial controls within business processes;
- Maintain a focus on controls throughout the project lifecycle where critical configuration and business change decisions are made;
- Design a security approach that supports business process control objectives and protects sensitive information assets;
- Ensure that the integrity of operational and financial information is maintained throughout the system transition; and
- Provide best practices IT control feedback based on SCAN Group's breadth of experience in IT risk management, application implementations, and information security.

The Enterprise Systems Control covers the following areas in an enterprise:-

- IT Operations;
- Business Processes;
- ICT Security; and
- Data Integrity.

IT Operations

The Enterprise Systems Control governs the overall IT operations in an enterprise emphasising business continuity and performance, capacity, asset and change management. It also provides technical support and help desk.

Business Processes

The Enterprise Systems Control also governs the importance of business processes in an enterprise by documenting the business processes, risk analysis, risk control, control business process design and implementation, and business processes optimisation.

ICT Security

The Enterprise Systems Control implements ICT Security in an enterprise by applying user access rights, solidify IT infrastructure (such as network, operating systems, and databases), monitoring and detection of information circulation and transaction, security policies and procedures, and ICT security administration.

Data Integrity

The Enterprise Systems Control strengthens data integrity in an enterprise by performing data mapping, data conversion, interfaces and audit trail.

4.2.1.3.8 Project Risk Management

Project Risk Management (PRM) provides management of an organisation with an objective and independent assessment of the inherent risks of any ICT Security Project and the effectiveness of controls planned or implemented to mitigate them. This valuable information assists management to control the associated risks and hence enable clients to take appropriate and timely actions to avoid project delays and failure.

SCAN Group has its own Project Management Methodology, which is customised from the methodology practiced by the Project Management Institute (PMI) and PRINCE 2.

Under SCAN Group's Project Management Methodology, the assigned project manager will develop project plan, set up, manage and control the project. He/she will also assist the Project Steering Committee to monitor and steer the project.

SCAN Group's PRM will closely look at the three elements of the Project, which are People, Process and Technology. The PRM will address the issues that arise from these elements as follows:-

People. Issues cover organisational change and the handling of training and education requirements must be carefully considered. If these are not thoroughly considered, the affected people may be resistant to use the new system.

Process. This addresses the activities relating to the restructuring of business processes, as a result of the project. Some alignment to the new processes may be required when introducing a new ICT system.

Technology. This addresses the risks that arise from the introduction of a new system. Issues pertaining to the support and maintenance of the system must be considered thus interruption may be avoided.

4.2.1.4 ICT Security Systems Integration

SCAN Group provides full ICT Security Systems Integration to meet specific client's needs. Basically, its ICT Security Systems Integration comprises two components as follows:-

- System Design and Implementation; and
- Third Party Software and Hardware.

4.2.1.4.1 System Design and Implementation

ICT Security System Integration is becoming more important as network and computer systems are increasing vulnerable. Such level of security requires complex and advanced cryptography, secure architecture, time needed to build such an architecture and resources to integrate multi-layered security features and constraints into the system. SCAN Group provides different packages of ICT Security System Integration such as the following:-

- develop complete application security architecture;
- integration of security products with the system hardware and software;
- customises applications with security features; and
- provides customisation with SCAN Group's indigenous encryption engine.

4.2.1.4.2 Third Party Software and Hardware

Part of an ICT Security System requires third party hardware and software, which are mainly generic in nature. They include the following:-

- servers and computers;
- computing peripherals;
- networking devices;
- operating systems;
- application systems; and
- system tools.

4.2.1.5 Managed Security Services

SCAN Group provides MSS which are outsourced by organisations who have decided to get a third party to be responsible for all their ICT Security. MSS operate on the principle of people, processes and technologies focusing on monitoring, detecting, responding, managing and preventing any form of disruption.

SCAN Group's MSS comprise the following:-

- An expert team of security consultants;
- Real-time network surveillance in ICT Security Operation Centre (SOC);
- Updating and patching of newly discovered vulnerabilities; and
- Periodic vulnerability scanning.

SCAN Group's MSS architecture comprise two main modules:-

- Proactive Protection
  - . ICT Security/Patches updates
  - . Network Policy Review and Updates
  - . Periodic Vulnerability scanning
  - . Periodic Penetration Testing
  - . Intrusion Detection
  - . ICT Security Diagnosis
  - . Threat Analysis
  - . Attack prediction
  - . Risk Management

- Reactive Response
  - . Incident Response Handling
  - . E-Forensic
  - . Rectification Action
  - . Post-Mortem Analysis

SCAN Group provides two types of MSS as follows:-

- On-site Management where SCAN Group provides resources for on-site ICT security management; and
- Remote Management where the SOC is located at SCAN Group's premises and SCAN Group's personnel will remotely manage client's ICT Security Systems.

4.2.1.6 Maintenance and Training

4.2.1.6.1 ICT Security System Maintenance

SCAN Group provides maintenance services for the ICT Systems and Software used by client. Maintenance includes among others, fixing software, hardware and system errors, and provision of periodic patches and updates.

4.2.1.6.2 ICT Security Training Programme

SCAN Group offers three categories of training modules for both technical and management categories as follows:

- Foundation
  - . Networking and TCP/IP
  - . Introduction to ICP Security
  - . UNIX: A Hands-on Introduction
  - . Internet Security and Applications
  - . Information Security Management System
- Intermediate
  - . Windows 2000/2003 Security and Administration
  - . UNIX Security and Hardening
  - . Incident Handling and Basic E-Forensic
  - . Basic Penetration Testing
  - . Firewalls and Perimeter Protections
  - . Cryptography and PKI
  - . Wireless Security
  - . Risk Management
  - . Business Impact Analysis
  - . Security Policy Development
- Advanced
  - . Windows Forensic
  - . UNIX Forensic
  - . HoneyNet
  - . Advanced Cryptography
  - . Java Security Programming
  - . Business Continuity Management

4. INFORMATION ON THE GROUP *(Cont'd)*

4.2.2 Technology Used

SCAN Group utilises Information and Communications Technologies in general and ICT Security technologies in particular in providing ICT Security products, services and solutions. Technologies used include the following:-

- Cryptography Technology
- Cryptographic Accelerators and Cluster Computing
- Information Technology
- Communications Technology
- Internet Technology
- Mobile Technology

4.2.2.1 Cryptography Technology

4.2.2.1.1 Cryptography System

SCAN Group uses Cryptography as one of its ICT Security portfolio of products and solutions. Cryptography is a system whereby it transforms (or encrypt) data into an unreadable format, called cipher text. Only those who possess a secret key can decrypt (or decipher) the message back into its original plain text.

An example of a simple cryptography system is to use a conversion table:

- If the message "SCAN" is to be encrypted, it will be converted to "VFDQ" using the table below, which acts as the encryption key:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Anyone accessing the encrypted "VFDQ" (this is the cipher text) will not have any idea what it normally means, unless it knows the encryption/decryption key which is the table of conversion.

- When the intended recipient receives the cipher text, he/she is aware of the conversion table and will decrypt "VFDQ" to become "SCAN" using the table below which acts as the decryption key:

D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. Cryptography systems depend on the secrecy of the encryption algorithm. In the above Cryptography system, the encryption/ decryption algorithm is to shift the position of the alphabets by three paces to the right of a normal ascending series of alphabets.

Another simple method is to assign numbers to each of the letters of the alphabet. The message is then converted to numbers based on this table of conversion. Assuming the encryption key is "5" the numerically converted message may then be multiplied by 5 to become another set of numbers. The recipient, knowing the "key" will then divide the cipher text by "5" and match the resultant set of numbers to the conversion table back to letters.

Using numbers is the preferred method of cryptographic algorithm as numbers can easily be manipulated.

The most critical part of the cryptographic algorithm is the encryption/decryption key. To prevent successful trial and error attempts (also known as brute force attempts), it is common to use one or more prime numbers as part of an algorithm to create the encryption/decryption key. The larger the prime number, the higher the number of possible combinations. Thus if the encryption/decryption key comprises only 1 digit, a maximum of ten attempts will allow someone to crack the encryption/decryption key. A 2-digit key will provide a maximum of 100 tries before the encryption/decryption key is cracked. As at May 2005, the largest known prime number has 7,816,230 digits, which was discovered by Dr Martin Nowak on 18 February 2005.

However, a large numbered key may slow down the encryption/ decryption process. Thus, the size of the key selected would need to depend on the level of security required.

There are two kinds of key-based encryption as follows:-

- Symmetric. Symmetric algorithms use the same key for encryption and decryption. This is sometimes known as secret-key Cryptography System.

- Asymmetric. Asymmetric algorithms use a different key for encryption and decryption. This is commonly known as public-key Cryptography System.

4.2.2.1.2 Public-Key Cryptography System

Public-key Cryptography System involves a public key, which is used for encrypting message, and a private key, which is used for decryption. The owner of the private key would be the only one who could decrypt the message. Anyone who knows the public key would not be able to decrypt the message.

Rivest-Shamir-Adleman

Rivest-Shamir-Adleman (RSA) is the most commonly used public-key algorithm. It can be used for both encryption/decryption and Digital Signatures.

RSA uses two large prime numbers multiplied together where the "modulus" is used as the public key and published for all to see. If anybody wants to encrypt a secret number to send to the publisher of the public-key, all he/she has to do is cube it, divide by the public-key and send the remainder from the division to the publisher. As the publisher of the public-key knows the two prime factors of the modulus, the original secret number can be recomputed from the remainder that was sent.

This algorithm is relatively strong and is difficult to break with a 1,024-bit encryption. The RSA algorithm can use a 2,048-bit encryption key, which would require today's fastest super computer many decades before it can crack the encrypted code using brute force method.

The benefit of this algorithm is the interoperability with most major protocols in today's network computing. It is the most important public-key Cryptography Systems.

Digital Signature Standard

Digital Signature Standard (DSS), a common standard that specifies a Digital Signature Algorithm (DSA) that is appropriate for applications requiring a digital rather than written signature.

The DSA provides the capability to generate and verify signatures. The Signature generation makes use of a private key to generate a digital signature and the signature verification makes use of a public key, which corresponds to the private key, except that it is not the same as the private key.

The strength of this algorithm has security level of around 80 bits, which raise concerns of possible successful attacks using special hardware. Generally DSA is fairly efficient but not as efficient compared to RSA.

Diffie-Hellman

Two people communicating over an insecure channel (such as the Internet) can compute a secret number that they both know but that cannot be computed from information intercepted on the channel. The "secret number" can then be used as an encryption key.

The Diffie-Hellman method uses prime numbers and modular mathematics to create a secret key. The Diffie-Hellman method overcomes the problem of distributing the secret key for it allows the construction of a common secret key over an insecure communication network. Unfortunately this protocol does not use countermeasures such as digital signatures.

4.2.2.1.3 Secret-Key Cryptography System

Secret-Key Cryptography Systems use the same key for both encryption and decryption and it is the more straightforward approach to data encryption hence mathematically less complicated than public-key cryptography.

Data Encryption Standard (DES and Triple-DES)

Data Encryption Standard (DES) is an encryption algorithm, which was developed by IBM in 1974 and was adopted as a standard by the US National Institute of Standards and Technology (NIST) in 1977.

DES can be considered strong for random hackers and individuals, but it is easily breakable with special hardware. This is because it uses a 56-bit encryption key.

Triple DES uses three 64-bit keys for encryption. Thus, Triple-DES was introduced which is arguably stronger than single DES but rather slower in processing.

Advanced Encryption Standard

Advanced Encryption Standard (AES) is a successor to DES. It can have key sizes ranging from 128 bits to 256 bits. AES was the selected proposed standard when NIST called for proposals for an official successor to DES that meets 21st century security needs. Besides AES, the other proposals were as follows:-

. MARS
. RC6
. Serpent
. Twofish

Blowfish

Blowfish has an encryption security level of 448 bits and it has gained a fair amount of acceptance in several applications.

Blowfish utilises the concept of randomised S-boxes whereby while doing the key scheduling, it generates large look-up tables by doing several encryptions. This concept has been proven to be highly resistant against many attacks.

Other types of Symmetric Cryptography Systems are as follows:-

- CAST-128
- International Data Encryption Algorithm (IDEA)
- RABBIT

4.2.2.1.4 Cryptographic Protocols

Cryptography works on many levels. The algorithm itself is one level and protocols are built on lower-level cryptographic algorithms.

Cryptographic protocols are as important as the algorithm because the overlying protocol reveals information on the keys used in encryption. Several well-known protocols and standards are as follows:

- *Domain name Server Security (DNSSEC),* a protocol to secure distributed name services.

- *Generic Security Services API (GSSAPI)* provides an authentication, key exchange, and encryption interface to different cryptographic algorithms.

- *Secure Socket Layer (SSL)/Transport Layer Security (TLS)*, protocols to secure World-Wide-Web (WWW) connections.

- *Secure Hypertext Transfer Protocol (SHTTP)*, protocol for providing more security for WWW transactions.

- *E-mail security and related services*, OpenPGP and Secure-MIME are two standards used.

- *PKCS*, standards to define safe ways to use RSA.

- *IEEE P1363: Standard Specifications for Public Key Cryptography*, standard for public key cryptography.

- *Secure Shell*, protocol used to secure terminal sessions and arbitrary TCP connections.

- *IPSec*, allowing particular programs to communicate on an unsecured network while maintaining security in the communication.

4.2.2.2 Cryptographic Accelerators and Cluster Computing

Cryptography systems require considerable processing power, sometimes up to one hundred times more processing power needed for non-encrypted packets. Cryptographic accelerators are used to increase the speed for encryption and decryption. The speed of encryption relies partially on the processing power of the computer. Faster processors in the computer can encrypt and decrypt faster compared to slower processors.

In cryptography, there is no limit to security level but the processing power in the computers stands as a barrier for achieving higher security level. Software based encryption algorithms can easily overburden a board's Central Processing Unit (CPU) and Random Access Memory (RAM).

In today's computing, organisations combine the processing powers together to form a virtual large processing unit. This is commonly achieved by implementing Cluster Computing. Cluster Computing focus on the ability to support computation across the organisation apart from traditional computer clusters or traditional distributed computing. It can also utilise the unused resources for solving massive computational problems.

In addition, new processors are becoming faster, more powerful and cheaper and will eventually not rely on cryptographic accelerators for high-speed encryption and decryption. Thus, Cluster Computing technology can be used in a number of ways to assist in the cryptography process:-

- as a low cost method to test the robustness of cryptographic algorithms; and
- as a means of providing faster encryption and decryption.

4.2.2.3 Information Technology

SCAN Group uses information technology (IT) in the development of its products as well as in the application of its products in the business environment for users. Within IT, there are a number of sub-sectors in which technologies are employed. These include:-

- Processing Hardware
- Operating Systems
- Software Applications
- Software Development Tools
- Databases
- Multimedia and Other Tools

4.2.2.4 Communications Technology

Computers require to communicate with each other as well as users need to access computers. As such, communications technologies are employed. Some of these communications technologies employed by SCAN Group include the following:-

- Local Area Network
  - . Devices (include computers, printer, scanners) that are connected together in close proximity usually in the same building
  - . Commonly uses IEEE 802.3 standard (also termed as Ethernet) protocol to connect devices together

- Wide Area Network
  - . Devices that are connected in a wider geographical area
  - . Commonly uses Transmission Control Protocol/Internet Protocol (TCP/IP) for communication
  - . Leased Lines, Integrated Services Digital Network (ISDN), Asynchronous Transfer Mode (ATM), Frame Relay and virtual private networks are commonly used to form Wide Area Network

- Internet
  - . Global collection of computer networks
  - . Uses Transmission Control Protocol/Internet Protocol (TCP/IP) for communication.

4.2.2.5 Internet

As the focus of ICT Security is data over network, unauthorised access is commonly via the public Internet. As such one of the main technologies used by SCAN Group is Internet technology. Some of these include the following:-

- browsers
- search engines
- electronic mail
- instant messaging
- electronic chat
- flash multimedia
- languages (for example, HTML, XML)
- communications protocol (TCP/IP)
- communications hierarchy (peer-to-peer, client-server)
- Three-tier Architecture Development
  - . Browser
  - . Middleware

. Database

The technology for Internet access has also evolved. Some of these include the following:-

- Digital leased line
- Analogue dial-up
- Integrated Services Digital Network (ISDN)
- Digital Subscriber Line (Asynchronous and Synchronous)
- Wireless broadband (802.11b, 802.11g)
- Third Generation (3G) wireless broadband
- Cable modem
- Satellite

4.2.2.6 Mobile Technology

SCAN Group also leverages from mobile technologies to keep up with technology innovations and striving to continually meet user needs. With a highly mobile workforce and the growing need to constantly keep in touch with the office while on the move, SCAN Group also uses and deploys secure mobile technologies in its product applications and solutions. The use of secure mobile technology provides added convenience and confidence to users of SCAN Group products and services. Some of the mobile devices used include the following:-

- mobile phones
- portable digital assistant (PDA)
- pocket PC

As such, the technologies used are modified to cater for the limitations of mobile devices. These include:-

- languages (J2ME)
- operating system (mobile windows, Palm OS, Symbian).

Some of the common mobile computing communication standards are as follow:

- *Wireless Application Protocol* (WAP) commonly used in mobile phones

- *General Packet Radio Services* (GPRS) commonly used in mobile phones
- *Third Generation (3G)* wireless broadband used in mobile phones and broadband Internet access

- *IEEE 802.15* is Wireless Personal Area Network (WPAN) or also known as Bluetooth commonly use in mobile phones, PDA and Pocket PC on a peer-to-peer basis

- *Infrared Data Association* (IrDA) a standard protocol data exchange over infrared light such as in Personal Area Networks

The use of mobile technologies require the used of different skill sets, tools and technologies.

4. INFORMATION ON THE GROUP *(Cont'd)*

4.2.3 Approvals, Major Licences and Permits Obtained

The major licences and permits obtained by the Group are as follows: -

Authority	Description	Major Conditions Imposed	Status of Compliance
Ministry of Finance	Registration of SCAN Associates with the Ministry of Finance in the following categories of supplies/services: - (a) Communication Equipments (040100); (b) Personal Computer and Related Peripherals and Services (210101); (c) Small to large multi-user systems and services (210102); (d) Workstations and Related Peripheral and Services (210103); (e) Software Product and Services (210104); (f) Other Computer related Services (210105); and (g) Networking Products and Services (210106)	(i) The approval granted is based on the information furnished by the Company. Should there be any changes from the information furnished, it should be made known to the MOF within 21 days from the date such changes occurred. (ii) SCAN Associates shall ensure that the categories stated in this approval does not overlap with any categories granted to another company which has common shareholders or directors and a common management with SCAN Associates. (iii) Renewal of registration must be made 3 months before the expiry date.	Met. Met. (Pending renewal where application was made on 12/06/ 2006)
Malaysian Agricultural, Research And Development Institute ("MARDI")	Registration of SCAN Associates with MARDI as a supplier of Personal Computer & Related Peripheral & Services; Small to Large Multi-User Systems & Services; Workstation and Related Peripheral & Services; Software/Networking Product & Services; and Other Computer Related Service and Communication Devices.	Nil	Not Applicable.
Government of Malaysia	Granting of MSC Status to SCAN Associates	The MSC Status entitles the Company to the incentives, rights and privileges provided under the Bill of Guarantees subject to the Company's continued adherence to the following criteria: - (i) Undertake and continue with such activities as specified in SCAN Associates' business plan as approved by MDC, as follows: (a) Development of Enterprise Public Key Infrastructure (PKI) Security solution, which comprises the following 3 components:	Met.

4. INFORMATION ON THE GROUP *(Cont'd)*

Authority	Description	Major Conditions Imposed	Status of Compliance
		• PKI Back-end trust Office component, which consists of Certificate Authority, registration Authority and Directory Server • PKI-enabled Security application suite, which consists of E-mail Security, FileDisk Encryption and Digital Time-stamping Recording System. • Cryptography Library, which consists of Cryptography Engine and Certificate Management Library	Met.
		(b) Development of Managed Security Services (MSS) solution, which comprises of Attack Monitoring System, Vulnerability Scanning system, Automatic Web Recovery System and Security Management Console.	Met.
		(c) Provision of Managed Security Services to enterprises	Met.
		(d) Provision of security consultancy and maintenance services for the abovementioned solutions	Met.
		(ii) locate the MSC-Status Company's headquarters and/or the implementation and operation of the MSC Qualifying Activities in a Designated Cybercity, within 6 months from 24 December 2002 and will seek MDC's prior written approval in the event of any changes in the location or address of the Company;	Met.
		(iii) ensure that at all times at least 15% of the total number of employees (excluding support staff) of the MSC-Status Company shall be "knowledge workers" (as defined by MDC);	Met.
		(iv) continuously comply with the MSC's environmental guidelines as determined by MDC from time to time;	Met.
		(v) submit to MDC a copy of the company's Annual Report and Audited Statements in parallel with submission to the Companies Commission of Malaysia; and	Met.
		(vi) comply with all such statutory, regulatory and/or licensing requirements as may be applicable	

4. INFORMATION ON THE GROUP *(Cont'd)*

Authority	Description	Major Conditions Imposed	Status of Compliance
Royal Customs and Excise Malaysia	Licence to provide taxable consultancy services pursuant to Section 8 of Service Tax Act, 1975	(i) This licence must be displayed at a safe and conspicuous place within the place of business. (ii) This licence must be submitted for amendment, renewal or cancellation, as the case may be, in accordance with the Service Tax Regulations 1975.	Met. Met.
Association Of The Computer And Multimedia Industry Malaysia ("PIKOM")	Approval of SCAN Associates application for membership in Pikom	Nil	Not Applicable.
Celcom (Malaysia) Berhad ("Celcom")	Registration of SCAN Associates with Celcom as a supplier of Information technology (IT) Hardware and Software, Small to Large Multi-user System & Services, Software product & services, Other computer related services, Networking product & Services, IT security equipment and Services, Professional Services and Information Technology (IT) Specialist.	Nil	Not Applicable.

As with other business, the Group's operations are subject to the government rules and regulation. Apart from the operation licence, there are no material government laws, regulations and policies that may impede on SCAN Group's performance and growth within a free enterprise environment.

SCAN Associates obtained MSC Pioneer Status in 2002. The MSC Pioneer status is valid for five years, after which they may be renewed subject to compliance. Among others, one of the main benefits of being an MSC Pioneer Status company is tax-free income.

4.2.4 Brand Names, Patents, Trade Marks, Licences, Technical Assistance Agreements, Franchises And Other Intellectual Property Rights

The following are the trademark, brand name and logo of SCAN Group.

ENTITY FOR BRANDING	LOGO, TRADE MARK AND/OR BRAND NAME
Cryptographic Software	TRUSTMatrix
Corporate Logo	"scan"

With the exception of some third party open source products bundled with its own in-house developed products, SCAN Group owns the intellectual properties for all its products, services and solutions. These also include the following product and packages:-

- Cryptoengine
- Cryptography System

SCAN Associates has submitted an application to register the mark "TRUSTMatrix" under Class 42 of the respective Trademark Acts/Regulations in Brunei, Indonesia, Malaysia and Singapore. As at the date hereof, the mark "TRUSTMatrix" has been registered in Brunei vide the certificate of registration dated 25 March 2006 and shall be valid until 26 May 2015.

In respect of the mark "scan", SCAN Associates has submitted an application to register under Class 42 of the respective Trademark Acts/Regulations in Brunei and Malaysia. An application for appeal has been submitted pursuant to Perbadanan Harta Intelek Malaysia's decision vide its letter dated 15 March 2006.

All the other applications are still pending the issuance of certificates of registration.

The source code to the base software and such related information is treated as copyright. As such, the Company should be able to avail itself to remedies for breach of copyright which include injunction, damages, accounts of profits and destruction orders.

The Group uses some Open Source softwares, which are free and does not require notification to the licensor of the software. Generally, the licensor disclaims all liabilities over any damages incurred from the usage of such application software. In order to mitigate this risk, the Group issues performance bond to its clients to assure its products performance. The Group is also considering further mitigation such as subscribing to professional indemnity insurance.

Some open source software licenses restrict the users' ability to commercialise the software. The Group manages these restrictions by developing and applying Plug-ins solution between the restricted software and the application developed by the Group. The solution enables the Group to distinguish and make known such restriction to the end users and licensees.

4.2.5 Dependency On Patents, Licences, Industrial, Commercial Or Financial Contracts And New Manufacturing Processes

As mentioned in Section 3(b), the Group is to an extent dependent on the protection of its proprietary intellectual properties.

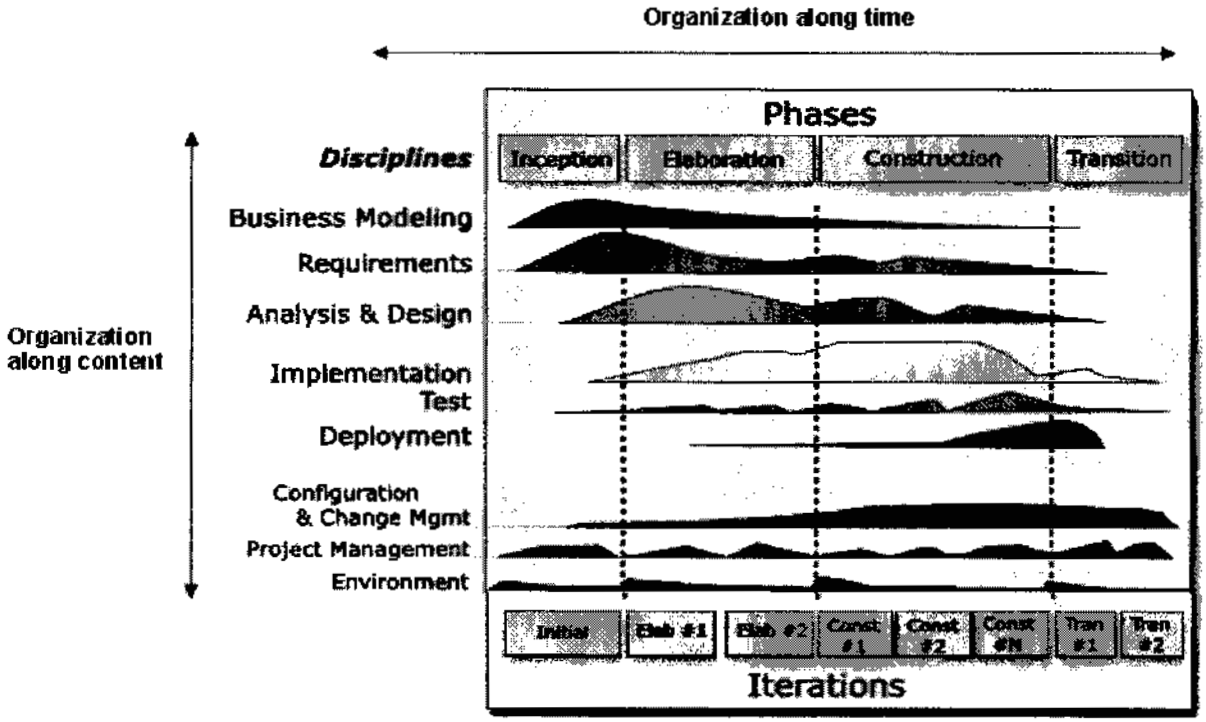
THE REST OF THIS PAGE IS INTENTIONALLY LEFT BLANK

4.2.6 Process Flow

4.2.6.1 Overview of the Development Case

The development case describes the development process that will be followed for the product development effort in any SCAN project.

This section describes how the process structure has been tailored. The Rational Unified Process is organised in both the time (the life cycle model, phases and iterations) and content (the disciplines to be used) as shown by the "iteration cycle graph" below:



Early iterations focus on requirement analysis and architectural design, whereas late iterations focus more on design, implementation, and testing.

The "iteration cycle graph" above illustrates typical proportions. Thus, part of the Iteration Plan is to decide how the various disciplines are to be exercised for each iteration.

(a) The Process Architecture

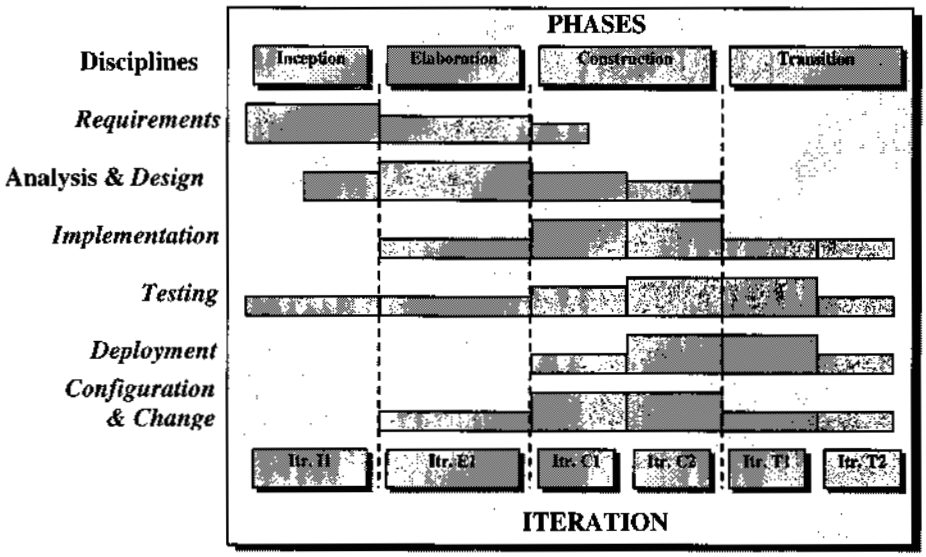
The process architecture adopted is that of the Rational Unified Process.

In this architecture there is a clear separation between the time dimension of a project (represented by the phases and milestones of the process lifecycle model, and the process components (the disciplines, workflow details, roles, activities, artefacts, templates and guidelines that define the static elements of the process).

4. INFORMATION ON THE GROUP *(Cont'd)*

(b) Lifecycle Model

The lifecycle adopted is based on the Rational Unified Process (RUP). It is tailored for any SCAN Group product development project as follows:



Lifecycle Model

In this tailored software lifecycle, it is advisable to iterate the RUP standard iteration.

To adapt to the Adaptive Software Development, the software is divided into release/version, cycle and build. One particular release consists of one or multiple cycles and one particular cycle consists of one or multiple builds.

One particular release is considered as either a system that has implemented all the required functionality or a system in a certain period of development stage or a system that has reached the end of the project, whichever comes first.

Client testing is not compulsory in each release but advisable, as each release is actually n^{th} number of the cycle. By the end of each cycle, end user testing is compulsory.

One particular cycle considered as a minor release will involve end user testing. Each cycle range from two to eight weeks depending on the requirements. For requirements that are ambiguous and volatile, the cycle duration could be as short as two weeks and for stable and clear requirements, the cycle duration could be as long as eight weeks. The first two cycles are mainly used to confirm the core requirements. At the end of each cycle, SCAN Group would undertake testing and this would be considered as acceptance testing.

A build is considered as the developer's view of the component. A new build is said to be ready when all are tested and components in the system are integrated and successfully compiled.

4. INFORMATION ON THE GROUP *(Cont'd)*

The duration of each build is not fixed. It depends on the size and complexity of the product development. The size and complexity of a product development does not affect the lifecycle.

The only difference between big and complicated product development and small and simple product development only lies on the number of cycles and builds. For a small and simple product, the cycle could be less then five and build could be less then ten. It all depends on the judgement of the product manager to plan and the involvement of the client at the beginning of the product development.

(c) Disciplines

The development-case for SCAN Group covers eight main disciplines:

- Requirements;
- Analysis and Design;
- Implementation;
- Testing;
- Release Management;
- Deployment;
- Configuration and Change Management; and
- Support.

The following table summarises the disciplines included in the process defined by this development case:

Discipline Configuration	Base/ Source Discipline	Comments
Requirements	RUP Discipline: Requirements	Produce only a subset of the artefacts.
Analysis and Design	RUP Discipline: Analysis & Design	Produce only a subset of the artefacts.
Implementation	RUP Discipline: Implementation	Produce only a subset of the artefacts.
Testing	RUP Discipline: Test	Produce only a subset of the artefacts.
Deployment	RUP Discipline: Deployment	Produce only a subset of the artefacts.
Release Management	Scan Standard	Nil
Configuration & Change Management	RUP Discipline: Configuration & Change Management	Based on the project standards & guidelines
Support	Scan Standard	Nil

Requirements

Requirement is defined as "a condition or capability to which a system must conform". The purpose of the Requirements Analysis discipline is as follows:-

- to provide better understanding of the system requirements;
- to define the boundaries of the system;
- to provide a basis for planning the technical contents of iterations;
- to provide a basis for estimating cost and time to develop the system; and

- to define a user-interface for the system, focusing on the needs and goals of the users.

To help explain the work involved in the Requirements discipline, we have organised the activities and artefacts into workflow details as shown below.

The workflow details are shown in a logical, sequential order. As indicated in the text above, they are applied continuously in varied order as needed throughout the project. Here they are shown in the sequence that you would most likely apply to the first iteration of a new project.

Analysis and Design

The purposes of the Analysis as follows:-

- to transform the requirements into a design of the system to be; and
- to ensure that the system's functional requirements are handled.

The purposes of the Design are as follows:-

- to adapt the results of analysis to the constraints imposed by non-functional requirements, the implementation environment, performance requirements, and so forth;
- refinement of analysis; and
- focuses on optimising the system's design while ensuring complete requirements coverage.

Therefore, the purpose of the analysis and design are as follows:-

- To translate the requirements into a specification that describes how to implement the system. The system designer/software designer/solution architect **must** first understand the requirements and transform the entire requirements into a system design by selecting the best implementation strategy; and
- To establish a robust architecture so that the system can easily understand, build and evolve.

The workflow details are shown in a logical, sequential order. As indicated in the text, they are applied continuously in varied order as needed throughout the project. Here they are shown in the sequence that you would most likely apply to the first iteration of a new project.

Implementation

Implementation is defined as "the implementation of the design". The purpose of implementation is:-

- to define the organisation of the code, in terms of implementation subsystems organised in layers;
- to implement the design elements in terms of implementation elements (source files, binaries, executables, and others);
- to test the developed components as units; and
- to integrate the results produced by individual implementers (or teams), into an executable system.

4. INFORMATION ON THE GROUP *(Cont'd)*

To help explain the work involved in the Implementation discipline, we have organised the activities and artefacts into workflow details as shown below.

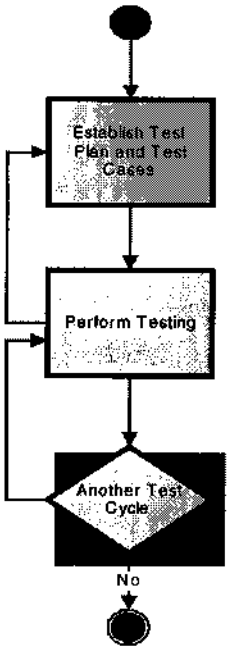
The workflow starts with structure the implementation and integration followed by implement components, integrate each subsystem, and finally integrate the system.

Testing

Testing is the means by which SCAN Group assesses the software product quality. The purpose of testing is to assess and report the findings regarding the level of quality achieved in the product. The test workflow involves:-

- verifying the interaction between objects and components;
- verifying the proper integration of all components of the software;
- verifying that all requirements have been correctly implemented; and
- identifying and ensuring that all discovered defects are addressed before software is deployed.

To help explain the work involved in the Testing discipline, we have organised the activities and artefacts into workflow details as shown below.



Testing Workflow

Deployment

The Deployment discipline describes the activities associated with ensuring that the software product is available for its end users.

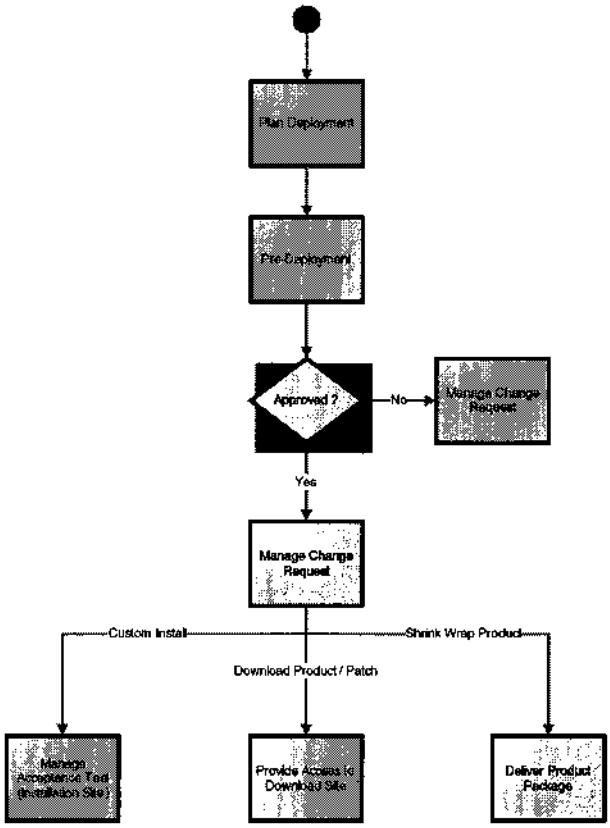
4. INFORMATION ON THE GROUP *(Cont'd)*

The Deployment discipline describes three modes of product deployment:-

- the custom install
- the 'shrink wrap' product offerings
- access to the software product over the internet

In each instance, there is emphasis on testing the product at the development site, followed by beta testing before the product is finally released to the customer.

To help explain the work involved in the Deployment discipline, the activities and artefacts have been organised into workflow details as shown below.



Deployment Workflow

Release Management

Release management is the final activity before the product is released. This will provide the information that links the problem to the source code of the system. It also makes sure that all marketing materials and related manuals are put into release. The activity also handles electronic release to different clients with different set of configurations.

Together with the release, the necessary supporting framework also needs to be established and put in place.

4. INFORMATION ON THE GROUP *(Cont'd)*

Release management typically manages two types of releases:-

- internal release (mainly for quality testing)
- product release, release for customers

All the internal and external releases have to be put under release management using the release version scheme provided. The result of the management would be the traceability of the release back to the specific version of a component, which has already included in the release.

Configuration and Change Management

Configuration and Change Management is the process, which controls the change of the artefacts and also maintains the integrity of the artefacts.

The purpose of the process is to control numerous artefacts produced by many people who join the project/program. It is mainly to avoid costly confusion or conflict of the following areas:-

- Simultaneous Update: A situation, which the same artefact gets modified or changed at the same time by different group of people with different change factors.

- Limited Notification: A situation where the changes do not get out to all the people involved in the project.

- Multiple Version: A situation where the artefacts are under different version for different state, such as production version, testing version, development version, etc.

It also benefits the project/program in areas such as:-

- Maintaining product integrity;
- Ensure completeness and correctness of the product;
- Provide stable development environment; and
- Provide traceability to what, why, who and when the changes were made.

Support

At the moment, SCAN Group only give support to the customer through email and phone. There are three level of product support:-

- First Level Support: First Level Support or Helpdesk will be the front person to assist the customer. He/she will be responsible to guide and to receive complains from the customer.

- Second Level Support: Second Level Support is high-level support, which incorporates testing and analysing the problems raised by the customer.

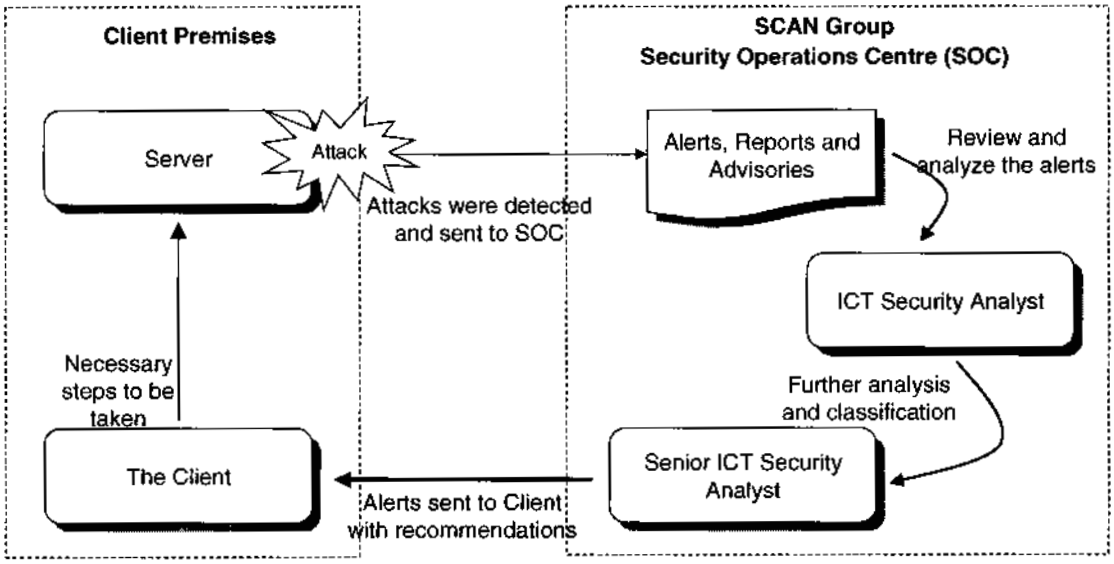
- Third Level Support: Third Level Support is the implementer of the solution. He/She is responsible for implementing the solution by modifying the programs.

Issue tracking System is used by all levels of support in order to manage and keep track the issues (bugs/problem) reported by the user.

4.2.6.2 Managed Security Services

SCAN Group provides Managed Security Services (MSS) which are outsourced by organisations who for reasons including lack of ICT Security skills and expertise, have decided to get a third party to be responsible for all or some of their ICT Security. SCAN Group is able to provide on-site or remote MSS. For on-site MSS, SCAN Group provides the expert personnel to be part of the management of ICT Security at the client's premises.

Whereas in remote MSS, SCAN Group uses its own in-house SOC and expert personnel to remotely monitor the Client's network security. The processes involve in MSS are depicted in the diagram below:-



Overview of Remote Security Monitoring Services Process

When there is an "attack" or an intrusion of any sort, SCAN Group's monitoring software will detect the intrusion and send alert to the console in the Security Operations Centre (SOC). The console is staffed by SCAN Group's ICT Security analysts 24 hours throughout the year. The ICT Security Analyst will review and analyse the alerts, and will confer with a Senior ICT Security Analyst for the best response. Once an appropriate response is determined, the ICT Security Analyst will inform the client about the intrusion and recommend appropriate action plan.

The client, on studying the recommendation will take the necessary action steps to counter the intrusion.

4.2.7 Estimated Market Coverage, Position and Share

Market Access

SCAN Group has gained market access into the Malaysian market and is currently developing the overseas markets especially in the Middle East, North Africa and South East Asia.