V skills
CERTIFIED
www.vskills.com

Certified Network Security Sample Material VS-1082

Vskills Certifications

Vskills Reading Material

Skills for a secure future

1. SECURITY PLANNING AND POLICY

A security policy is a document which lists plans to protect the physical and information technology (IT) assets and is continuously updated as technology and requirements change. It may include an acceptable use policy, a description of how to educate employees, security measurements to enforce and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

An information security management system (ISMS) is a collection of policies and procedures for management of crucial data. The aim is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security and data breach. An ISMS is usually focused on employee behavior and processes as well as particular type of data, such as customer data. ISO 27001 is a specification for creating an ISMS which does not mandate specific actions, but includes suggestions for documentation, internal audits, continual improvement, and corrective and preventive action.

Any good system of governance should be resilient to attacks by frauds, inadvertent virus, and a variety of motivated cyber crimes through unauthorized access and even to a nation-sponsored cyber war and in the scenarios of disaster and warfare.

1.1. Security Planning

In a world where conducting business online isn't optional, organizations can protect themselves by making a comprehensive security plan and seeing it through–just like they do for any other aspects of the operation.

Planning involves risk assessment f organization, identifying assets and their risks, enlisting threats and attacks to assets and planning to address the same.

Basic Risk Assessment

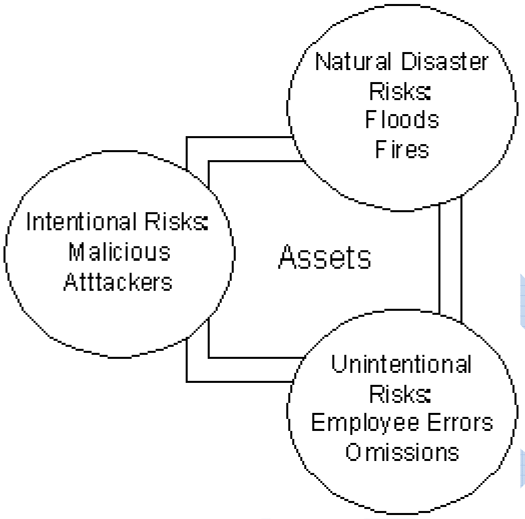
Risk assessment is a very important part of computer security planning. No plan of action can be put into place before a risk assessment has been performed. The risk assessment provides a baseline for implementing security plans to protect assets against various threats. There are three basic questions one needs to ask in order to improve the security of a system:

- ✓ What assets within the organization need protection?
- ✓ What are the risks to each of these assets?
- ✓ How much time, effort, and money is the organization willing to expend to upgrade or obtain new adequate protection against these threats?

You cannot protect your assets if you do not know what to protect against. Computers need protection against risks, but what are risks? In simple terms, a risk is realized when a threat takes advantage of a vulnerability to cause harm to your system. After you know your risks, you can then create policies and plans to reduce those risks.

There are many ways to go about identifying all the risks to your assets. One way is to gather personnel from within your organization and have a brainstorming session where you list the various assets and the risks to those assets. This will also help to increase security awareness within your organization.

Risks can come from three sources: natural disaster risks, intentional risks, and unintentional risks. These sources are illustrated in the following figure.


Natural Disaster Risks: Floods Fires
Intentional Risks: Malicious Atttackers
Assets
Unintentional Risks: Employee Errors Omissions

Companies are dynamic, and your security plan must be too. Update your risk assessment periodically. In addition, redo the risk assessment whenever you have a significant change in operation or structure. Thus, if you reorganize, move to a new building, switch vendors, or undergo other major changes, you should reassess the risks and potential losses.

Identifying the Assets

One important step toward determining the risks to assets is performing an information asset inventory by identify the various items you need to protect within your organization. The inventory should be based on your business plan and the sensitivity of those items. Consider, for example, a server versus a workstation. A server has a higher level of sensitivity than a typical user's workstation. Organizations should store the inventory online and categorize each item by its importance. The inventory should include everything that the organization would consider to be valuable. To determine if something is valuable, consider what the loss or damage of the item might be in terms of lost revenue, lost time, or the cost of repair or replacement. Some of the items that should be on your item inventory are:

Physical items

- ✓ Sensitive data and other information
- ✓ Computers, laptops, palmtops, etc.
- ✓ Backups and archives
- ✓ Manuals, books, and guides
- ✓ Communications equipment and wiring
- ✓ Personnel records

- ✓ Audit records
- ✓ Commercial software distribution media

Non-physical items

- ✓ Personnel passwords
- ✓ Public image and reputation
- ✓ Processing availability and continuity of operations
- ✓ Configuration information.
- ✓ Data integrity
- ✓ Confidentiality of information

For each asset, the following information should be defined:

- ✓ Type: hardware, software, data
- ✓ General support system or a critical application system
- ✓ Designated owner of the information
- ✓ Physical or logical location
- ✓ Inventory item number where applicable
- ✓ Service levels, warranties, key contacts, where it fits in to supplying availability and or security, and replacement process

Identifying Risks to the Assets

After identifying the assets, it is necessary to determine all the risks that can affect each asset. One way of doing this is by identifying all the different ways an asset can be damaged, altered, stolen, or destroyed. For example:

The asset:

- ✓ Financial information stored on a database system

The risks:

- ✓ Component failure
- ✓ Misuse of software and hardware
- ✓ Viruses, Trojan horses, or worms
- ✓ Unauthorized deletion or modification
- ✓ Unauthorized disclosure of information
- ✓ Penetration ("hackers" getting into your machines)
- ✓ Software bugs and flaws
- ✓ Fires, floods, or earthquakes
- ✓ Riots

In order to develop an effective information security policy, the information produced or processed during the risk analysis should be categorized according to its sensitivity to loss or disclosure. Most organizations use some set of information categories, such as Proprietary, For Internal Use Only, or Organization Sensitive. The categories used in the security policy should be consistent with any existing categories. Data should be broken into four sensitivity classifications with separate handling requirements: sensitive, confidential, private, and public. This standard data sensitivity classification system should be used throughout the organization. These classifications are defined as follows:

- ✓ Sensitive. This classification applies to information that needs protection from unauthorized modification or deletion to assure its integrity. It is information that requires a higher than normal assurance of accuracy and completeness. Examples of sensitive information include organizational financial transactions and regulatory actions.
- ✓ Confidential. This classification applies to the most sensitive business information that is intended strictly for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization, its stockholders, its business partners, and/or its customers. Health care-related information should be considered at least confidential.
- ✓ Private. This classification applies to personal information that is intended for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization and/or its employees.
- ✓ Public. This classification applies to all other information that does not clearly fit into any of the above three classifications. While its unauthorized disclosure is against policy, it is not expected to impact seriously or adversely affect the organization, its employees, and/or its customers.

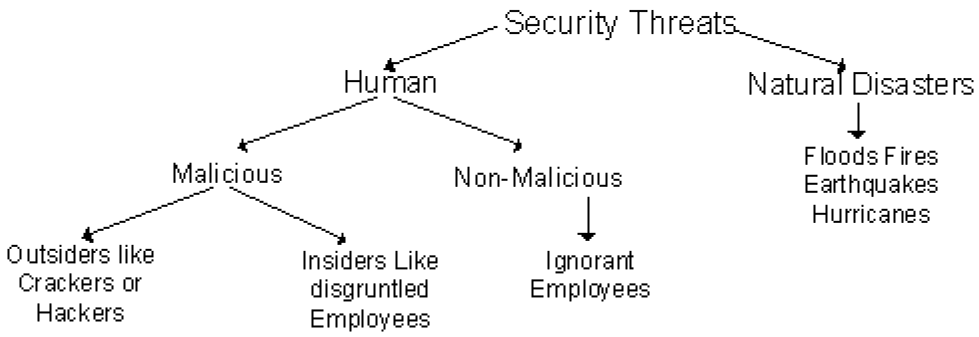
After identifying the risks and the sensitivity of data, estimate the likelihood of each risk occurring. Quantifying the threat of a risk is hard work. Some ways to estimate risk include:

- ✓ Obtaining estimates from third parties, such as insurance companies.
- ✓ Basing estimates on your records, if the event happens on a regular basis.
- ✓ Investigating collected statistics or published reports from industry organizations.
- ✓ Basing estimates on educated guesses extrapolated from past experience. For instance:
  - ✓ Your power company can provide an official estimate of the likelihood that your building will experience a power outage in the next year.
  - ✓ Past experience and best guess can be used to estimate the probability of a serious bug being discovered in your vendor software.

Once all the risks have been realized for each asset, it is necessary to identify whether the damage caused will be intentional or accidental.

Identifying Type of Threat and Method of Attack

A threat is any action or incident with the potential to cause harm to an organization through the disclosure, modification, or destruction of information, or by the denial of critical services. Security threats can be divided into human threats and natural disaster threats, as the following picture illustrates.



Human threats can be further divided into malicious (intentional) threats and non-malicious (unintentional) threats. A malicious threat exploits vulnerabilities in security policies and controls to launch an attack. Malicious threats can range from opportunistic attacks to well-planned attacks.

Non-malicious human threats can occur through employee error or ignorance. These employees may accidentally cause data corruption, deletion, or modification while trying to capture data or change information. (Hardware or software failures, while not a human threat, are other non-malicious threats.)

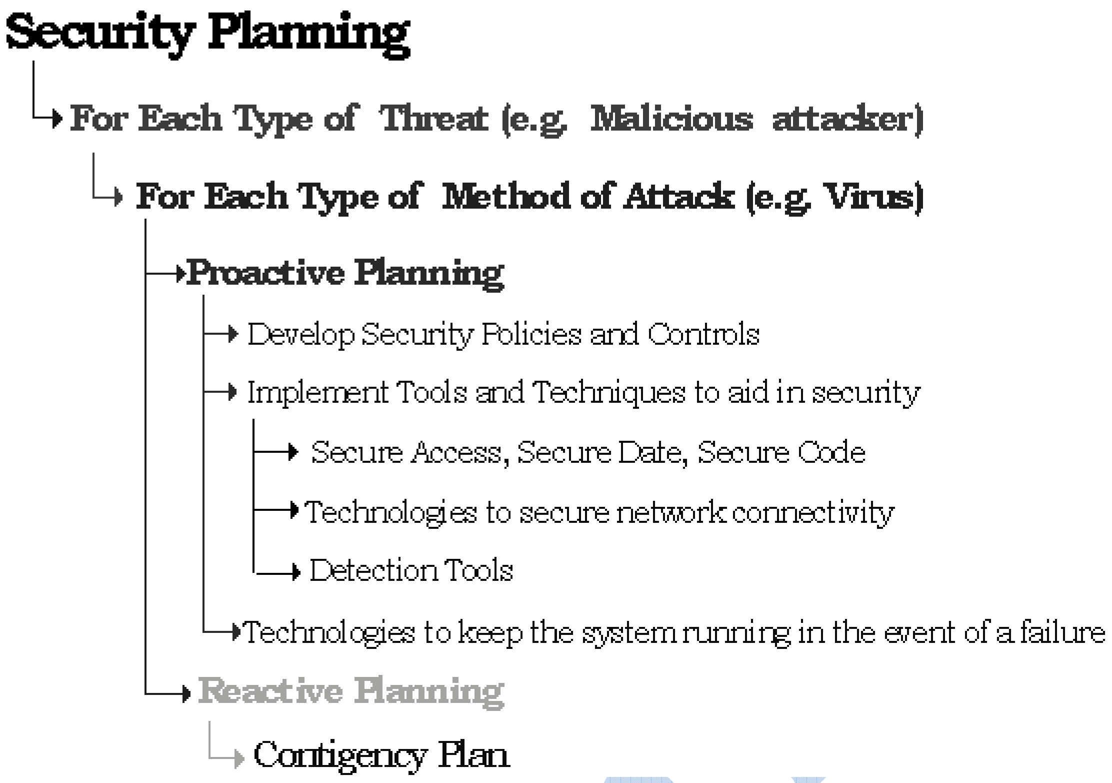
In understanding these various threats, it is possible to determine which vulnerabilities may be exploited and which assets are targeted during an attack. Some methods of attack include:

- ✓ Social engineering
- ✓ Viruses, worms, and Trojan horses
- ✓ Denial of service attack tools
- ✓ Packet replaying
- ✓ Packet modification
- ✓ IP spoofing
- ✓ Password cracking

Proactive Security Planning

After assessing your risk, the next step is proactive planning. Proactive planning involves developing security policies and controls and implementing tools and techniques to aid in security.

As with security strategies, it is necessary to define a plan for proactive and reactive security planning. The proactive plan is developed to protect assets by preventing attacks and employee mistakes. The reactive plan is a contingency plan to implement when proactive plans have failed.


Security Planning
For Each Type of Threat (e.g. Malicious attacker)
For Each Type of Method of Attack (e.g. Virus)
Proactive Planning
Develop Security Policies and Controls
Implement Tools and Techniques to aid in security
Secure Access, Secure Date, Secure Code
Technologies to secure network connectivity
Detection Tools
Technologies to keep the system running in the event of a failure
Reactive Planning
Contigency Plan

Reactive Security Planning

In reactive planning the goal is to get the business back to normal operations as fast as possible in the event of a disaster. By having efficient and well thought out contingency plans, this goal can be achieved.

Contingency Plan - A contingency plan is an alternative plan that should be developed in case an attack causes damage to data or any other assets, stopping normal business operations and productivity, and requiring time to restore them. The ultimate goal of the contingency plan is to maintain the availability, integrity, and confidentiality of data. It is the proverbial "Plan B." There should be a plan per type of attack and/or per type of threat. A contingency plan is a set of steps that should be taken in case an attack breaks through the security policies and controls. The plan should address who must do what, when, and where to keep the organization functional. For example:

- ✓ Moving productivity to another location or site
- ✓ Implementing disaster recovery plans.
- ✓ Contacting vendors and consultants
- ✓ Contacting clients
- ✓ Rehearsed the plan periodically to keep staff up to date with current contingency steps.

The following points outline the various tasks to develop a contingency plan:

- ✓ Address the organization's current emergency plan and procedures and how they are integrated into the contingency plan.

- ✓ The current emergency response procedures should be evaluated and their effect on continuous operation of business.
- ✓ Planned responses to attacks and whether they are adequate to limit damage and minimize the impact on data processing operations should be developed and integrated into the contingency plan.
- ✓ Backup procedures, including the most recent documentation and disaster recovery tests.
- ✓ Disaster recovery plans should be added to provide a temporary or longer operating environment. Disaster recovery plans should cover the required levels of security to see if they continue to enforce security throughout the process of recovery, temporary operations, and when the organization moves back to its original processing site or to the new processing site.

Draw up a detailed document outlining the various findings in the above tasks. The document should list:

- ✓ Any scenarios to test the contingency plan.
- ✓ The impact that any dependencies, assistance outside the organization, and difficulties in obtaining essential resources will have on the plan.
- ✓ A list of priorities observed in the recovery operations and the rationale in establishing those priorities.

A contingency plan should be tested and revised by someone other than the person who created and wrote it. This should be done to test whether the contingency plan is clearly outlined so that anybody who reads it can implement the plan.

Security Policy

A company's security plan consists of security policies. Security policies give specific guidelines for areas of responsibility, and consist of plans that provide steps to take and rules to follow to implement the policies.

Policies should define what you consider valuable, and should specify what steps should be taken to safeguard those assets. Policies can be drafted in many ways. One example is a general policy of only a few pages that covers most possibilities. Another example is a draft policy for different sets of assets, including e-mail policies, password policies, Internet access policies, and remote access policies.

Two common problems with organizational policies are:

- ✓ The policy is a platitude rather than a decision or direction.
- ✓ The policy is not really used by the organization. Instead it is a piece of paper to show to auditors, lawyers, other organizational components, or customers, but it does not affect behavior.

1.2. Security Policies and Guidelines

A security policy is driven by the corporate decisions regarding risk based on the business context. It is the result of determining what is at risk, and how to reduce that risk. The same set of threats and risks may be viewed as less severe by a more risk accepting organization. A security policy is a layers of policies, on top of procedures and practices. It is akin to a pyramid, with the top layer of being corporate security policy. It sets the high-level direction for the organization. It's scope is organization wide and represents a general statement of the security goals. This corporate policy is both static, and non-technical, being goal driven and not specifying technologies. It provides broad guidance for the organization, leaving more dynamic and technical details to lower policy layers.

Standards take the general goals and restates them in terms of specific technology areas. Below this are practices and procedures, the most technical and dynamic layers of policies. These represent the details needed to implement the overall security policy. Practices are detailed steps to implement the technology. Procedures are steps used to interface the technology with the environment (users, operators, and so on). At this layer the procedures may specify products and specific processes to be used. A standard would state a more specific requirement stating that a single sign-on technology is needed across all applications and systems. The practices and procedures would specify identity management and access control products, as well as processes to populate and manage users.

Types of Security Policies

Policies can be defined for any area of security. It is up to the security administrator and IT manager to classify what policies need to be defined and who should plan the policies. There could be policies for the whole company or policies for various sections within the company. The various types of policies that could be included are:

- ✓ Password policies with administrative responsibilities and user responsibilities
- ✓ E-mail policies
- ✓ Internet policies
- ✓ Backup and restore policies

Password Policies - The security provided by a password system depends on the passwords being kept secret at all times. Thus, a password is vulnerable to compromise whenever it is used, stored, or even known. In a password-based authentication mechanism implemented on a system, passwords are vulnerable to compromise due to five essential aspects of the password system:

- ✓ A password must be initially assigned to a user when enrolled on the system.
- ✓ A user's password must be changed periodically.
- ✓ The system must maintain a "password database."
- ✓ Users must remember their passwords.
- ✓ Users must enter their passwords into the system at authentication time.
- ✓ Employees may not disclose their passwords to anyone. This includes administrators and IT managers.

Password policies can be set depending on the needs of the organization. For example, it is possible to specify minimum password length, no blank passwords, and maximum and minimum password age. It is also possible to prevent users from reusing passwords and ensure that users use specific characters in their passwords making passwords more difficult to crack.

Administrative Responsibilities - Many systems come from the vendor with a few standard user logins already enrolled in the system. Change the passwords for all standard user logins before allowing the general user population to access the system. For example, change administrator password when installing the system.

The administrator is responsible for generating and assigning the initial password for each user login. The user must then be informed of this password. In some areas, it may be necessary to prevent exposure of the password to the administrator. In other cases, the user can easily nullify this exposure. To prevent the exposure of a password, it is possible to use smart card encryption in conjunction with the user's username and password. Even if the administrator knows the password, he or she will be unable to use it without the smart card. When a user's initial password must be exposed to the administrator, this exposure may be nullified by having the user immediately change the password by the normal procedure.

Occasionally, a user will forget the password or the administrator may determine that a user's password may have been compromised. To be able to correct these problems, it is recommended that the administrator be permitted to change the password of any user by generating a new one. The administrator should not have to know the user's password in order to do this, but should follow the same rules for distributing the new password that apply to initial password assignment. Positive identification of the user by the administrator is required when a forgotten password must be replaced.

User Responsibilities - Users should understand their responsibility to keep passwords private and to report changes in their user status, suspected security violations, and so forth. To assure security awareness among the user population, we recommend that each user be required to sign a statement to acknowledge understanding these responsibilities.

The simplest way to recover from the compromise of a password is to change it. Therefore, passwords should be changed on a periodic basis to counter the possibility of undetected password compromise. They should be changed often enough so that there is an acceptably low probability of compromise during a password's lifetime. To avoid needless exposure of users' passwords to the administrator, users should be able to change their passwords without intervention by the administrator.

E-mail Policies - E-mail is increasingly critical to the normal conduct of business. Organizations need policies for e-mail to help employees use e-mail properly, to reduce the risk of intentional or inadvertent misuse, and to assure that official records transferred via e-mail are properly handled. Similar to policies for appropriate use of the telephone, organizations need to define appropriate use of e-mail. Organizational polices are needed to establish general guidance in such areas as:

- ✓ The use of e-mail to conduct official business
- ✓ The use of e-mail for personal business
- ✓ Access control and confidential protection of messages
- ✓ The management and retention of e-mail messages

It is easy to have e-mail accidents. E-mail folders can grow until the e-mail system crashes. Badly configured discussion group software can send messages to the wrong groups. Errors in e-mail lists can flood the subscribers with hundreds of error messages. Sometime errors messages will bounce back and forth between e-mail servers. Some ways to prevent accidents are to:

- ✓ Train users what to do when things go wrong, as well as how to do it right.
- ✓ Configure e-mail software so that the default behavior is the safest behavior.
- ✓ Use software that follows Internet e-mail protocols and conventions religiously. Every time an online service gateways its proprietary e-mail system to the Internet, there are howls of protest because of the flood of error messages that result from the online service's misbehaving e-mail servers.

Using encryption algorithms to digitally sign the e-mail message can prevent impersonation. Encrypting the contents of the message or the channel that it's transmitted over can prevent eavesdropping. Using public locations like Internet cafes and chat rooms to access e-mail can lead to the user leaving valuable information cached or downloaded on to internet computers. Users need to clean up the computer after they use it, so no important documents are left behind. This is often a problem in places like airport lounges.

Internet Policies - The World Wide Web has a body of software and a set of protocols and conventions used to traverse and find information over the Internet. Through the use hypertext and multimedia techniques, the Web is easy for anyone to roam, browse, and contribute to.

Web clients, also known as Web browsers, provide a user interface to navigate through information by pointing and clicking. Browsers also introduce vulnerabilities to an organization, although generally less severe than the threat posed by servers. Various settings can set on Internet Explorer browsers by using Group Policy in Windows 2000.

Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. There are many areas of Web servers to secure: the underlying operating system, the Web server software, server scripts and other software, and so forth. Firewalls and proper configuration of routers and the IP protocol can help to fend off denial of service attacks.

Backup and Restore Policies - Backups are important only if the information stored on the system is of value and importance. Backups are important for a number of reasons:

- ✓ Computer hardware failure. In case certain hardware devices such as hard drives or RAID systems fail.
- ✓ Software Failure. Some software applications could have flaws in them whereby information is interpreted or stored incorrectly.
- ✓ User Error. Users often delete or modify files accidentally. Making regular backups can help restore deleted or modified files.
- ✓ Administrator Error. Sometimes administrators also make mistakes such as accidentally deleting active user accounts.
- ✓ Hacking and vandalism. Computer hackers sometimes alter or delete data.
- ✓ Theft. Computers are expensive and usually easily to sell. Sometimes a thief will steal just the hardware inside the computer, such as hard drives, video cards, and sound drivers.
- ✓ Natural disasters. Floods, earthquakes, fires, and hurricanes can cause disastrous effects on computer systems. Building can be demolished or washed away.
- ✓ Other disasters. Unforeseeable accidents can cause damage. Some examples are if a plane crashes into buildings or if gas pipes leak and cause explosions.

Information that should be backed up includes:

- ✓ Important information that is sensitive to the organization and to the continuity of operations. This includes databases, mail servers, and any user files.
- ✓ System databases, such as registries and user account databases.

Certifications

Accounting, Banking and Finance
– Certified AML-KYC Compliance Officer
– Certified Business Accountant
– Certified Commercial Banker
– Certified Foreign Exchange Professional
– Certified GAAP Accounting Standards Professional
– Certified Financial Risk Management Professional
– Certified Merger and Acquisition Analyst
– Certified Tally 9.0 Professional
– Certified Treasury Market Professional
– Certified Wealth Manager

Big Data
– Certified Hadoop and Mapreduce Professional

Cloud Computing
– Certified Cloud Computing Professional

Design
– Certified Interior Designer

Digital Media
– Certified Social Media Marketing Professional
– Certified Inbound Marketing Professional
– Certified Digital Marketing Master

Foreign Trade
– Certified Export Import (Foreign Trade) Professional

Health, Nutrition and Well Being
– Certified Fitness Instructor

Hospitality
– Certified Restaurant Team Member (Hospitality)

Human Resources
– Certified HR Compensation Manager
– Certified HR Stafffing Manager
– Certified Human Resources Manager
– Certified Performance Appraisal Manager

Office Skills
– Certified Data Entry Operator
– Certified Office Administrator

Project Management
– Certified Project Management Professional

Real Estate
– Certified Real Estate Consultant

Marketing
– Certified Marketing Manager

Quality
– Certified Six Sigma Green Belt Professional
– Certified Six Sigma Black Belt Professional
– Certified TQM Professional

Logistics & Supply Chain Management
– Certified International Logistics Professional
– Certified Logistics & SCM Professional
– Certified Purchase Manager
– Certified Supply Chain Management Professional

Legal
– Certified IPR & Legal Manager
– Certified Labour Law Analyst
– Certified Business Law Analyst
– Certified Corporate Law Analyst

Information Technology
– Certified ASP.NET Programmer
– Certified Basic Network Support Professional
– Certified Business Intelligence Professional
– Certified Core Java Developer
– Certified E-commerce Professional
– Certified IT Support Professional
– Certified PHP Professional
– Certified Selenium Professional
– Certified SEO Professional
– Certified Software Quality Assurance Professional

Mobile Application Development
– Certified Android Apps Developer
– Certified iPhone Apps Developer

Security
– Certified Ethical Hacking and Security Professional
– Certified Network Security Professional

Management
– Certified Corporate Goverance Professional
– Certified Corporate Social Responsibility Professional

Life Skills
– Certified Business Communication Specialist
– Certified Public Relations Officer

Media
– Certified Advertising Manager
– Certified Advertising Sales Professional

Sales, BPO
– Certified Sales Manager
– Certified Telesales Executive

& many more job related certifications

Contact us at :
Vskills
011-473 44 723 or **info@vskills.in**
www.vskills.com