One of Many Books in the Need to Know Series from BrainMass

EVERYTHING YOU NEED TO KNOW ABOUT

Performing a Network Risk ANALYSIS

By Rob Beachy

Ideal for Information Technology Professionals

BRAINMASS

www.brainmass.com

Everything You Need to Know About Performing a Network Risk Analysis

By Rob Beachy

What Is This Book?

Everything You Need to Know publications are the best way to get a quick but detailed overview of a specific topic. Within the pages of this book, you'll find exactly what you need in order to understand the key concepts of this topic. You'll find yourself completely prepared for the next stage of your learning as it relates to this topic. Within every book, we include a collection of the most important terms and their definitions so that whenever you're in need of a refresher, you can easily refer back and remind yourself of what you're dealing with.

Within this eBook you will learn the steps involved in performing a risk analysis and why they are important. A proper risk analysis will allow you and management to understand your technology assets and their vulnerabilities. You will also identify threats to your assets and steps to protect them.

This book is ideal for the Information Technology professional in charge of the operation and security of a network of any size. Individuals with the need to define their assets and proactively protect them from hostile threats in an ever growing technology landscape will benefit from reading this eBook.

Table of Contents

Introduction

Whether in the public or private sector, businesses rely on information systems to carry out their business functions. Information systems can range from simple office networks, financial and personnel systems to highly specialized systems, such as those found in the military. Information systems are vulnerable to threats that can have a negative impact on an organization's operations, assets and reputation. These threats, both known and unknown, take advantage of system vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. Threats can be calculated attacks, environmental interferences, and machine errors and can result in great harm to business continuity. It is a necessity that management, at all levels, understand their responsibilities and are held accountable for managing information security risk.

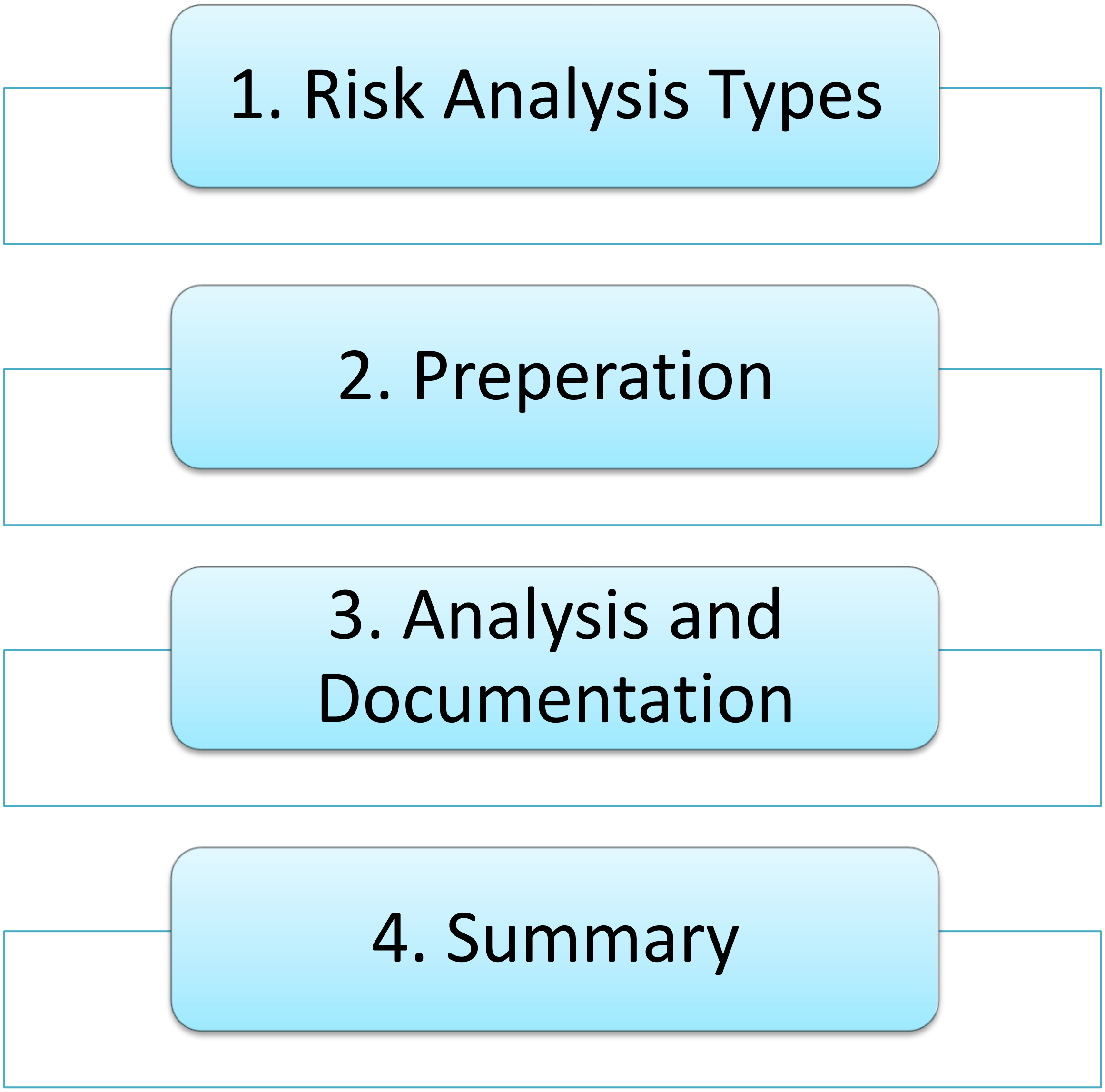
A Network Risk Analysis (NRA) is one of the key components of an organizational risk management process. A NRA will identify, prioritize, and estimate risk to an information system that may disrupt operations, assets, processes, and business continuity.
The purpose of a NRA is to identify:

- Threats to information systems
- Vulnerabilities internal and external to information systems
- Impact to business continuity that may occur given the potential for threats exploiting vulnerabilities
- The likelihood that harm will occur.

The end result (or benefit) of performing a risk analysis is the understanding of the level of risk within the network. NRAs are used to evaluate information system security related risks associated with corporate governance and management activities, mission/business processes or enterprise architecture, and funding of information security programs. NRAs are also used to support a corporate risk management framework (security categorization, security control selection, security control implementation, security control analysis, information system authorization, and monitoring).

Everything You Need to Know

This book is split into different sections or levels to make understanding important areas of the network risk analysis easier to comprehend. Within this eBook you will learn about the two types of risk analyses, how to prepare your risk analysis, and how to perform the risk analysis as well as document your findings.



1. Risk Analysis Types

2. Preperation

3. Analysis and Documentation

4. Summary

1. Risk Analysis Types

A network is comprised of material and non-material assets. Material assets include servers, switches, hubs, printers, and computers. Non-material assets are those assets that cannot be physically touched such as data. There are two distinctively different types of risk analyses that can be performed to help protect these assets: qualitative and quantitative. Each has its own distinct purpose and neither one is right or wrong. It is up to the individual performing the analysis to determine which is most beneficial in the realm of his/her own business strategy.

1.2 Qualitative

A qualitative risk analysis assesses the impact and likelihood of identified risks. A qualitative risk analysis takes into consideration the potential of occurrence and impact a risk has on the company's assets. A qualitative risk analysis focuses on three areas:

1. Inherent Risk
2. Controls/safeguards
3. Residual Risk

The combination of the inherent risk value together with the controls generates a residual risk level.

This approach assumes that the risk has an inherent value or score as opposed to a dollar figure and that this risk can be assessed under normal working conditions. A high risk score is not good; a low risk score is good.

When controls/safeguards are linked to a risk, it is saying that these controls are mitigating part of the risk. It is important to remember that it is not possible to mitigate 100 percent of a risk, but you need to find a point where management will accept the risk level.

Each control has a level of effectiveness – this describes how well the control is functioning in the management of the risk. A high measure is good; a low measure is not good.

The residual risk is calculated by querying the number of controls and each of their individual measures, and determining how much of the risk remains in the context of the control analysis. The goal is to bring the residual risk as close to zero as possible.

1.2.1 Impact

Impact describes the level of the impact to the company should the risk happen. An example scale of impact and scoring is shown in Table 1.

Table 1: Sample Scale of Impact

Category	**Score**
Not Significant	1
Low	2
Moderate	3
High	4
Catastrophic	5

Behind each Impact category lays a score between 1 and 5. A low impact category results in a lower score. The impact could be defined in varying ways depending on the company's structure or business needs. For example, the impact could represent financial impacts, infrastructure impacts, or business continuity impacts.

1.2.2 Likelihood

Likelihood describes the possibility the risk will occur. You can have a risk with a catastrophic impact, yet the likelihood of it occurring is rare. A sample likelihood table is shown in Table 2.

Table 2: Likelihood

Category	**Score**
Rare	1
Unlikely	2
Possible	3
Likely	4
Almost Certain	*5*

Behind each Impact category lays a score between 1 and 5. A low impact category results in a lower score. The Likelihood can be described as the frequency a risk may happen.

1.2.3 Inherent Risk Score

The Inherent Risk Score is a simple multiplication of Impact and Likelihood generating a score between 1 and 25. A sample Impact/Likelihood Impact matrix can be seen in Table 3.

Table 3: Sample Impact/Likelihood Matrix

	Impact				
	Not Significant	Minor	Moderate	Major	Catastrophic
Likelihood	1	2	3	4	5
Rare	1	2	3	4	5
Unlikely	2	4	6	8	10
Possible	3	6	9	12	15
Likely	4	8	12	16	20
Almost Certain	5	10	15	20	25

1.2.4 Controls/Safeguards

Controls and safeguards are mitigating factors that are put into place to offset the chances or impact a risk may have.

Examples of controls are antivirus software, firewalls, and locked doors. Anything that will lessen the chance or impact of a risk can be considered a control.

Controls, like likelihood and impact, also have a score. The higher the control's score the more effective that control is. A control may be used against different risks and may hold a different value for each risk. A control is represented as a percentage. For example: If the risk is the system being infected with a virus, antivirus software would be a control that may hold a value of 80 percent. This is to say that, by installing antivirus software, the risk is lowered by 80 percent leaving only 20 percent of its original inherent risk. The goals of controls are to mitigate the risk and reduce its inherent risk to as close to 0 as possible. In a calculation, it may be possible to bring a risk down to and below 0, but in reality you can never completely mitigate a risk.

It may be helpful to have a table that you can refer to for scores, but different controls may hold different scores based on the risk. If we use the previous example of the system being infected by a virus, a locked door to the server room may hold a mitigation value of 5 percent. This would be a different value if the risk were someone shutting down the servers. A locked door in this case may hold a value of 80 percent. A sample control effectiveness table is shown in Table 4.

Table 4: Sample Control Effectiveness

Control	**Effectiveness**
Control 1	12.5 percent
Control 2	12.5 percent
Control 3	15 percent
Combined Effectiveness	30 percent

1.2.5 Residual Risk

Residual risk is the amount of risk that is left after calculating the inherent risk and then taking into consideration the mitigating controls. Residual risk represents the actual risk. The table below shows an example of this calculation. The “Total Overall Control Effectiveness” column represents a combination of all the mitigating controls for that risk. The Residual Risk calculation is (Impact*Likelihood)*(100-controls). The 100 represents 100 percent risk. This is the risk of nothing is done to mitigate the risk and is always 100. A sample risk calculation table is shown in Table 5.

Table 5: Risk Calculation

Risk	**Impact**	**Likelihood**	**Inherent**	**Total Overall Control**	**Calcul ation**	**Residual**

				Effectiveness		
Risk 1	4	5	20	53.58 percent	20 * (100-53.58)	9.28

The final risk score is displayed as high, moderate, or low. A sample risk scoring table is shown in Table 6.

Table 6: Risk Scoring Table

Residual Risk	**Risk Category**
1-5	Low
6-15	Moderate
16-25	High

These categories and scores can be customized to match the requirements of each individual company.

1.2 Qualitative

In a quantitative risk analysis, the goal is to try to calculate the actual monetary value for each of the assets gathered during the risk analysis. For example, the value of each asset is estimated in terms of what it would cost to replace it, the cost in lost productivity, the cost to brand reputation, and other indirect costs if the asset was unavailable. This process requires the user to attempt to use the same objectivity when computing asset exposure, cost of controls, and all of the other values that are identified during the risk management process.

The input items from the quantitative risk analyses provide clearly defined goals and results. The following items generally are derived from the results of the risk analysis: 1) assignment monetary values for assets, 2) creation of a comprehensive list of significant threats, 3) identification of the probability of each threat occurring, 4) the loss potential for the company on a per threat basis annually, 5) the production of recommended safeguards, controls, and actions.

Assets must be identified and valued accurately to get a meaningful analysis. To determine the monetary value of an asset, which business executives rely on to decide the funds to use to protect an asset, you must calculate these three factors: 1) the overall value of the asset, 2) the immediate financial impact of losing the asset, 3) the indirect impact of losing the asset. To calculate these three factors it will be important to understand the several key items: the Single Loss Expectancy (SLE), Annual Rate of Occurrence (ARO), Annual Loss Expectancy (ALE), Cost of Controls, and the Risk on Security Investment (ROSI). These items are used together to determine the amount of risk on an asset in terms of monetary value.

1.2.1 Determining the Single Loss Expectancy (SLE)

The SLE is the total amount of revenue that is lost from a single occurrence of the risk. It is a monetary amount that is assigned to a single event that represents the company's potential loss amount if a specific threat exploits vulnerability. (The SLE is similar to the impact of a qualitative risk analysis.) The SLE is calculated by multiplying the asset value by the exposure factor (EF). The exposure factor represents the percentage of loss that a realized threat could have on a certain asset. If a web server has an asset value of $3,000, and a fire results in damages worth an estimated 25 percent of its value, then the SLE in this case would be $750. This is an oversimplified example and there likely would be other expenses that would need to be considered.

1.2.3 Determining the Annual Rate of Occurrence (ARO)

The ARO is the number of times that one may reasonably expect the risk to occur during a single year. With very little actuarial data available, making this estimate is very difficult. To estimate the ARO, companies must rely on past experience and/or consult security risk management experts and security and business consultants that may track this type of data.
The ARO is similar to the probability of a qualitative risk analysis.

1.2.3 Determining the Annual Loss Expectancy (ALE)

The ALE is the total amount of money that the company will lose in one year if nothing is done to mitigate the risk. This is calculated by multiplying the SLE by the ARO. The ALE is similar to the relative rank of a qualitative risk analysis. For example, if a fire at a business's web facility results in $5,000 in damages and ARO of a fire-taking place has an ARO value of 0.2

(indicating twice in ten years), and then the ALE value in this case would be $1,000 ($5,000 × 0.2 = $1,000).

The ALE provides a value that the company can work with to budget what it will cost to establish controls or safeguards to prevent this type of damage. It is important to quantify the possibility of a risk and how much damage, in monetary terms, the threat may cause in order to be able to know how much should be spent to protect against the potential consequence of the threat.

1.2.4 Determining the Cost of Controls

Determining the cost of controls requires accurate estimates on how much purchasing, testing, deploying, operating, and maintaining each control would cost. Such costs would include:

- Buying or developing the control
- Deploying and configuring the control
- Maintaining the control
- Contending with the loss of convenience or productivity that the control might impose.

For example, to reduce the risk of fire damaging a web farm, a company might consider deploying an automated fire suppression system. It would need to:

- Hire a contractor to design and install the fire suppression system
- Monitor the system on an ongoing basis
- Perform periodic preventative maintenance
- Recharge it with whatever chemical retardants the system uses.

1.2.5 Risk On Security Investment (ROSI)

The ROSI tries to validate the amount of money that is used to protect an asset. Estimate the cost of controls by using the following equation:
(ALE before control) - (ALE after control) - (annual cost of control) = ROSI
For example, the ALE of the threat of an attacker bringing down a web server is $12,000, and after the suggested safeguard is implemented, the ALE is valued at $3,000. The annual cost of maintenance and operation of the safeguard is $650, so the ROSI is $8,350 each year as expressed in the following equation: $12,000 - $3,000 - $650 = $8,350.

2. Preparation

Once you have determined the type of risk analysis that you are going to perform, the next step in conducting a NRA is to prepare for the analysis. The objective of this step is to establish a guideline for the risk analysis. During the preparation stage, steps such as gathering requirements for conducting the risk analysis, specific analysis methodologies to be employed, procedures for selecting risk factors to be considered, scope of the analysis, degree of formality, and requirements that facilitate consistent and repeatable risk determinations across the company are taken. Preparing for risk analysis includes the following specific tasks:

- Identifying the purpose
- Identifying the scope
- Identifying vulnerabilities, loss types and threats

2.1 Identifying the Purpose

Identify the purpose of the risk analysis requires the defining the risk analysis in terms of the information the analysis is intended to produce and the decisions the analysis is intended to support.

Once the purpose is defined, the individuals performing the risk analysis will have sufficient detail in order to fully conduct the analysis and can be assured that the purpose will be achieved. The purpose of the risk analysis is influenced by whether the analysis is:

- An initial analysis
  - Establishing a baseline
  - Identifying threats and vulnerabilities, impacts to company operations and assets, and other risk factors to be monitored or tracked over time as part of risk monitoring.
- An annual review (update)
  - Ongoing determinations of the effectiveness of security controls
  - Changes to organizational information systems or environments (example: changes to hardware, firmware, software; changes to controls; changes to mission/business processes, common infrastructure and support services, threats, vulnerabilities, or facilities.
  - Results from compliance verification activities

2.2 Identifying the Scope

The scope of the risk analysis determines the limitations of the analysis. Risk analysis scope affects the amount of information available to make risk-based decisions and is determined by the area being analyzed. The scope identification will determine what assets the risk analysis will consist of. These will be the assets that will have vulnerabilities, threats and controls/safeguards applied to during the analysis phase. Assets can include, but are not limited to: people and skills, goodwill, hardware, software, data, documentation, supplies physical equipment, and money. Establishing the scope of risk analysis helps a company determine:

- What business areas and assets are being addressed in the risk analysis (example: Information Technology, Accounting, etc)
- What parts of company are affected by the risk analysis and how are they affected
- What decisions will the risk analysis results support (control financing, purchasing of additional safeguards)
- How long the risk analysis results are relevant
- What triggers an update to the risk analysis?

2.3 Identifying Vulnerabilities, Loss Types, Controls, and Threats

Once the assets have been identified, all of the vulnerabilities and associated threats need to be identified for each. The individuals performing the analysis need to identify the vulnerabilities that could affect each asset's integrity, availability or confidentiality. All of the relevant vulnerabilities need to be identified and documented so that the necessary countermeasures can be implemented. A list of common vulnerabilities can be found in Appendix A.

After determining assets vulnerabilities, a list of threats that could take advantage of those vulnerabilities can be compiled. For a list of common threats see Appendix B.

After vulnerabilities and threats are identified, the next step is to determine the types of losses that could occur of the risk to the asset was to take place. A common list of loss types can be found in Appendix C.

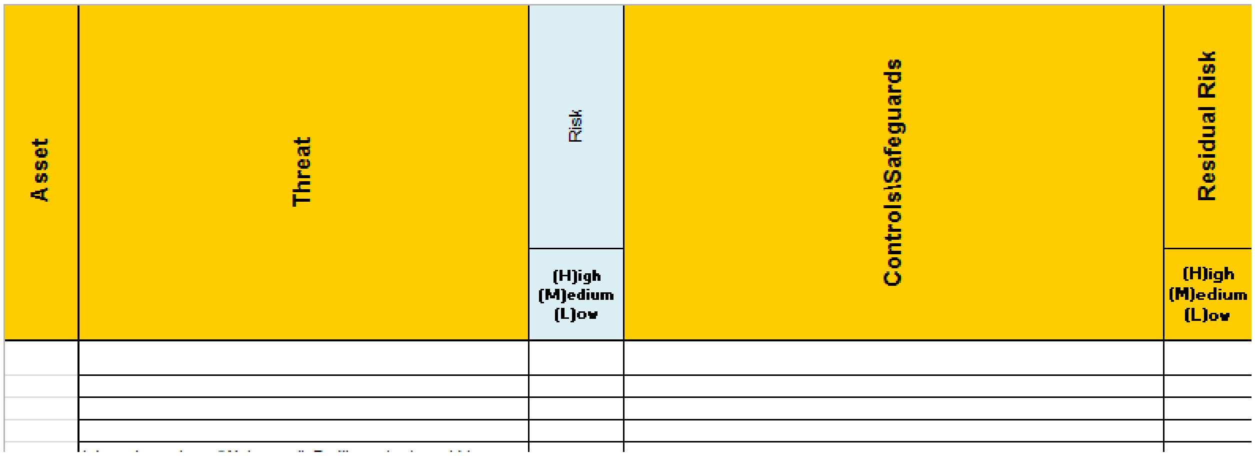
Since there is a large amount of vulnerabilities and threats that can affect the different assets, it is important to be able to properly categorize them. The goal is to determine which threats and vulnerabilities could cause the most damage so that the most critical items can be taken care of first. This is the point of developing mitigating controls and safeguards. A list of common controls can be found in Appendix D.

3. Analysis and Documentation

Now that you have decided the type of risk analysis you are performing (qualitative or quantitative), compiled all the data on assets, vulnerabilities, threats, and controls/safeguards, the only thing left to do is to analyze your data and document your findings in a format that can be presented to management.

There is no standard format that the documentation must be compiled in. During the "Defining the Purpose" phase, the information the analysis was intended to produce and the decisions the analysis was intended to support were defined. This will help in the documentation of the results. Many risk analyses are documented in a spreadsheet format. Although using a spreadsheet format is typical, it is not required. Management may have a specific format that they wish to see the documentation in and may, or may not; require a written report to accompany the spreadsheet. An example of a risk analysis spreadsheet is shown in Figure 1. Documentation required is often dictated by management. When no direction is supplied as to the required output, the documentation should list, at a minimum, the assets being analyzed, threats to those assets, controls linked to the asset, and residual risk.

If needed, you can also supply the background data you compiled during the early phases of the risk analysis.



Asset	Threat	Risk	Controls\Safeguards	Residual Risk
		(H)igh (M)edium (L)ow		(H)igh (M)edium (L)ow

Figure 1: Sample Risk Analysis Spreadsheet

4. Summary

Additional security almost always involves additional expense. As this does not directly generate income, it often needs to be justified in financial terms. The Risk Analysis process can directly generate such justification for security recommendations

Regardless if you use a qualitative or quantitative risk analysis, it should result in an easy to understand document that can be used and understood by employees and managers at every level. A network risk analysis can enable security to become part of the enterprises culture, allowing management to take more of the responsibility for ensuring an adequate and appropriate level of security.

A major benefit of the application of Risk Analysis is that it brings a consistent and objective approach to all security reviews. This not only applies across different applications, but different types of business systems.

It should also embrace those systems not under the direct control of IT management...paper based systems, PC Systems, or systems utilizing other office equipment.

Glossary

ALE – Annual Loss Expectancy. The amount of money a company would lose annual if the risk is not mitigated.

ARO - The number of times that one may reasonably expect the risk to occur during one year.

Asset – Any item of value.

Exposure Factor - represents the percentage of loss that a realized threat could have on a certain asset.

Impact – The result to business operations if a risk occurs.

Residual Risk – The remaining risk after factoring in controls/safeguards.

Risk – The possibility of a threat taking advantage of an asset's vulnerability.

Risk Analysis - The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.

SLE – Single Loss Expectancy. The total amount of revenue that is lost from a single occurrence of the risk.

Threat – The potential for a threat-source to exercise a specific vulnerability.

Vulnerability - A flaw or weakness in system security procedures, design, implementation or internal controls that could be exercised and result in a security breach or a violation of the system's security policy.

Additional Resources

20 Critical Security Controls: http://www.sans.org/critical-security-controls/cag3_1.pdf

Common Vulnerability Scoring System: http://www.first.org/cvss/v1/guide

Microsoft Threat Research and Response: http://www.microsoft.com/security/portal/

RAIS: http://rais.ornl.gov/

Threat Analysis Modeling: http://www.cert.org/octave/

United States Computer Emergency Readiness Team: http://www.us-cert.gov/

Appendix A

Vulnerabilities

System Access Control
Accountability
Administration
Applications
Audit Trails
Compliance
Data Integrity
Disclosure
Documentation
Emergency/Incident Response
Evaluation
Fire Suppression/Smoke Evacuation
Information Classification
Maintenance
Management/Organization
Policies & Standards
Procedures
Training, General
Security Controls
Security Incident Management
Risk Management Program
Communications
Configuration Management
Data Backup/Storage
Device & Media Control
Disaster Recovery Plan
Contingency Planning
Facility Physical Security
Privacy and GLBA
Security Awareness & Training
Authentication
Security Planning
Personnel

Appendix B

Threats

Air Conditioning Failure
Chemical/Biological Contamination
Blackmail
Bomb Threats
Cold/Frost/Snow
Communications Loss
Computer Intrusion
Data Destruction
Data Disclosure
Data Integrity Loss
Denial of Service Attacks
Earthquakes
Eavesdropping/Interception
Fire, False Alarm
Fire, Major
Fire, Minor
Flooding/Water Damage
Fraud/Embezzlement
Hardware Failure
Malicious Code
Computer Misuse
Power Loss
Sabotage/Terrorism
Storms/Hurricanes
Substance Abuse
Theft of Assets
Theft of Data
Vandalism/Rioting
Errors, Configuration
Errors, Data Entry
Burglary/Break In/Robbery
Identity Theft

Appendix C

Loss Types

Delays/Denials
Direct Loss (Financial)
Intangibles/Reputation
Modification
Indirect Loss
Legal

Appendix D

Controls\Safeguards

Physical Access Control
Application Controls
Audit Trails
Classification Markings
Contingency /Disaster Recovery Plan
Contract Specifications
Encryption
Detection Systems
Documentation
Electrical Power
Emergency Response
File/Program Control
Fire Suppression
Grounding Systems
Insurance
Life Cycle Management
Material Segregation
Monitoring/Intrusion Detection System
New Construction
Operating Procedures
Organizational Structure
Passwords/Authentication
Personnel Clearances
Personnel Control
Preventive Maintenance
Property Management
Redundant Power
Risk Analysis
Security Classification
Security Plan
Security Policy
Security Staff
System Validation
Technical Surveillance
Training
Visitor Control
Authentication
Anti-Virus Software
Firewall, Hardware
Firewall, Software
Data Backup
Off-site Storage
Redundant Facility/Hot-site
Biometrics
Change Control
Continuity Plan
Incident Response
Intrusion Detection
Personnel Security

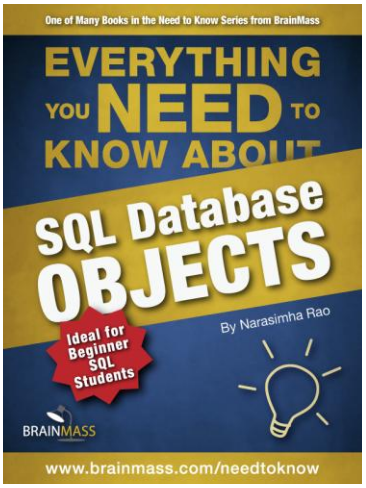
About the Author

Rob Beachy is the current Vice President of Information Technology for a community bank located in Michigan. He received his Bachelor’s degree in Information Systems from the University of Phoenix, graduating with a perfect 4.0 GPA. He went on to obtain a Master of Science in Information Assurance from Davenport University in Grand Rapids, Michigan with a GPA of 3.96.

Mr. Beachy holds certification in Novell, Microsoft, and holds a CompTIA Security+ certification. He is an active BrainMass expert and enjoys sharing his knowledge with lifelong learners. Mr. Beachy has completed a National Security Systems Information Systems Security (INFOSEC) professional’s course in 2010.

More eBooks from BrainMass

There are a number of other books in the BrainMass eBook Library. Here are a selection that you might be interested in:



One of Many Books in the Need to Know Series from BrainMass

EVERYTHING YOU NEED TO KNOW ABOUT

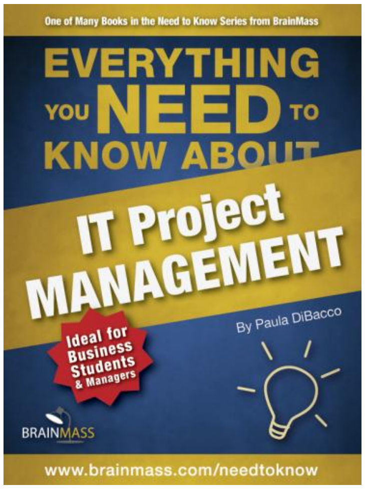
SQL Database OBJECTS

Ideal for Beginner SQL Students

By Narasimha Rao

BRAINMASS

www.brainmass.com/needtoknow



One of Many Books in the Need to Know Series from BrainMass

EVERYTHING YOU NEED TO KNOW ABOUT

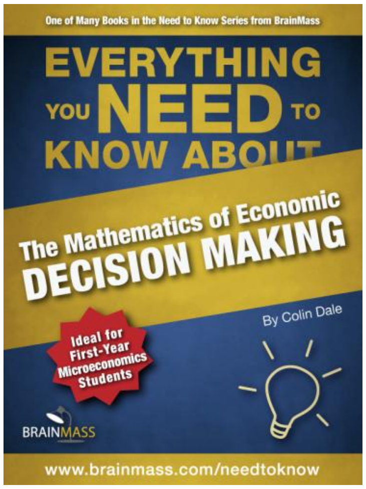
IT Project MANAGEMENT

Ideal for Business Students & Managers

By Paula DiBacco

BRAINMASS

www.brainmass.com/needtoknow



One of Many Books in the Need to Know Series from BrainMass

EVERYTHING YOU NEED TO KNOW ABOUT

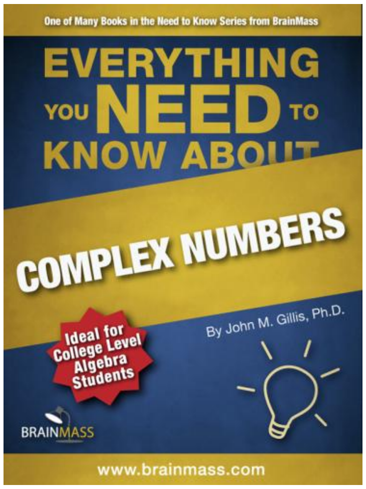
The Mathematics of Economic DECISION MAKING

Ideal for First-Year Microeconomics Students

By Colin Dale

BRAINMASS

www.brainmass.com/needtoknow



One of Many Books in the Need to Know Series from BrainMass

EVERYTHING YOU NEED TO KNOW ABOUT

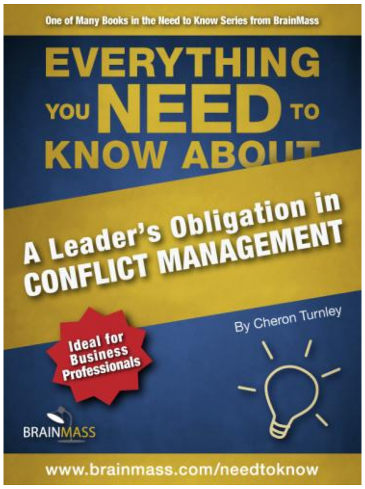
COMPLEX NUMBERS

Ideal for College Level Algebra Students

By John M. Gillis, Ph.D.

BRAINMASS

www.brainmass.com



One of Many Books in the Need to Know Series from BrainMass

EVERYTHING YOU NEED TO KNOW ABOUT

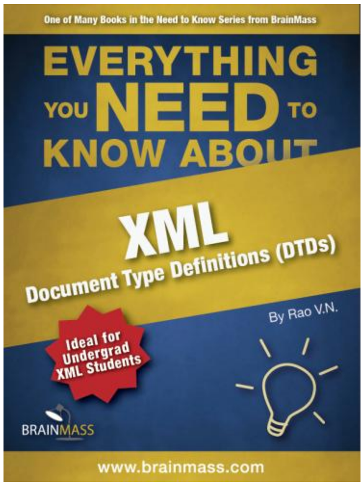
A Leader's Obligation in CONFLICT MANAGEMENT

Ideal for Business Professionals

By Cheron Turnley

BRAINMASS

www.brainmass.com/needtoknow



One of Many Books in the Need to Know Series from BrainMass

EVERYTHING YOU NEED TO KNOW ABOUT

XML Document Type Definitions (DTDs)

Ideal for Undergrad XML Students

By Rao V.N.

BRAINMASS

www.brainmass.com

To read more about these books and more, click on the link below:

http://brainmass.com/ebooks