Unit 3 - Risk Management

1. Introduction
2. An Overview of Risk Management
3. Risk Identification
4. Risk Assessment
5. Risk Control strategies
6. Selecting a Risk Control Strategy
7. Quantitative versus Qualitatative Risk Control Practices
8. Risk Management Discussion Points ,Recommended Risk Control Practices
9. Record Layer Protocol

Introduction

Definition- Risk management process is a framework for the actions that need to be taken ,It begins with identifying risks, goes on to analyze risks, then the risk is prioritized, a solution is implemented, and finally, the risk is monitored.

Five steps- Risk management process are identification, assessment, mitigation, monitoring, and reporting risks

Three types-Business Risk, Non-Business Risk, and Financial Risk.

Two ways to reduce- prevention and control

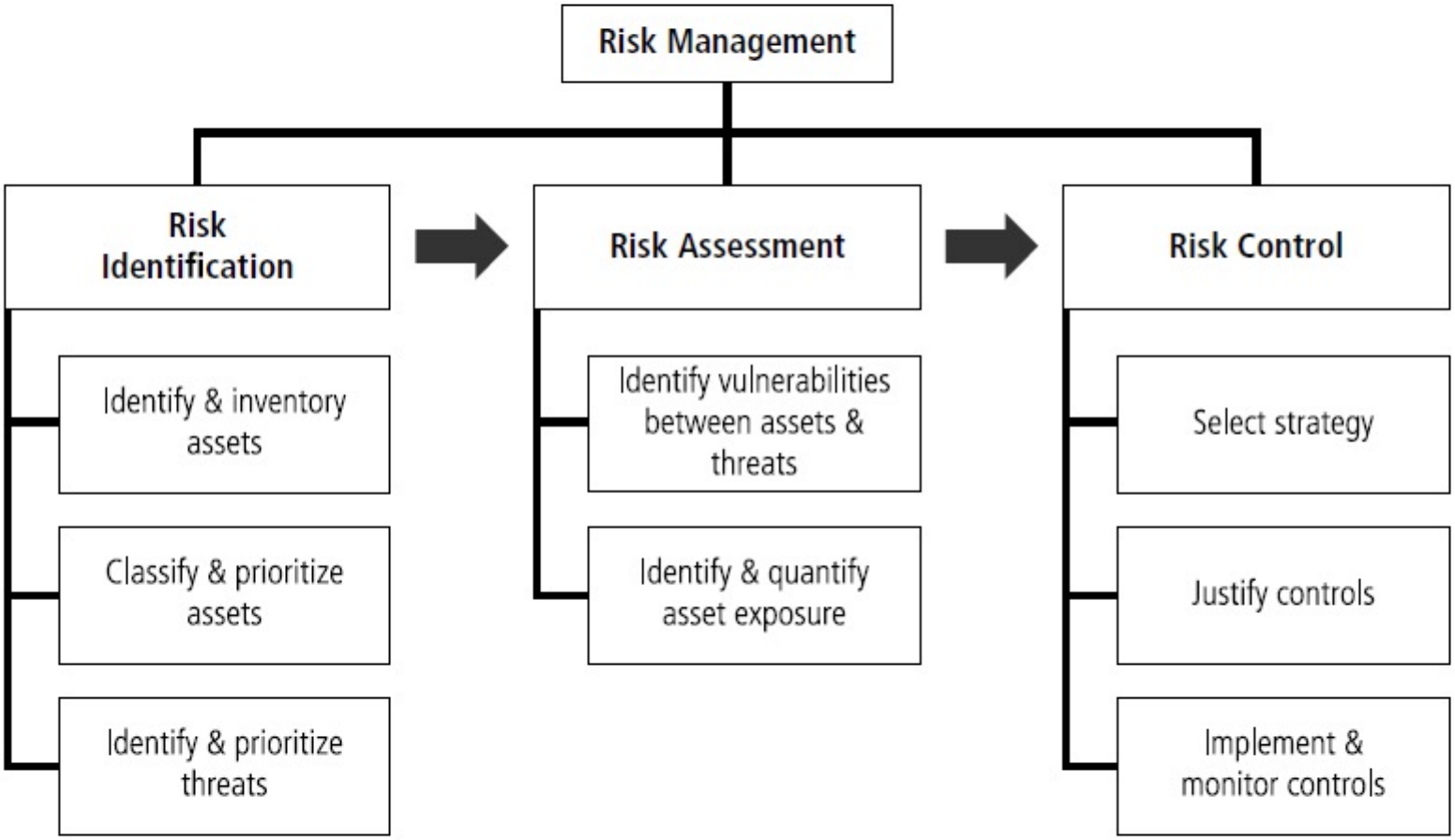
Risk management involves three major undertakings: risk identification, risk assessment, and risk control.

Risk identification is the examination and documentation of the security posture of an organization's information technology and the risks it faces.

Risk assessment is the determination of the extent to which the organization's information assets are exposed or at risk.

Risk control is the application of controls to reduce the risks to an organization's data and information systems.

Components of Risk Management

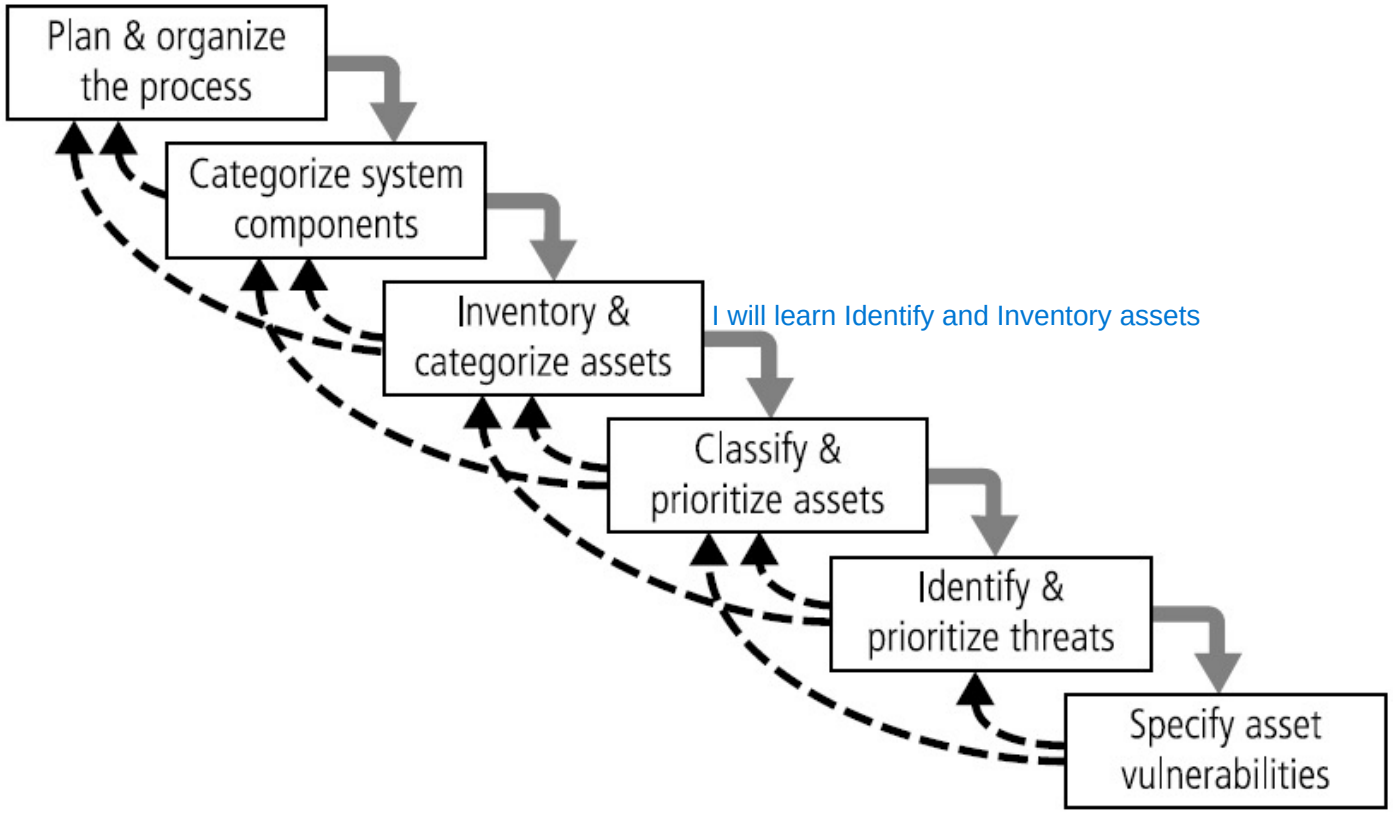


Communities of interest are also responsible for the following:

- Evaluating the risk controls
- Determining which control options are cost effective for the organization
- Acquiring or installing the needed controls
- Ensuring that the controls remain effective

Risk Identification

Once the Organizational assets have been identified, a threat assessment process identifies and quantifies the risks facing each asset.



Plan and organize process -> categorize system components -> Asset identification and inventory or Identify Assets and inventory -> CLassify assets and prioritize them-> Identify threats and prioritize them -> specify asset vulnerabilities

Asset identification and inventory
Classify assets and prioritize them

Plan and Organize the Process

Asset Identification and Inventory

Classifying and Prioritizing Information Assets

Information Asset Valuation

Identifying and Prioritizing Threats

Vulnerability Identification

Aakhiri mein ye bata do ki mareez ko kya problem ho sakti hai? i.e Specify Asset vulnerabilities

Plan and Organize the Process

Follow - project management principles

Risk can exist everywhere in the organization, representatives will come from every department from users, to managers, to IT and info-sec groups

The process must then be planned out, with periodic deliverables, reviews, and presentations to management. Once the project is ready to begin, a meeting

Organization ready to actually begin the next step—identifying and categorizing assets

Asset Identification and Inventory

Traditional System Components	SesSDLC Components	Risk Management System Components
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

Data Classification and Management

Confidential: Used for the most sensitive corporate information controlled, even within the company.

Internal: only by corporate employees, authorized contractors,

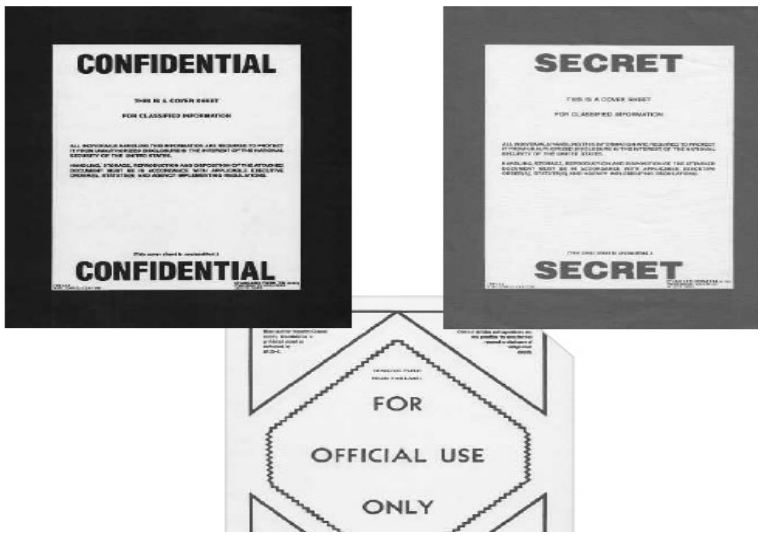
and other third parties.

External: All information that has been approved by management for public release.

Management of Classified Data

*Clean desk policy

*Dumpster diving



Information Asset Valuation

System Name: SLS E-Commerce
Date Evaluated: February 2012
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2—Supplier orders (outbound)	Confidential	High
EDI Document Set 2—Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Information Asset Prioritization

Information Asset	Criteria 1: Impact to Revenue	Criteria 2: Impact to Profitability	Criteria 3: Impact to Public Image	Weighted Score
Criterion Weight (1-100) Must total 100	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Identifying and Prioritizing Threats

Threat	Example
Compromises to intellectual property	Piracy, copyright infringement
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail of information disclosure
Missing, inadequate, or incomplete controls	Software controls, physical security
Missing, inadequate, or incomplete organizational policy or planning	Training issues, privacy, lack of effective policy
Quality of service deviations from service providers	Power and WAN quality of service issues
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of property

Vulnerability Identification

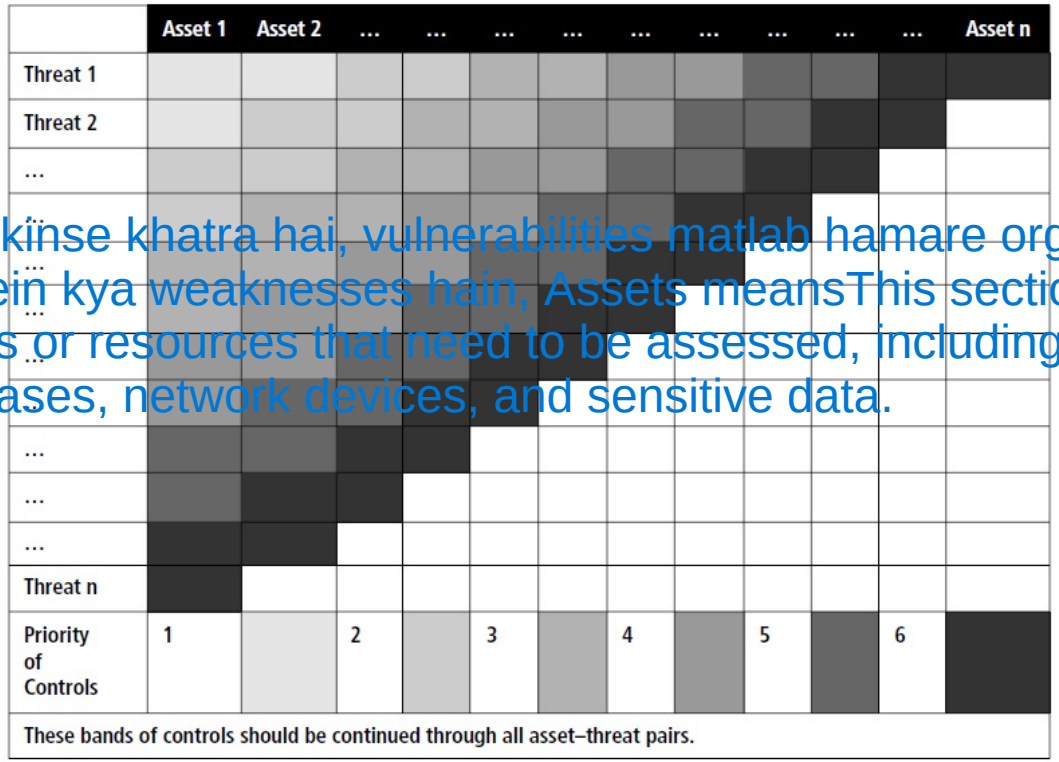
Categories of Threats Ranked by Greatest to Least Threat	2009 Ranking	2003 Ranking
Espionage or trespass	1	4
Software attacks	2	1
Human error or failure	3	3
Missing, inadequate, or incomplete organizational policy or planning	4	—
Missing, inadequate, or incomplete controls	5	—
Theft	6	7
Compromises to intellectual property	7	9
Sabotage or vandalism	8	5
Technical software failures or errors	9	2
Technical hardware failures or errors	10	6
Forces of nature	11	8
Quality of service deviations from service providers	12	10
Technological obsolescence	13	11
Information extortion	14	12

Threats-vulnerabilities-assets (TVA) worksheet

Threats-vulnerabilities-assets (TVA) worksheet in preparation for the addition of vulnerability and control information during risk assessment.

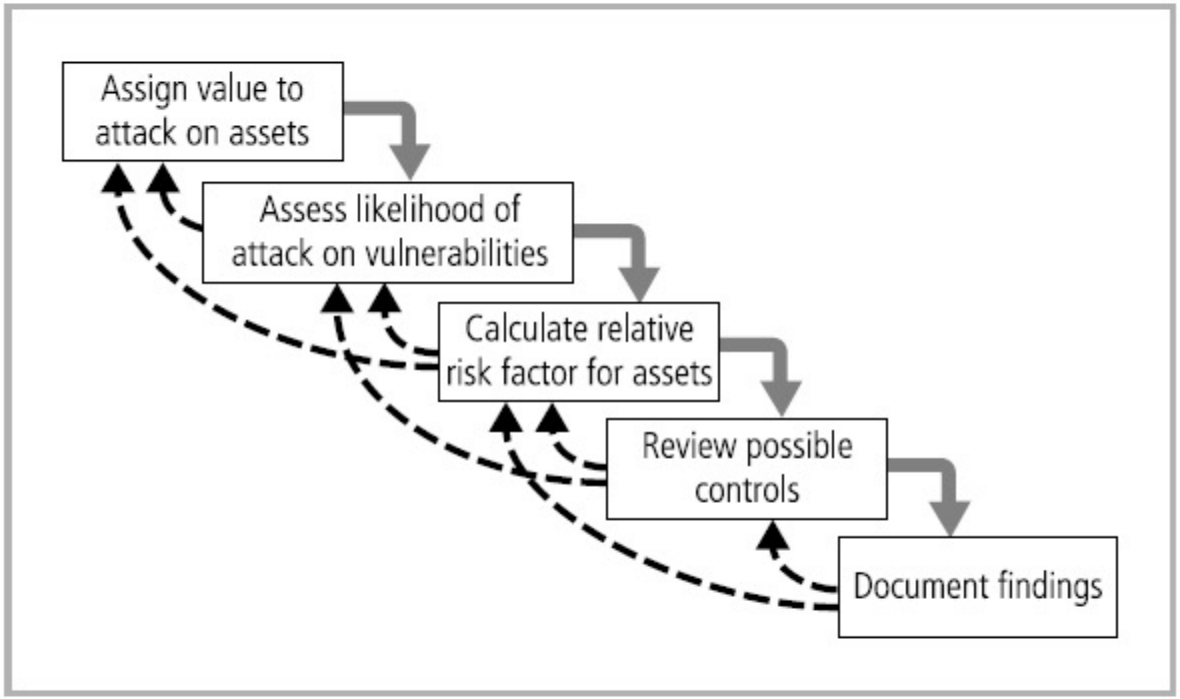
T1V1A1—Vulnerability 1 that exists between Threat 1 and Asset 1

T2V1A1—Vulnerability 2 that exists between Threat 2 and Asset 1 … and so on.



Threats matlab kinse khatra hai, vulnerabilities matlab hamare organization ke environment mein kya weaknesses hain, Assets meansThis section lists all the important assets or resources that need to be assessed, including hardware, software, databases, network devices, and sensitive data.

Risk Assessment



Likelihood

Risk Determination

Identify Possible Controls

Documenting the Results of Risk Assessment .

Likelihood

Between 0.1 (low) and 1.0 (high)

The likelihood of a fire has been estimated actuarially for each type of structure.

The likelihood that any given e-mail contains a virus or worm has been researched.

The number of network attacks can be forecast based on how many assigned network addresses the organization has.

Risk Determination

Risk Determination provides a quantitative **risk** value representing the systems exposure to a **threat** exploiting a particular vulnerability after current controls have been considered.

This quantitative value is in the form of a **Risk** Score.

A **risk** score basically follows the following

formula: **RISK**= IMPACT x LIKELIHOOD.

Documenting the Results of Risk Assessment

Asset: List each vulnerable asset.

Asset Impact: Show the results for this asset from the weighted factor analysis worksheet.In the example, this is a number from 1 to 100.

Vulnerability: List each uncontrolled vulnerability.

Vulnerability Likelihood: State the likelihood of the realization of the vulnerability by a threat agent, as noted in the vulnerability analysis step. In the example, the number is from 0.1 to 1.0.

Risk-Rating Factor: Enter the figure calculated from the asset impact multiplied by likelihood. In the example, the calculation yields a number from 1 to 100.

The ranked vulnerability risk worksheet is the initial working document for the next step in the risk management process: assessing and controlling risk.

Identify Possible Controls

create a preliminary list of potential controls.

There are three general categories of controls: **policies, programs, and technologies**

Policies are documents that specify an organization's approach to security. There are four types of security policies: general security policies, program security policies, issue-specific policies, and systems-specific policies.

Programs are activities performed within the organization to improve security. These include security education, training, and awareness programs.

Technologies are the technical implementations of the policies defined by the organization.

Asset	Asset Impact or Relative Value	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Web server denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.01	1

Table 4-9 Ranked Vulnerability Risk Worksheet

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns ranked value of risk rating for each uncontrolled asset-vulnerability pair

Table 4-10 Risk Identification and Assessment Deliverables

Risk Control Strategies

Development has created the ranked vulnerability worksheet, the team must choose one of five basic strategies to control each of the risks that result from these vulnerabilities.

The five strategies are defend, transfer, mitigate, accept, and terminate

Defend

Attempts to prevent the exploitation of the vulnerability.

Preferred approach and is accomplished by means of countering threats, removing vulnerabilities from assets, limiting access to assets, and adding protective safeguards.

There are three common methods used to defend:

Application Of Policy

Education And Training

Application Of Technology

Implementing the Defend Strategy Organizations can mitigate risk to an asset by

countering the threats it faces or by eliminating its exposure.

It is difficult, but possible, to eliminate a threat.

Another defend strategy is the implementation of security controls and safeguards to deflect attacks on systems and therefore minimize the probability that an attack will be successful.

Transfer

The transfer control strategy attempts to shift risk to other assets, other processes, or other

The owner of the information asset, IT management, and the information security team must ensure that the *disaster recovery requirements* of the outsourcing contract are sufficient and have been met *before they are* needed. If the outsourcer fails to meet the contract terms, the consequences may be far worse than expected.

Mitigate

attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation. This approach requires the creation of three

Types of plans: the incident response plan, the disaster recovery plan, and the business continuity plan.

Plan	Description	Example	When Deployed	Time Frame
Incident Response Plan	Actions an organization takes during incidents (attacks)	• List of steps to be taken during disaster • Intelligence gathering • Information analysis	As incident or disaster unfolds	Immediate and real-time reaction
Disaster Recovery Plan	Preparations for recovery should a disaster occur; strategies to limit losses before and during disaster; step-by-step instructions to regain normalcy	• Procedures for the recovery of lost data • Procedures for the reestablishment of lost services • Shutdown procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business Continuity Plan	Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DR plan's ability to restore operations	• Preparation steps for activation of secondary data centers • Establishment of a hot site in a remote location	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term operation

Accept

The accept control strategy is the choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation.

This may or may not be a conscious business decision.

The only industry-recognized valid use of this strategy occurs when the organization has done the following:

Determined the level of risk

Assessed the probability of attack

Estimated the potential damage that could occur from attacks

Performed a thorough cost benefit analysis

Evaluated controls using each appropriate type of feasibility

Decided that the particular function, service, information, or asset did not justify the cost of protection

Terminate

The terminate control strategy directs the organization to avoid those business activities that introduce uncontrollable risks.

If an organization studies the risks from implementing business-to-consumer e-commerce operations and determines that the risks are not sufficiently offset by the potential benefits, the organization may seek an alternate mechanism to meet customer needs—perhaps developing new channels for product distribution or new partnership opportunities.

By terminating the questionable activity, the organization reduces the risk exposure.

Selecting a Risk Control Strategy

Feasibility Studies

Cost Benefit Analysis (CBA)

Evaluation, Assessment, and Maintenance of Risk Controls.

Selecting a Risk Control Strategy

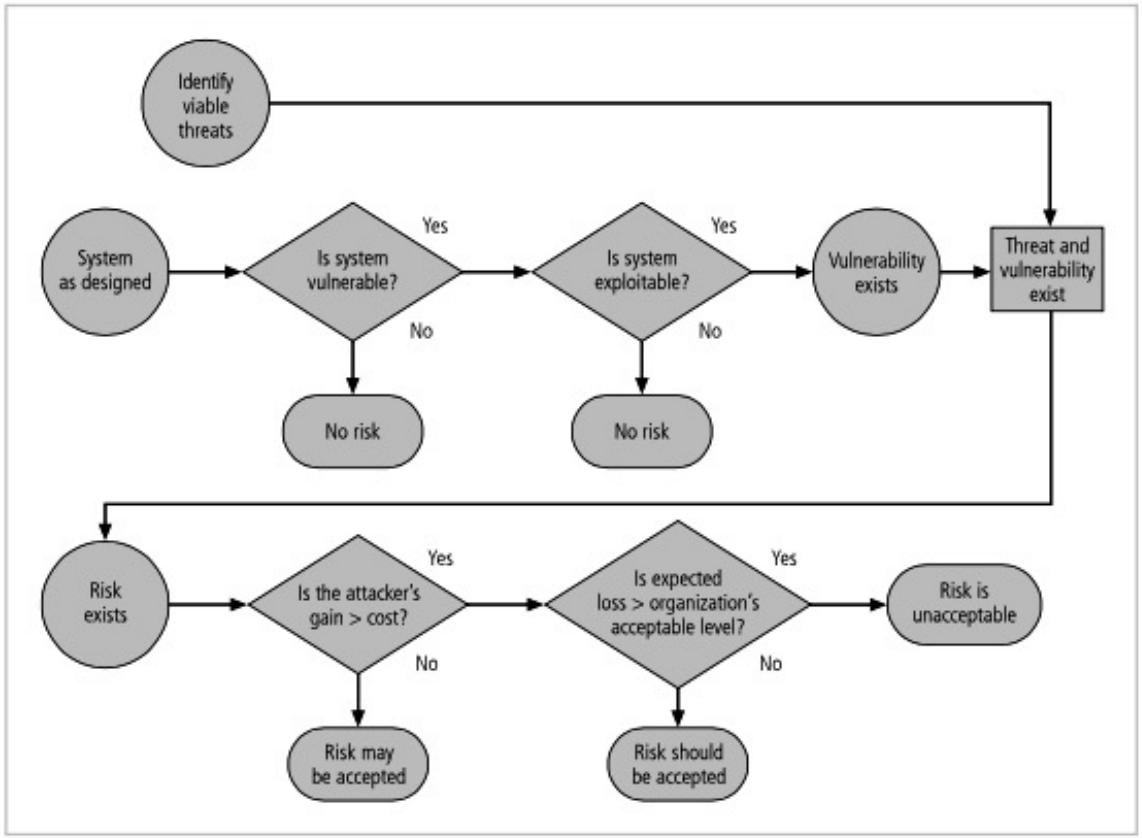
Weighing the benefits of the different strategies, keep in mind that the level of threat and value of the asset should play a major role in strategy selection.

When a vulnerability (flaw or weakness) exists: Implement security controls to reduce the likelihood of a vulnerability being exercised.

When a vulnerability can be exploited: Apply layered protections, architectural designs, and administrative controls to minimise the risk or prevent occurrence.

When the attacker's cost is less than his or her potential gain: Apply protections to increase the attacker's cost (e.g., use system controls to limit what a system user can access and do, thereby significantly reducing an attacker's gain).

When potential loss is substantial: Apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.


Identify viable threats
System as designed
Is system vulnerable?
Yes
No
No risk
Is system exploitable?
Yes
No
No risk
Vulnerability exists
Threat and vulnerability exist
Risk exists
Is the attacker's gain > cost?
Yes
No
Risk may be accepted
Is expected loss > organization's acceptable level?
Yes
No
Risk should be accepted
Risk is unacceptable

Feasibility Studies

The organization must explore all the economic and noneconomic consequences of the vulnerability facing the information asset.

Attempt to answer the question, “What are the actual and perceived advantages of implementing a control as opposed to the actual and perceived disadvantages of implementing the control?”

There are also many methods an organization can use to identify the disadvantages of specific controls.

Cost avoidance is the process of preventing the financial impact of an incident by implementing a control.

Benefit

Value that an organization realises by using controls to prevent losses associated with a specific vulnerability.

The amount of the benefit is usually determined by valuing the information asset or assets exposed by the vulnerability and then determining how much of that value is at risk and how much risk there is for the asset.

A benefit may be expressed as a reduction in the annualized loss

Asset valuation

The process of assigning financial value or worth to each information asset.

Some argue that it is virtually impossible to determine the true value of information and information-bearing assets.

Perhaps this is one reason why insurance underwriters currently have no definitive valuation tables for assigning worth to information assets.

The value of information differs within organizations and between organizations,

Cost Benefit Analysis (CBA)

Must consider the economic feasibility of implementing information security controls and safeguards

It is only common sense that an organization should not spend more to protect an asset than the asset is worth.

The formal decision- making process is called a **cost benefit analysis** or an **economic feasibility study**

Some of the items that affect the cost of a control or safeguard include the following:

Cost of development or acquisition (purchase cost) of hardware, software, and services Training fees (cost to train personnel)

Cost of implementation (cost to install, configure, and test hardware, software, and services)

Service costs (vendor fees for maintenance and upgrades)

Cost of maintenance (labor expense to verify and continually test, maintain, and update)

Once an organization has estimated the worth of various assets, it can begin to examine the potential loss that could occur from the exploitation of a vulnerability or a threat occurrence.

This process results in the estimate of potential loss per risk.

Questions that must be asked here include:

What damage could occur, and what financial impact would it have?

What would it cost to recover from the attack, in addition to the financial impact of damage?

What is the single loss expectancy for each risk?

A **single loss expectancy (SLE)**

exposure factor (EF), which is the expected percentage of loss that would occur from a particular attack, as follows:

SLE =asset value *exposure factor (EF)

where EF equals the percentage loss that would occur from a given vulnerability being exploited.

This is usually determined through an **annualized loss expectancy (ALE)**, which is calculated from the ARO and SLE, as shown here:

ALE= SLE* ARO

While many techniques exist, the CBA is most easily calculated using the ALE from earlier assessments before the implementation of the proposed control, which is known as ALE(prior). Subtract the revised ALE, estimated based on the control being in place, known as ALE(post). Complete the calculation by subtracting the **annualized cost of the safeguard (ACS)**.

CBA =ALE(prior) -ALE(post) -ACS

Evaluation, Assessment, and Maintenance of Risk Controls

The selection and implementation of a control strategy is not the end of a process.

The strategy, and its accompanying controls, must be monitored and reevaulated on an ongoing basis to determine their effectiveness and to calculate more accurately the estimated residual risk.

How this cyclical process is used to ensure that risks are controlled.

Note that there is no exit from this cycle; it is a process that continues for as long as the organization continues to function.

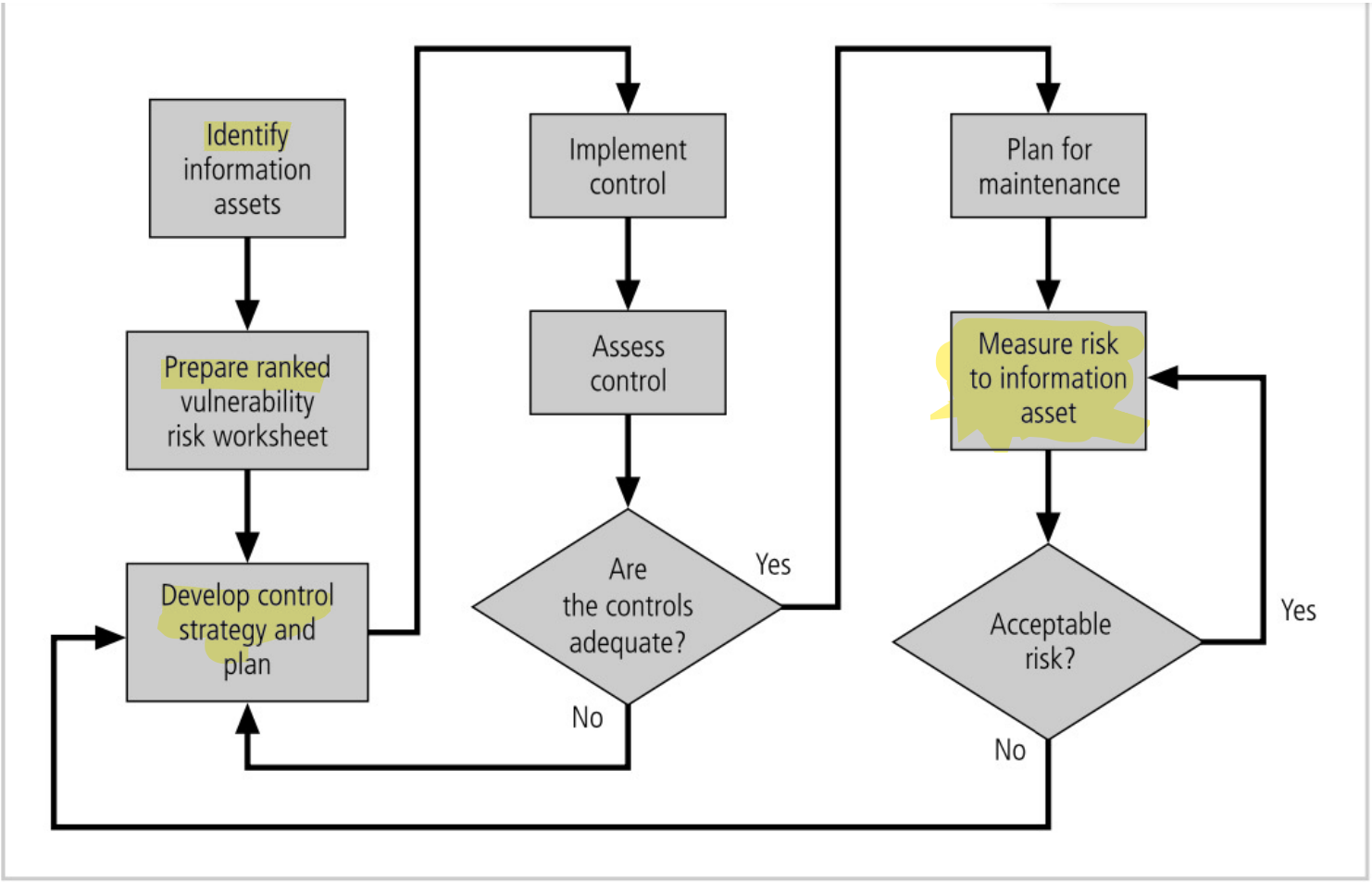


Figure 4-9 Risk Control Cycle

Quantitative Versus Qualitative

Risk Control Practices.

Benchmarking and Best Practices.

Other Feasibility Studies

* The many steps described were performed using actual values or estimates.

* This is known as a **quantitative assessment**. However, an organization could decide that it put specific numbers on these values.

* Fortunately, it is possible to repeat these steps using an evaluation process, called **qualitative assessment,** that does not use numerical measures.

Benchmarking and Best Practices

** Benchmarking can yield great benefits in the education of executives and the realized performance improvements of operations.*

** determine strategic areas of opportunity.*

**that delivers the marked and impressive results so often noted.*

**allows one to make a direct comparison.*

**Any identified gaps are improvement areas.*

When benchmarking, an organization typically uses one of two types of measures to compare practices

* *metrics-based measures*
* *process-based measures.*

Metrics-based measures are comparisons based on numerical standards

* Such as: Numbers of successful attacks
    * **Staff-hours spent** on systems protection
    * **Dollars spent** on protection Numbers of security personnel
    * Estimated value in dollars of the information lost in successful attacks
    * **Loss in productivity** hours associated with successful attacks .

An organization uses rank competing organizations with a similar size or market to its own and then determines the difference →**performance gap**,work on to improve its

Process-based measures are generally less focused on numbers and are more strategic than metrics-based measures.

*Organization is interested in benchmarking

* Examine the activities an individual company performs its goal, rather than the specifics of how goals are attained.

* The primary focus is the *method* the organization uses to accomplish a particular process, rather than the out- come.

* **Two categories of benchmarks** are used:

Standards Of Due Care And Due Diligence

Best Practices.

*Security efforts that seek to provide a superior level of performance in the protection of information are referred to as best business practices or simply best practices or recommended practices.

Applying Best Practices

*The preceding sections have presented a number of sources you can consider when applying standards to your organization.

* You can study the documented best practice processes or procedures that have been shown to be effective and are thus recommended by a person or organization and evaluate how they apply to your organization. When considering best practices for adoption.

* Does your organization resemble the identified target organization with the best practice under consideration?

* Is your organization in a similar industry as the target?

* Does your organization face similar challenges as the target?

* If your organization has no functioning information security program, a best practice

* your organizational structure similar to the target's? Obviously, a best practice proposed for a small home office setting is not appropriate for a multinational company.

* Are the resources your organization can expend similar to those identified with the best practice? If your approach is significantly limited by resources, it is not useful to submit a best practice proposal that assumes unlimited funding.

*Use antivirus software.

* Use strong passwords.

* Verify your software security settings.

* Update product security.

* Build personal firewalls.

* Back up early and often.

* Protect against power surges and loss.

For the small businesses Microsoft recommends the following:

*Protect desktops and laptops—Keep software up to date, protect against viruses, and set up a firewall.

* Keep data safe—Implement a regular backup procedure to safeguard critical business data, set permissions, and use encryption.

* Use the Internet safely—Web sites, popups, and animations can be dangerous. Set rules about Internet usage.

* Protect the network—Remote network access is a security risk you should closely monitor. Use strong passwords and be especially cautious about wireless networks.

* Protect servers—Servers are the network's command center—protect your servers.

* Secure business applications—Make sure that software critical to your business operations is fully secure around the clock.

* Manage desktops and laptops from the server—Without stringent administrative procedures in place, security measures may be unintentionally jeopardized by users.

Problems with the Application of Benchmarking and Best Practices

*The biggest problem with benchmarking and best practices in information security is that organizations don't talk to each other.

* A successful attack is viewed as an organizational failure.

* Because valuable lessons are not recorded, disseminated, and evaluated, the entire industry suffers.

* Sharing stories, and publishing the lessons learned.

* Refuse even to acknowledge,

* Much less publicize,

* Another problem with benchmarking is that no two organizations are identical.

* Even if two organizations are producing products or services in the same market, their sizes, composi- tions, management philosophies, organizational cultures, technological infrastructures, and budgets for security may differ dramatically.

* A third problem is that best practices are A moving target.

* What worked well 2 years ago

* Addition to the methods, techniques, policies, guidelines, educational and training

* One last issue to consider is that simply researching information security benchmarks

* Doesn't necessarily prepare A practitioner for what to do next. However, preparing for past threats does not safeguard against new challenges to come.

Other Feasibility Studies

*Other qualitative approaches that can be used to determine an organization's readiness for any proposed set of controls are operational, technical, and political feasibility analyses

Organizational Feasibility

* Examines how well the proposed information security alternatives will contribute to the efficiency, effectiveness, and overall operation of an organization.

* Other words, the proposed control must contribute to the organization's strategic objectives.

Operational Feasibility

* **Operational feasibility** analysis examines user acceptance and support, management acceptance and support, and the overall requirements of the organization's stakeholders.

* Also known as **behavioral feasibility**, because it measures the behavior of users.

* *Communicate* with system users throughout the development of the security program, letting them know that changes are coming.

Technical Feasibility

*** Consider the technical feasibilities of their design, implementation, and management. Some safeguards, especially technology-based safeguards, are extremely difficult to implement, configure, and manage.**

Political Feasibility

*** Within organizations, political feasibility determines what can and cannot occur based on the consensus and relationships among the communities of interest**

Risk Management Discussion Points

*Not every organization has the collective will or budget to manage
*decide when it was live

Risk Appetite
Residual Risk
Documenting Results

Risk Appetite

*Risk appetite defines the quantity and nature of risk that organizations are willing to accept as they evaluate the tradeoffs between perfect security and unlimited accessibility.

* Critical tool for effective decision making

* Help the management to understand → allocate the resource accordingly

* Services company, regulated by government and conservative by nature, may seek to apply every reasonable control and even some invasive controls to protect its information assets.

* Nonregulated organizations →avoid the negative publicity

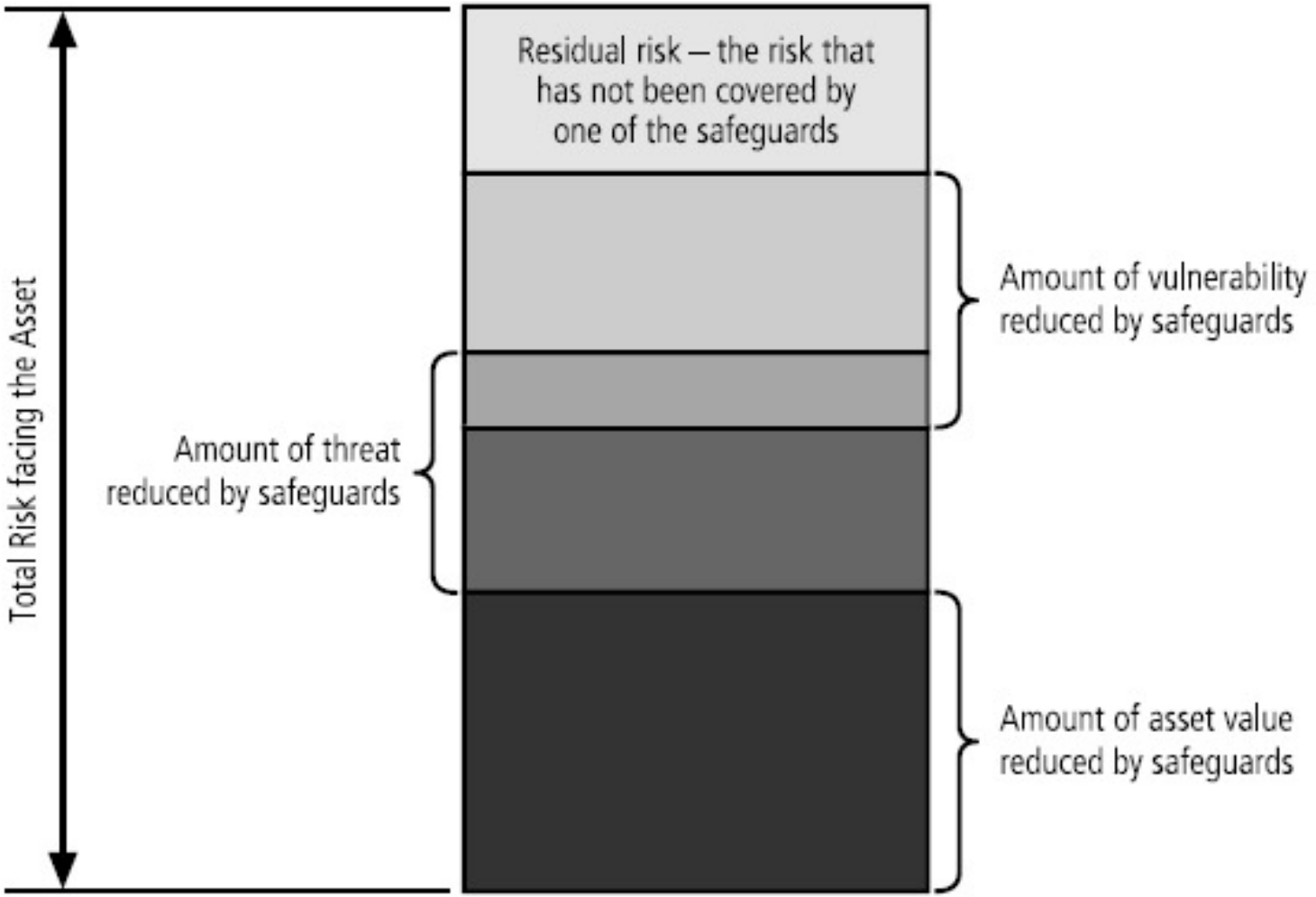
Residual Risk

Even when vulnerabilities have been controlled as much as possible, there is often still some risk that has not been completely removed, shifted, or planned for another way, “residual risk is a combined function of

(1) a threat less the effect of threat-reducing safeguards,

(2) a vulnerability less the effect of vulnerability-reducing safeguards

(3) an asset less the effect of asset value-reducing safeguards



gure 4-10 Residual Risk

Documenting Results

*****The results of risk assessment activities can be delivered in a number of ways: -a report on asystematic approach to risk control

-a project-based risk assessment

-topic-specific risk assessment.

*overall risk management program, it requires a systematic report that enumerates the opportunities for controlling risk.

*This report documents a series of proposed controls, each of which has been justified by one or more feasibility or rationalization approaches.

* At a minimum, each information asset-threat pair should have a documented control strategy that clearly identifies any residual risk remaining after the proposed strategy has been executed

Recommended Risk Control Practices

*Planned expenditures must be justified and budget authorities

* Not money ,focus on the goal

* This underlines the importance of developing strong justifications for specific action plans and providing concrete estimates in those plans.

* Another factor to consider is that each control or safeguard affects more than one asset-threat pair.

* Firewall- -greatest value to as many asset-threat pairs as possible.,

another fact of the risk management problem

* To put it more simply, if you put in one safeguard, you decrease the risk associated

* To make matters even more complex, the action of implementing a control may change the values assigned or calculated in a prior estimate.

* There is an ongoing research for ways to design security architectures

Record Layer Protocol

- Responsible for securing application data and verifying its integrity and origin.
- It manages the following:
  - Dividing outgoing messages into manageable blocks,
  - Reassembling incoming messages.
  - Compressing outgoing blocks
  - Decompressing incoming blocks (optional)
- Record **layer** is the one that handles the actual data.
- It gets data from the application **layer**, encrypts it, fragments it to an appropriate size, as determined by the algorithm, and sends it on to the Transport **Layer**.

- Record Protocol takes message to be transmitted, fragments the data into manageable blocks , protects the records, and transmits the result.
- Received data is verified and decrypted, reassembled, and then delivered to higher-level client.
- The record layer fragments information blocks into TLSPlaintext records carrying data in chunks of 2^14 bytes or less.
- Message boundaries are handled differently depending on the underlying Content Type. Any future content types must specify appropriate rules.
- Note that these rules are stricter than what was enforced in TLS

SSL Record Layer protocol has got the below functions to fulfill.

- Breaking Down the Data from Application layers, with fixed length.
- Compress the Data
- Add Message Authentication Code, Which is calculated with the help of Integrity Key.
- Encrypt the packets(which was broked down with fixed length).
- Add SSL header's in the packets with fixed length. Which consists the following headers, which combinely form a 5byte header.

- Designed to provide three essential **services** to all applications running above it:

  -Encryption

  -Authentication

  -Data integrity.

- Record Protocol Header contents in SSL
  - 1 Byte Protocol Definition
  - 2 Byte Protocol version
  - 2 Byte Length
- The **purpose** of the **record protocol** is to take an application message to be transmitted, fragment the data which needs to be sent, encapsulate it with appropriate headers and create an object just called a **record**, which is encrypted and can be forwarded for sending under the TCP **protocol**.