O'REILLY®

Early Release

RAW & UNEDITED

# Certified Information Systems Security Professional (CISSP) Study Guide

## Essential Exam Prep

Kevin Henry

# Certified Information Systems Security Professional (CISSP) Study Guide

## Essential Exam Prep

With Early Release ebooks, you get books in their earliest form—the author's raw and unedited content as they write—so you can take advantage of these technologies long before the official release of these titles.

**Kevin Henry**

**Certified Information Systems Security Professional (CISSP) Study Guide**

by Kevin Henry



Published by O'Reilly Media, Inc., 141 Stony Circle, Suite 195, Santa Rosa, CA 95401.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*https://oreilly.com*). For more information, contact our corporate/institutional sales department: 800-998-9938 or *corporate@oreilly.com*.

Acquisitions Editor: Simina Calin

Development Editor: Corbin Collins

Production Editor: Gregory Hyman

Cover Designer: Susan Brown

Cover Illustrator: Susan Brown

Interior Designer: David Futato

Interior Illustrator: Kate Dullea

October 2026: First Edition

**Revision History for the Early Release**

- 2025-09-25: First Release

See *https://oreilly.com/catalog/errata.csp?isbn=9798341652941* for release details.

979-8-341-65294-1

[LSI]

# Brief Table of Contents (*Not Yet Final*)

# Chapter 1. Introduction to the CISSP

**A NOTE FOR EARLY RELEASE READERS**

With Early Release ebooks, you get books in their earliest form—the author's raw and unedited content as they write—so you can take advantage of these technologies long before the official release of these titles.

This will be the first chapter of the final book.

If you'd like to be actively involved in reviewing and commenting on this draft, please reach out to the editor at *ccollins@oreilly.com*.

You have just started on a project that is sure to make a positive difference in your life and career. The CISSP is the gold standard for information security management and opens doors of opportunities and increased job satisfaction. The CISSP has already changed the lives of many people, and you are next! This is the right place to start.

Through this Study Guide you will become familiar with all the topics covered in the CISSP examination. You will quickly notice that instead of focusing on memorizing dull materials, the topics will be understandable and useful, packed with content that you can use every day. As many of my students have said, they come back to revisit these materials frequently and use them as guideposts to help

them in being a more confident, capable, and effective security professional.

This chapter introduces the CISSP examination. You will learn what you can do to prepare and increase your chances of success on examination day. Even if you never plan to sit for the examination, reading this Study Guide will teach you a lot that will find useful everyday.

Let’s get started on your certification journey with a review of the CISSP certification and the structure of the examination.

## The CISSP

The CISSP, short for Certified Information Systems Security Professional, is a certification issued by the International Information Systems Security Certification Consortium. For a number of years this consortium was known as $(ISC)^2$, though now it has changed its name to ISC2.

Originally this consortium was put together by several security organisations that recognized the need for a standard that defined the requirements to be a security professional.

Through the work of many volunteers, a taxonomy was built of all the topics that every security professional should be familiar with, called the *common body of knowledge* (CBK). The CISSP certification is based on the content of the CBK..

In the early days of the CISSP, the CBK was divided into 10 domains (or subject areas). The purpose of the domains was to arrange the various knowledge topics into a

manageable structure. The course used to prepare for the certification examination was two weeks long.

Times have changed. Few people can afford to be out of the office attending a course for two weeks, so the courses were shortened to one week. For instructors, the shortening of the course meant that a lot of content has to be covered in the reduced timeframe, leaving very little time to develop and dig into the materials. In the early days, there were no Study Guides or other materials available to assist the student in preparing for the exam. Now a CISSP course is supported and augmented by many additional resources that present the content of the CBK in an effective and varied format to address all learning modalities. These resources provide each student the ability to learn at a speed they are comfortable with and to explore the content in a way that is not just based on memorization, but also on the understanding required to apply the knowledge in the way that is to be expected of a security professional.

For a number of years, Hal Tipton and I were the co-chairs of the CBK. Various approaches were taken to define what content should be testable for a CISSP candidate. Today's CBK consists of eight domains, although many topics are addressed in multiple domains. The challenge for a CISSP course or Study Guide is to arrange the topics in a manner that supports logical learning and topic development – but without repeating content frequently. Therefore, this book will frequently introduce and expound on a topic in one chapter and then link to that topic where it is covered in the content of other domains and chapters.

Note that the CISSP is a *security management* certification. The CISSP was the pioneer in establishing a security management certification and has a very good balance

between both technical and management areas. This requirement to know security *management* and yet to understand how to manage security *technology* is a challenge for many CISSP candidates.

One CISSP candidate may be excellent in a technical area but weak in management; another candidate may be very good in the management areas of policies and risk management but not know what a firewall does or how to manage it. Both types will have to work hard to pass the examination. They will have to become familiar with the areas in which they do not have expertise, and will need to ensure a well-rounded knowledge in their more comfortable areas. I have often seen students fail the exam in the areas they thought they knew well. A trap for many students is to neglect developing their strengths, not realizing that their experience is one-sided and incomplete. The candidate may know how their organization does things, but be ignorant of other ways or approaches to do the same tasks.The goal of this book is to help you pass the examination, to become a true security professional who can add value to the organizations you work for, and to be a leader in information security management.

This benefit of holding the CISSP certification is that it demonstrates a good balance between the technical and management areas. A CISSP is someone who has passed an examination that requires knowledge of management skill, but who also knows how to manage the security practitioners and administrators who operate and configure firewalls and many other technologies on a day-to-day basis.

The first, and probably most important, tip for a technical person preparing for the CISSP is to remember to think like a manager. Every candidate must approach the CISSP

exam thinking like a manager. Managers see that there are few absolute, correct answers. Instead, a number of different alternatives or options must be considered. Remember that the goal is not ultimate security – it is *adequate* security. Adequate security is a level of security that secures the business without restricting it. Adequate security is feasible based on tight budgets and conflicting demands. It is a level of security that aligns with the mission of the organization and is compliant with laws, regulations, and best practice.

The security manager will never have enough budget - or enough time - to accomplish everything that the manager wishes or needs to do. The security manager must do the best they can, weighing each security alternative carefully while understanding that in some cases one option may be better than another. Likewise, the CISSP examination presents a question or item and four possible solutions. The challenge is to choose the *right* solution based on the context and content of the question. All four answers provided may be technically correct, but the CISSP candidate must select the “BEST” answer option based on knowledge and experience.

Many have claimed that the CISSP examination is tricky. I don’t really like that. The CISSP examination is tough. A multiple-choice exam is one of the hardest types of tests to do. With an essay type of question, the candidate can dance around a topic and mention various things and, perhaps, get partial marks. In a multiple-choice exam only one answer is worth a mark, and the others are worth nothing. Each of the answers provided requires consideration and analysis. This requires more than memorization – a candidate cannot just memorize that *this* is the right answer for *this* question. That’s what makes the CISSP

exam hard to prepare for. The exam requires the *application* of knowledge. Knowledge is necessary, but experience is what differentiates between one answer and another. You can know the rules and theory of how to play tennis or golf – but there is a vast difference between knowledge and the ability to apply the knowledge and play at a professional level. The CISSP expects you to manage information security at a professional level.

That's why, in my view, the examination is very good. I went to the director of professional programs at ISC2 following an examination I had just taken and told him that the questions that were asked were good questions. They were based on topics that I should know about and therefore the questions were not tricky, but rather, they were exact.

> **TIP**
>
> The secret to preparing for the CISSP is to think like a manager not like a technician.

Let's continue our analogy that sitting for the CISSP examination can be compared to playing tennis against a pro. You would expect that each shot you face will be a hard one. In the game you will face many difficult shots, and with each you need to consider what is the spin on the ball, what is the direction of the shot, and what is the depth of the shot? So it is with the questions on the CISSP exam. Each one is hard. Some questions are more in-depth than others. Some have a spin that you must recognize. It is important to read the question carefully to understand what the direction of the question is. In some cases, you may need to think in a different way. A very good sample

question that I've seen in the past asks, "What is a purpose of a firewall?" The usual approach is to consider that a firewall is used to filter incoming traffic. But that is an incomplete understanding. The correct understanding is that a firewall is used to *protect* one network from another. So, a firewall should also examine outgoing traffic. It's important to know how a firewall protects you from an outside adversary by restricting incoming traffic, but the *best* answer may be related to ensuring that the firewall protects the people outside of the organization from an attack originating in your network.

## Sample Questions

This Study Guide contains many sample questions and test-taking tips to help you prepare for the CISSP exam. Sample questions create familiarity with the structure of exam questions and help to develop the analysis skills needed when facing the real exam questions. However, the purpose of the sample questions in this book, or from other sources, is *not* to measure your readiness for the exam.

Let me explain. A candidate may be scoring 95% on a sample test and think that they are ready for the exam, yet still fail the exam badly. The problem with an approach based solely on answering sample questions correctly is that it often leads to memorization instead of review and analysis. Memorization of sample questions provides the correct answer to a question that is not on the exam. ISC2 diligently ensures that questions available in sample tests are not used in the real exam. So, should you bother with sample questions if the questions are not real? Absolutely.

The goal of a sample question is to help you review the topic that the sample question is based on. The topic of the

sample question should always be based on a topic contained in the CBK. Reviewing the topic ensures familiarity with that topic.

An approach I recommend is to read the question—then stop. Now re-read the question (or *stem* as it is properly called) and explain the question to yourself. Use other words. Understand the topic in the question. Look at the spin and what the writer of the question is really trying to emphasize. Try to determine what the question is really trying to ask.

Now, this is not easy. Even in the real exam there will be questions you look at and say, “I don’t have a clue, and I don’t know what this question is asking.” But relax (easy for me to say). Use your analysis skills and experience to dig into the question and the answers. Should you guess? That is okay too. In fact, it is better to guess and be wrong than it is to just leave it and check the answer later. You will remember the correct answer better if you actually guess the wrong answer than if you leave it blank.

Then read and consider all the answers that are given. For each one do an analysis of why this answer is good or why this one is bad. Maybe this “wrong” answer would be a correct answer to a different question. Review each answer and link it to a relevant topic. Link topics together and understand the topic in its context.

Doing a sample test is not a sprint or a race. Just like in the real exam, you have time. Take a deep breath and focus. Take time to think. I often recall the story of a doctor training to be a heart surgeon. In his first surgery, he was warned not to sever the main artery, or the patient would bleed out in three minutes. But then he was assured that even if you do cut the main artery, don’t stress—even the

worst surgeon can stitch the artery back together in less than a minute. You have time. Take it and use it wisely. More questions are answered wrong because they were rushed than because the time was short.

Again, read all four answers – remember that more than one answer can be correct, but only one answer is the *best*. You only get a point if you choose the best answer – there are no points for being close. By analyzing the question and all four answers, each sample question becomes a review of maybe three or four different topics. This is the true value of sample questions: to exercise the brain, to review multiple topics, and to help you prepare for the rigor and difficulty of the CISSP examination.

## The CBK

The pool of questions used for the CISSP examination has questions on every topic in the common body of knowledge. The CBK is a high-level overview (taxonomy) of the examination topics and is derived from a more precise document known as the *detailed content outline* (DCO). The CISSP is frequently reviewed by a group of subject matter experts and certification holders to ensure that the examination is up-to-date and relevant to what a security professional should know.

The CISSP CBK is divided into eight domains, and each domain has its own level of weighting or importance on the examination. The domain of Security and Risk Management is the most important domain – weighted at 16% of the exam, whereas, for example, Asset Security is only weighted at 10% of the exam. Figure 1-1 shows the breakdown of the weights of the domains.

## CISSP CAT Examination Weights

| Domains | Average Weight |
|---|---|
| 1. Security and Risk Management | 16% |
| 2. Asset Security | 10% |
| 3. Security Architecture and Engineering | 13% |
| 4. Communication and Network Security | 13% |
| 5. Identity and Access Management (IAM) | 13% |
| 6. Security Assessment and Testing | 12% |
| 7. Security Operations | 13% |
| 8. Software Development Security | 10% |
| **Total** | **100%** |

*Figure 1-1. Breakdown of the weights of the domains*

The only authoritative source for questions about the CISSP examination is the ISC2 website. It has extensive information on the exam structure and marking. All CISSP candidates should review the CISSP website as part of their preparation. The exam rules change on a regular basis, and no one wants a surprise on examination day.

**WARNING**

This book is an explanation of the exam and advice on how to prepare for it, but the ISC2 website is the ultimate and only authority.

The CISSP examination candidate should be prepared for questions on every topic listed in the CBK. Be comfortable in all eight domains to a level not just of knowledge but also application of knowledge. Do not just focus study time on your areas of strength or experience, or the topics you like. Learn all topics within the CBK (and that is exactly what this book is aiming to help you do) because the adaptive structure of the examination will home in on areas of weakness and expose any gaps in knowledge or understanding. It is possible to pass the exam even if you score below the required proficiency in one domain – but don't run that risk.

You cannot just do well in one or two domains and really poorly in the others. This is a balanced exam and requires a study plan that covers all the topics to an advanced level of understanding—not just to memorize, but to understand them. Understand the topics in the CBK well enough that you could explain them to another person.

A common problem that some candidates have had is to be really good in one area – perhaps networking. They know all about networks and network components, better than anyone else in the exam room, but they fail the exam. Why? Because it's not a network exam. It's a network *security* exam. You must understand network security, not just network operations. Also, you may be very good at the network hardware you have used, yet not be familiar with

network hardware or design used by other companies, or in other regions of the world.

To such a candidate’s surprise they actually do poorly in their domain in which they are an expert. Then they blame the exam. They do not consider that the exam is about security management, not about protocols and ports. It includes familiarity with various solutions – not just the ones they have experience in. It is important to review all domains in the CBK - even the domains you are comfortable in. Ensure that you review all topics carefully to make sure you have understood that topic from all angles, not just from your own background or experience.

## The Study Plan

There is no single authoritative source for preparing for the CISSP exam. This book is a great help to preparing, but so are several others. None is perfect. Some people learn by reading, others by doing, or listening. Many of my students have used my books along with attending instructor-led training or online courses. Reading and hearing things in different ways may increase understanding or retention.

**TIP**

It is important to have a study plan. Take notes. Explain concepts to yourself. Meditate on a topic until it is understood. Link one topic to another topic and see how all the pieces of security fit together. Do sample questions and explain the answers. Like a game show – take the answers to a sample question and create new questions for them. Some domains such as Security and Risk Management are more heavily weighted on the exam and deserve a larger portion of study time, whereas Software Development Security is only weighted at 10% and should not be the main domain the candidate studies. Repetition is good. Take a few minutes every hour, or at least several times a day, and just do a quick review. Setting an exam date is a good idea for many people. Then trace back and allocate study time for each domain up to the exam date.

How long should you take to prepare? That depends on experience, work commitments, distractions, family, and availability of the exam. Many of my students have done the exam at the end of a weeklong course and most passed. Some have waited a few weeks so that they could have more time to dig into the materials – others knew that the moment they were back at work and home that they would not have time to study and waiting a few weeks would only be to their detriment.

**TIP**

Study all topics and thoroughly cover each domain before moving on to another domain. Then, the day before the exam do a once-over review.

## The CISSP Examination Today

The CISSP examination used to be a paper-based, six-hour-long marathon of 250 questions. The candidate waited

weeks to get their results. Many other candidates in the exam room would get the same questions. However, the CISSP exam has changed since then. Now the CISSP exam uses computerized adaptive testing (CAT). The CISSP CAT examination contains 125-150 multiple choice and advanced items, including charts, tables, calculation, order response, drag and/or hotspots, scenario-based, or video-based questions.

CAT testing is tailored for each examination candidate. Initially each candidate will start with an item that is well below the passing standard. Following the candidate's response to an item, the scoring algorithm will re-estimate the candidate's ability based on the difficulty level of all items presented and all the previous answers provided for those items. After each item is answered, the item-selection algorithm determines the next item to present to the candidate with the expectation that a candidate should have approximately a 50% chance of answering that item correctly. With each additional item answered, the computer's estimate of the candidate's ability becomes more precise. Through this iterative process, the intent is to gather as much information as possible about a candidate's true ability level more efficiently than traditional, linear exams. Read more about this here.

## Examination Scoring and Certification

The passing mark for the CISSP is at least 700 points out of a possible 1000 points. This is a scaled score based on the number of items answered correctly. Once the scoring algorithm has confidently determined whether the candidate will pass or fail the examination, the exam will stop, and the candidate will be advised of their result. A

candidate that passed with the minimum number of questions has demonstrated a thorough understanding of the CISSP exam topics. The following from ISC2 describes the scoring of the CISSP examination:

> *The proficiency is defined as meeting or exceeding the "passing standard." Candidates must score above the proficiency level in order to pass the exam. A single pass/fail result is calculated on the total of all operational items administered for the examination. ISC2 exams are compensatory exams which allow for a higher number of items answered correctly in one domain to compensate for a lower performance in another domain. If a candidate performs very well in a more heavily weighted domain where a high number of items are included on the exam, and only performs near proficiency or even below proficiency, in a lesser weighted domain, where a fewer number of items are included, there is a possibility that a candidate may pass the exam—but there is no guarantee. Domain performance is provided to candidates who do not pass the exam for purposes of diagnostic feedback for future exam preparation, as follows:*
>
> - *Below proficiency: Below the passing standard*
> - *Near proficiency: Close to the passing standard*
> - *Above proficiency: Above the passing standard*

If a candidate fails the exam, the letter they are given as they leave the exam room will rank their results per domain. This enables the candidate to know which areas to focus on before sitting for the examination again. There are rules around doing a re-sit for the exam that require a waiting period before the candidate can sit for the exam again.

The goal, of course, is to pass the *first* time, and the goal of this book is to help you be prepared so that you can be successful and confident.

Once you have passed the examination, you can apply for the certification. To do this you fill in an online form listing your experience and have that form endorsed by a fellow certification holder or by ISC2 itself. There is an annual fee associated with the CISSP certification, and each certification holder is required to obtain Continuing Professional Education (CPE) credits each year. The CISSP certification is valid for three years, and as a Certified CISSP you do not have to re-sit for the exam so long as you maintain good standing with ISC2 by paying the annual maintenance fee (AMF) and submitting the required number of CPE credits in a timely manner.

## Test-Taking Tips

In case you haven't figured it out yet, the CISSP examination is hard. Challenging. Threatening. But doable. Preparation is the key, and the more prepared you are, the more likely you are to experience exam success. It is quite probable that I have taught more CISSP candidates than anyone else in the world, and the percentage of candidates who pass is very high. If you go through this book, absorb the materials, and follow a good study plan, then you should pass.

**NOTE**

Never forget: this exam is *not* about knowledge – it is about *how to think*. It's about how to approach the topics, and then how to approach the examination.

When you enter the examination room, be prepared to be there for the full three hours. Do not rush, panic, stress, or try to set a record for the fastest exam completed. (By the way, the record is about one hour with a pass).

Do all this in the lead-up to exam day:

- Have a study plan and try to keep the information fresh in your mind for the days leading up to the exam.
- Get sleep. This is not a memorization test – it is an analysis test and your mind needs to be sharp – not exhausted.
- Leave for the exam location in plenty of time, maybe early enough for a coffee, tea or a last-minute review before the exam starts. You do not want to be stressed because of traffic or anything else.
- Make sure you have the required Identification documents with the name used to register for the exam available.

## The Exam Environment

It is unlikely that you will be allowed anything, even water, in the examination room, but you will be permitted to take breaks during the examination. However, the exam is three hours long, and the timer for the exam does not stop when you take a break. If the exam timer ends before the candidate has completed the exam, the scoring algorithm may still grant a passing mark based on the completed items. This is explained in more detail on the ISC2 website. Here’s my advice:

- Use your time wisely. There will likely be questions on the exam that you did not expect or are unfamiliar with. Security is a broad topic, and no one knows everything. Using your analysis skills, read the question and answers and make the best guess you can.
- Once you have answered a question, you *cannot* go back to review or revise your answer.
- As with a tennis match, do not expect to win every point or get every question correct. A candidate can pass the exam even with a number of incorrect answers – a pass is 700 points out of a possible 1000.
- When you stumble on a question, move on. Win the next one. Each question is a new challenge. Do not get discouraged or downhearted.
- Remember that most people believe that they are failing when they are in the exam – but most people pass, so their belief was wrong. Try not to think about it. You know the exam will be tough. Do your best and keep a positive attitude.
- Read and consider all the answers, and *think like a manager*. Look for the high-level answers that may even include the other answers.
- Step back and think about the question. Look for key words. A frequent mistake is to think one answer has to be absolutely right. Life is rarely like that. Choose the best answer, even if the best answer would be wrong ten percent of the time. Go with the 90%.

- Sometimes the answer you are looking for is not even there. This type of question tests the depth of your knowledge or perhaps approaches the question from a different angle. If the answer you think would be best is not one of the options, then the exam tests if you can choose the *next best*.
- Some questions will ask the order of a process. Requiring the exam candidate to put each of the steps in a process in the correct order. It can help to choose the first and the last steps before filling in the ones in the middle.
- Never choose the “I Don’t Know” answer. Sometimes there is an answer provided that you are not familiar with, and a natural tendency is to think that must be the right answer. It rarely is. First, consider all the other answers and only choose the one you are not familiar with if you know that the others are not correct.

All that said, the truth is it is very hard to concentrate for three hours. Take frequent breaks. Maybe after 15 or 20 questions just sit back in your chair for a moment. Relax. Take a few breaths. Clear your mind and recharge a bit. Just for a moment or two. Then you will be in fresh shape to tackle the next questions without trying to function on a drained mental battery.

Do your best and be confident. Going through this book will help you prepare. There is no guarantee that anyone will pass. Some people are better at tests than other people are. But I can guarantee one thing: just passing or failing the exam does not mean you are better or worse at your job. This is merely a test. Your worth is measured by the value you bring to your organization and the world around you.

Yes, it is nice to pass – but if not, then be reconciled to the plan to try again. Learn a bit more. Learn from the experience and try again.

## Summary

This chapter provided a quick look at the CISSP exam and study strategies to help you prepare for the exam. Its aim is to help you know how to approach the examination and content of the CBK.

Later chapters will examine each topic in more detail as we progress through each domain and topic of the common body of knowledge. In many cases, the important thing to remember is that this is not just an exercise in memorization. All the way through this book you need to focus on what is important, and why it is important, so that you understand the justification and the reason that this material is included in the CBK. In the end, the goal of this book is to help you be a better information security professional, as well as to help you be prepared to pass the CISSP examination.

We will look at many things as we step through the various chapters and domains of the CBK, and throughout it is important to relate what is covered to real life. This examination is not based on theory or some types of abstract concepts. It is based on the knowledge that is required to be used by an information security professional in real life. Remember that the examination questions (or *items* as they are officially called) are written by people like you. The question writers want to ensure that the questions are relevant and based on important information that information security professionals should know.

We’ve looked at many different topics throughout this chapter – about the exam, about study strategies, and test-taking techniques. It is good to frequently review and go back and dig into the topics that we’ve discussed in this book until you have a good, thorough understanding of each topic. Do the sample questions. Use those questions as a way to ensure a solid understanding of the concepts that those questions are based on.

Through all of this, be confident. You have chosen a good path that will help you to be a true information security professional. Be diligent and thorough in your studying so that you will be comfortable in all of the domains and topics in the CBK.

# Chapter 2. Risk Management

**A NOTE FOR EARLY RELEASE READERS**

With Early Release ebooks, you get books in their earliest form—the author's raw and unedited content as they write—so you can take advantage of these technologies long before the official release of these titles.

This will be the third chapter of the final book.

If you'd like to be actively involved in reviewing and commenting on this draft, please reach out to the editor at *ccollins@oreilly.com*.

Risk management is an important part of security management. It could easily be said that risk management sits at the core of many different business decisions, and the operations of many departments is based on risk – business continuity, incident management, security, and audit all use risk as the foundation for their activities.

In this chapter you will learn the knowledge and skills necessary to be a security expert with an excellent foundation in risk management. You will see the value of risk management and the techniques used to make risk management an effective part of security management.

There are two sections in the CISSP that are truly practical and logical. This makes these sections relatively easy to understand and follow. Those two are Cryptography and

Risk Management. Many people are afraid of these two topics but there is no need for that – by the end of this chapter you will understand risk management, and by the end of the cryptography chapter you will undoubtedly be fascinated with crypto.

This chapter steps through the entire risk management process in a logical and practical manner matching theory with practice, and knowledge with understanding.

## Risk Management Overview

Risk management Is based on structure and a methodology. For this book, we are going to follow the standards of NIST, the National Institute of Standards and Technology in the US, because these standards are freely available and align very well with other risk management standards such as ISO/IEC 27005.

Risk is an essential part of daily business operations. Every day, organisations have to acknowledge and assess risk in order to function as an organization. Risk can be described as an event that may impact the assets of the organization.

If we use the example of a financial institution, a bank has to decide whether or not to loan money to a customer that has applied for a loan. The bank knows that there is always the risk that the customer will not be able to pay back the loan, thereby putting the assets of the bank at risk. So, the bank has to determine whether it is in the interests of the bank to grant that loan or would it be better to practice risk avoidance and deny the customer's loan request. But taking risk is necessary for a bank. If the bank never loans out money it will not be able to make a profit. The bank earns a profit when it takes on the risk of loaning money – as long as the money is re-paid. But the bank can lose money if the

customer defaults or does not pay back the money. So, the challenge for the bank is to find the right balance between accepting the risk and loaning money to a customer or avoiding the risk and not making any profit.

Every time we cross the street, we take a risk. We mitigate, or reduce, the risk by checking for traffic, watching where we step, and following the rules put in place. We all acknowledge and manage risk every day, and by taking the risk we can enjoy the benefits of life, to go shopping, to visit friends, or to explore new places.

Risk is based on an understanding of what could go wrong and the weighing of the options of whether or not the risk is worth the reward. But risk is also a very personal decision. Maybe, when we are younger, we take greater risks but as we become older, we become a little more careful. It is the same in business. Some businesses encourage innovation and creativity. Management encourages employees to take a risk and try new ideas. Sometimes, we even hear the expression, “Fail forward.” If people to take a chance, or take a risk, and it does not work out, it’s best to learn from it and move ahead.

Risk has very positive and very negative potential effects. A risk of investing in research for a new product could result in immense profits for the organization, however that investment of both time and money could be lost if the new product doesn’t work out.

During this chapter we are going to take an in depth look at risk and how we can manage risk. It should be emphasized that the objective of managing risk is not to eliminate, or even minimize, risk. Rather, the objective of risk management is to be able to determine what is the *appropriate* level of risk the organization should take. For

us, as security managers, we will normally look at risk from a more negative perspective. We will examine the risk to information systems and how there could be a loss of asset value or impact on business mission if an information system fails. But we should always remember that for most of the organization risk is a positive and natural part of doing business every day.

## The Risk Management Process

The core concept or objective of risk management is to protect assets. Assets are defined as an item that is of value to its owner. An asset may be tangible – something that can be touched, like money, property, or inventory; or assets may be intangible – like reputation, customer confidence, employee morale, or ideas. The general rule is 'never to pay more to protect something than it is worth.' But what is an asset worth? In most cases, the value of an asset is determined by its owner. The owner of the asset is therefore the risk owner, and it is the owner that decides how to manage risk.

But asset value is not a simple calculation. As will be seen later in the risk assessment section, there are many factors that can influence asset value – such as regulations, historical or sentimental value, value to a competitor, and future earnings.

Risk can be defined as the probability of an event and its consequences to an asset. When identifying risk, the risk assessor must calculate the probability the risk event will happen, and the consequences or impact of the risk event, whether the consequences are either positive or negative. This requires the risk professional to be able to understand

how to assess the level of risk and provide value through good risk management.

As security professionals we focus on the identification, treatment, and monitoring of information security risk. Information security risk considers the probability that an adverse event will affect an information system and, thereby, affect the business that relies on that information system. Information system risk is therefore related to the ability of the business to reach its goals. The challenge for the security professional is to ensure that the level of risk is within the acceptable limits of risk as defined by senior management.

Risk management should always be structured and methodical. Risk should be managed in a thorough, consistent manner, and timely manner. A structured approach to risk management attempts to identify and mitigate risk before an adverse event happens rather than only conducting an analysis of an event only after the event happens.

It is easy to understand risk management when we approach it in a logical manner. The risk management process can be seen in Figure 2-1.

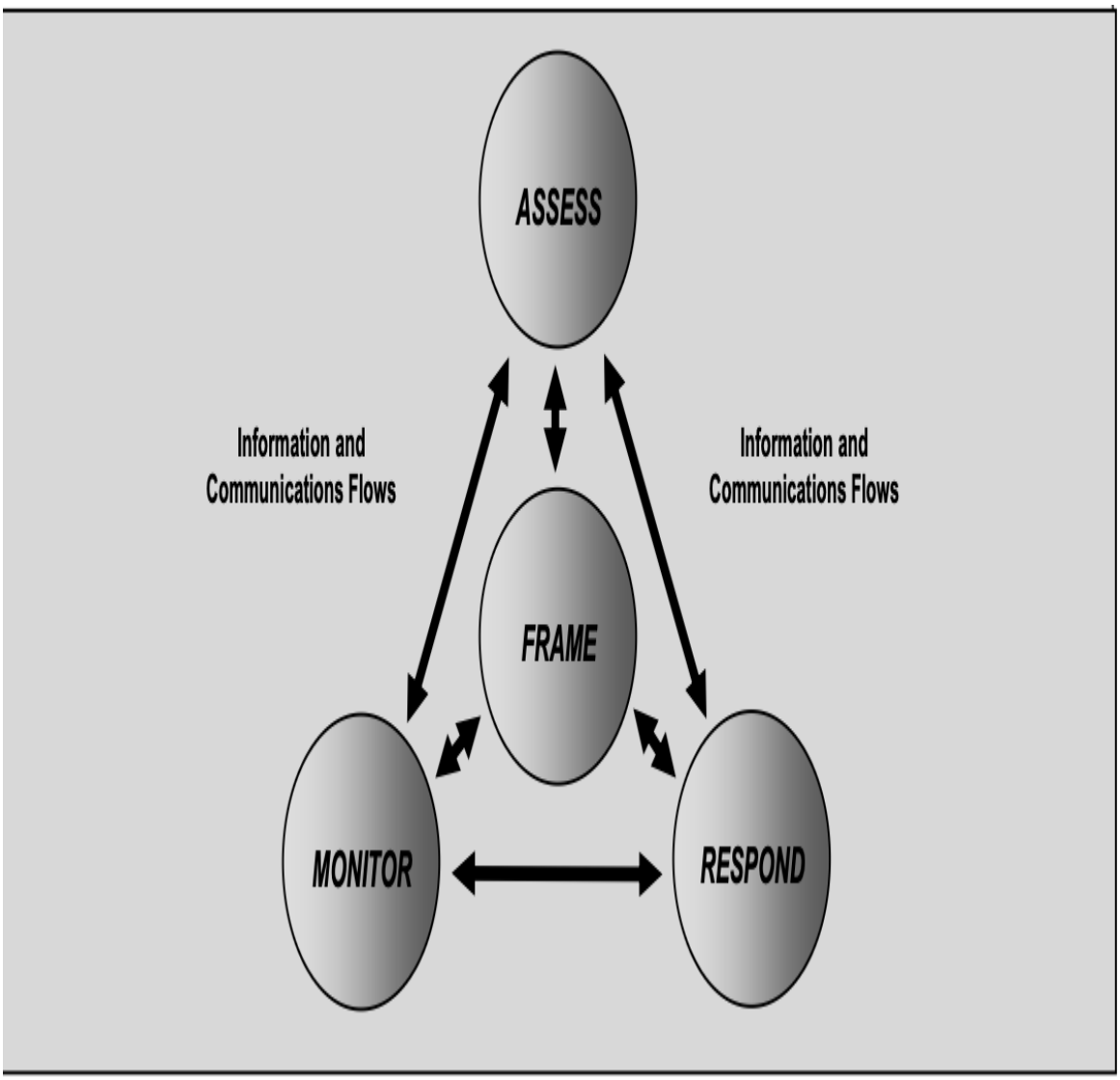


*Figure 2-1. Overview of the Risk Management Process as per NIST SP800-39 page 8 Fig 1*

We will step through each of the four phases of Figure 2-1 to get an understanding of how all the steps in the risk management process link together.

## Enterprise Risk Management

Risk should be managed across the enterprise in a consistent manner. That means that organizational risk is assessed and managed consistently in all departments, and in all locations. An advantage of enterprise risk

management is that the results of a risk assessment in one department can be compared with the results of an assessment in another department. Also, because risk is being managed at an enterprise level, rather than just at a systems level, it tends to have a higher profile and be better supported and prioritized by senior management.

There are many different risk management methodologies, and each has its advantages and disadvantages. It usually does not matter which methodology an organization selects, it is just important to learn to use the methodology correctly, efficiently, and consistently.

The challenge with risk management is that it is an inexact science. It can easily be said that risk management provides a low level of precision, but it is the best tool we have to justify our security program.

Figure 2-2 shows the tiers of risk and describes how risk is addressed at different levels in the organization.

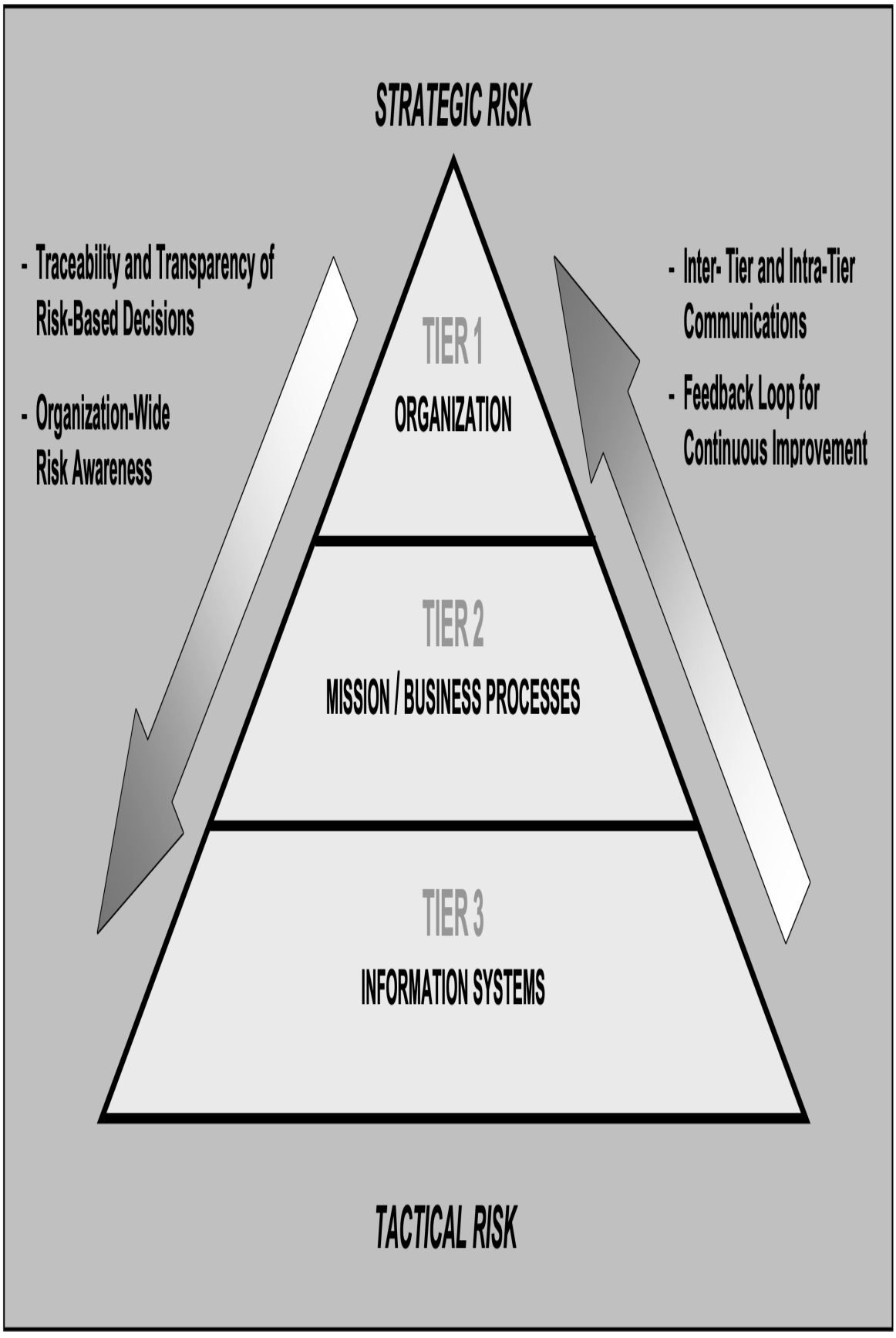
STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
- Inter- Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

*Figure 2-2. Structure of organizational risk as per NIST SP800-39*

Tier One risk is risk that would affect the entire organization. This is risk that affects the survivability of the organization and the ability of the organization to remain in business. Therefore, it is strategic risk. Risk that may emerge over a period of years as a market changes, an organization that operates gasoline stations is slow to implement electric vehicle chargers, a telecom company sees revenue fall from landline and long-distance telephone charges, a company that manufactures or repairs typewriters sees their market disappear. If an organization does not adapt, transform or re-invent itself, it may quickly fall from being a market leader to being obsolete and bankrupt. The primary responsibility for managing this risk is the board of directors and senior management of the organization.

Tier Two risk is risk at a department or business process level. A call center relies on information systems to provide customer service. An organization sells their products using a web application and an interruption to the underlying information systems that those departments rely on would pose the risk that the organization cannot deliver products or services and loses sales.

Tier Three risk is the risk to information systems. What could cause those systems to fail? Hardware? Software? Network outages? Mistakes? Configurations? Attackers? The examination of information systems risk is the identification of all forms of threats that could impact information system operations.

This diagram shows how information systems failures can lead to business process failures, and business process failures can affect strategic or organizational survivability.

That is why it’s important that there is continuous communication from the lower levels up to the very top of the organization. This allows senior management to be aware of issues or problems that need to be addressed at lower levels.

Direction and risk-based decisions are passed from the higher tiers to the lower tiers. The business, for example, mandates to the information systems level to ensure redundancy, resilience, and required levels of performance, and tier one directs risk-based decisions to tier two. This directs the business mission and business processes to adapt and change to a different strategic business direction.

This diagram clearly shows the management of risk right from a strategic to a tactical level, and, as we will see later on in the monitoring and reporting part of this chapter, communication between the tiers allows for proper risk governance. This enables the senior management team to properly execute their responsibilities as risk owners and ensure that risk is properly managed at both the business and information systems level.

## The Steps in Risk Management

As shown in the earlier diagram, there are four steps in the Risk Management Process. Each step is interrelated in that each step supports, and depends on, the other steps.

### Frame Risk

This step is at the center of the risk management process. All other steps link to and are both driven by, and communicate with, this step. In other risk management

methodologies this step has been called ‘scope’ or ‘context.’

Figure 2-3 summarizes some of the factors that influence the Frame Risk step.

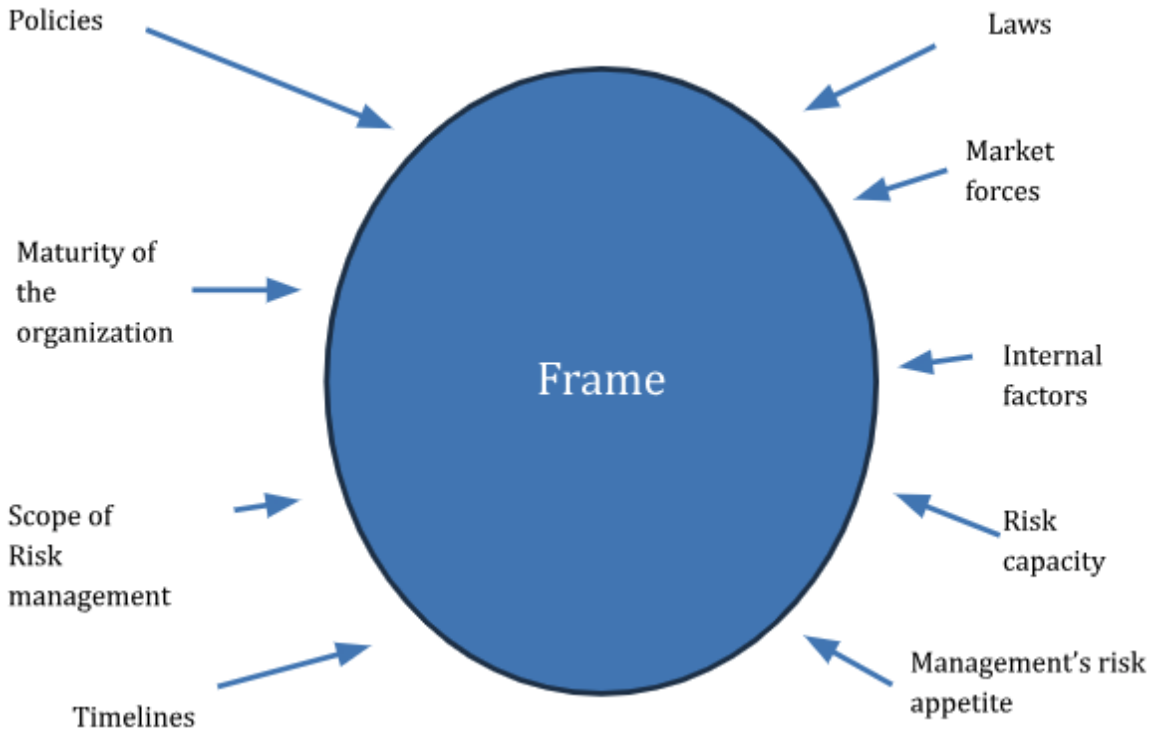


*Figure 2-3. Factors that Influence the Risk Frame*

Many risk management projects fail to deliver value to their organisations. There can be many reasons for this, put perhaps some of the most common reasons are poor project management and a lack of support from senior management. Structured project planning can help avoid many risk management project failures, and perhaps one of the main reasons for failure has been the incorrect determination of project scope.

The project manager needs to manage scope and prevent the problems associated with scope creep, where the scope of the project grows in an uncontrolled and unsustainable

manner; or conversely. the failure to adequately address all areas within project scope.

The determination of scope for a risk management project scope has to consider “should the scope of the risk management effort be based on an individual information system, or on a specific business process, or a department, or one geographic location?”

Scope should be determined so that the scope of the project is of a manageable size - yet not so small as to be repetitive. In some cases, the scope may be determined by management requesting the review of a certain system or a certain process.

Other factors that influence the frame step are laws, or changes in regulations, that can require an assessment of risk and compliance. Other internal factors, such as financial pressures, age of systems and equipment, availability of skilled personnel, and new projects that are being planned can influence the focus, scope, and objective of the risk assessment.

In planning a risk assessment, the risk and security professional must seek an understanding of many risk factors, such as risk capacity and organizational maturity. Risk capacity measures the ability of the organization to absorb loss. Management of the organization may want to take on a large risk, but the organization simply does not have the financial strength to do so.

The maturity of the organization, including the presence of policies and market forces that can drive require changes in the organization also influence the approach to managing risk.

One of the most important outcomes of the frame step is to have a clear understanding of management’s appetite for

risk. The next step in the risk management process is to conduct risk assessments, and to provide management with a risk assessment report that identifies and prioritizes risk. It is critical that the risk assessor knows management's risk appetite so that the risk assessment reports will align with management's priorities and provide value to the organization.

## Assess

The assess step of the risk management methodology is driven by the criteria and scope of the risk frame step as seen in Figure 2-4.

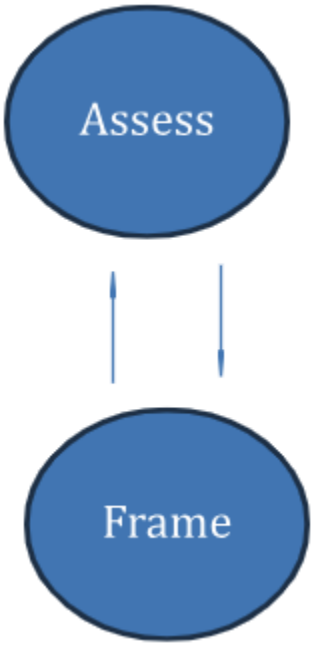


*Figure 2-4. Relationship between Risk and Controls*

The assess step identifies and prioritizes risk. The outcome of the assess step is a risk assessment report that is, initially, provided to management through communicating the results of the risk assessment back to the Frame step. Management can then accept or reject the risk assessment

report. Rejection of the report could be because management does not agree with the results of the assessment including risk prioritization, risk levels, or risk-related recommendations. The rejection of the report could require the risk management team to conduct a re-assessment of the risk. This re-assessment may result in an iterative process where the risk assessment is re-calculated until management accepts the risk assessment report.

## Determination of Risk

Figure 2-5 from NIST describes the risk assessment process. We will step through each of these steps as we examine how to conduct a risk assessment.

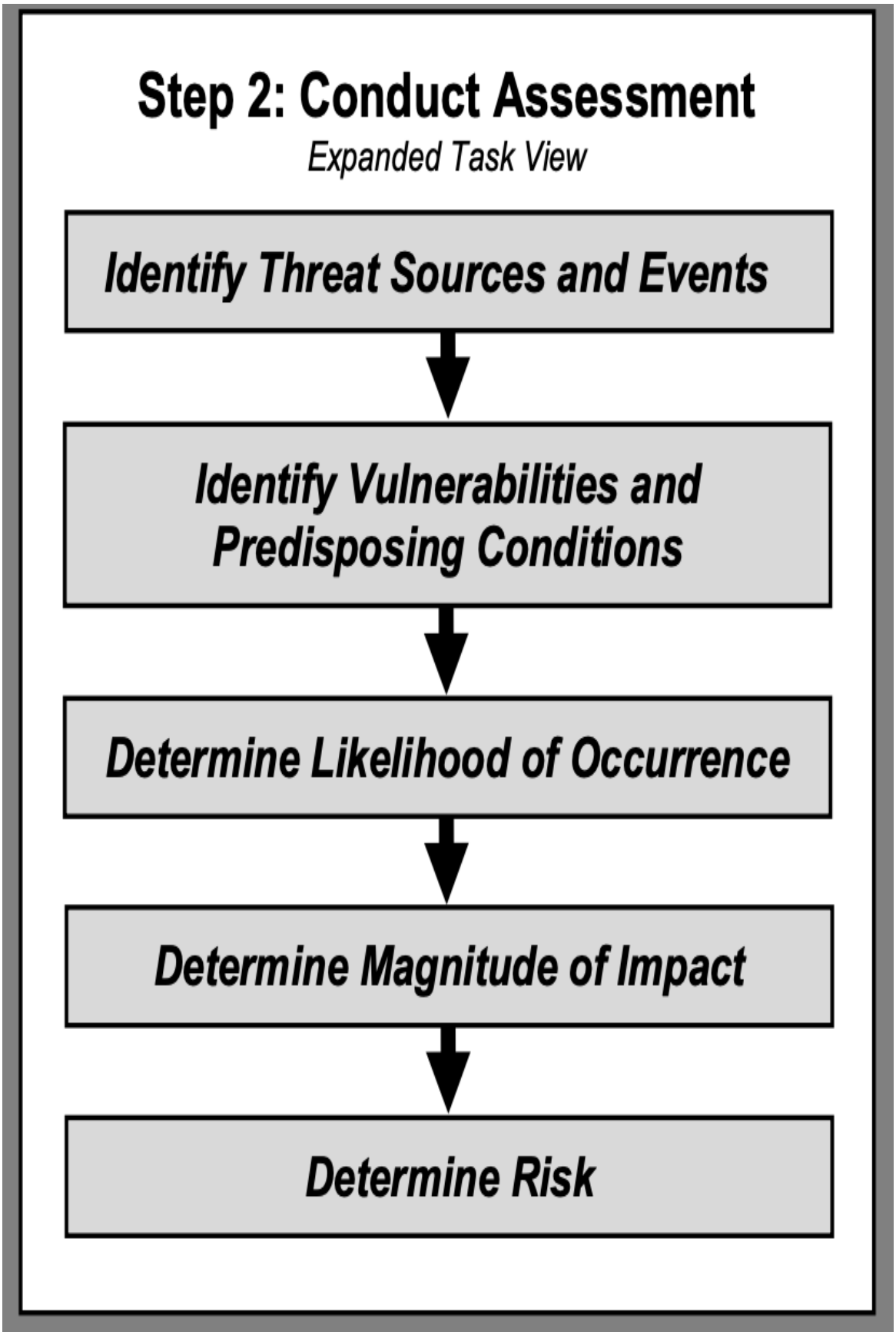
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk

*Figure 2-5. Risk Assessment process as per NIST SP800-30r1*

Risk is based on the likelihood and potential for an adverse event to impact the value of an asset. This requires the determination of asset value and the calculation of the consequence or impact on asset value of various types of adverse events. As described earlier it can be difficult to properly determine the value of assets – and, as covered in the CISSP Asset Management chapter, the first challenge is to discover and document which assets an organization has. Many server rooms are full of equipment that was installed years earlier, but no one knows what that equipment does, or supports, until it breaks.

An asset is an item that is of value to its owner. ISO/IEC27005 divides assets into two categories:

- Primary/business assets – information or processes of value for an organization
- Supporting assets – components of the information system on which one or several business assets are based.

Asset value is often related to criticality. In other words, how essential is the asset to business operations? In that case, the value of the asset can be calculated on the cost to the business if the asset was unavailable, not just on the value of the asset itself, but rather on the value to the business process that depends on that asset.

Determination of the value of supporting assets also has to include the identification of dependencies. A primary/business asset may be dependent on a supporting asset. This dependency may be hidden and not obvious at first glance, and yet if there is problem with a supporting asset, the primary asset may be severely impacted.

The identification of supporting assets may often be described as *discovery*. The risk practitioner and security manager have to probe and discover these dependencies so that the risk assessment will be accurate. An example I like to use is diesel fuel. It is relatively straightforward to recognize that electrical power is essential for information technology and systems to operate. The security manager ensures adequate power, backup batteries, and generators to maintain operations even if the normal power supply is interrupted. But in a large-scale crisis, diesel fuel may be hard to acquire, and the generators are useless without fuel. It is easy to check, ‘Is there backup power?’ while doing a risk assessment but did the risk practitioner also dig deeper to ensure that fuel supplies are arranged. As information system managers, it is easy to overlook something that is the responsibility of another department and find that the organization is vulnerable to an undiscovered risk.

Risk management can easily be understood when we consider the risk associated with driving a vehicle, for example, a car. The car itself has a certain value. This value can be related to the cost of replacing the car if it was damaged. But that is not an accurate way to calculate the value of the asset - the car. We know that a car can be used to carry a family, drive to work, go on a vacation, get to a doctor’s appointment, and thereby provides an important service to its owner. The risk assessment of a car accident may consider the car to have minimal value, but the impact on the owner and the owner’s family can be catastrophic. Even an inexpensive car can be essential to get to work and generating income but even a minor accident could lead to serious injury to the passengers in the car. Therefore, calculation of risk must consider not only the value of the

asset itself, but also the impact that the loss or damage to that asset would have on the bigger picture.

This is where the risk practitioner, the security manager, and the IT manager often stumble during risk management. These managers' natural tendency is to calculate risk based on the impact of the risk event on the device itself whereas, the true impact of risk is measured by the value that device provides as it supports the business. A failed hard drive may only cost a few hundred dollars to replace – but the interruption to a critical business application caused by that failed hard drive could be significant.

## Threat Actors

The determination of risk continues by understanding the sequence of factors associated with a risk event. Figure 2-6 describes the risk event chain.

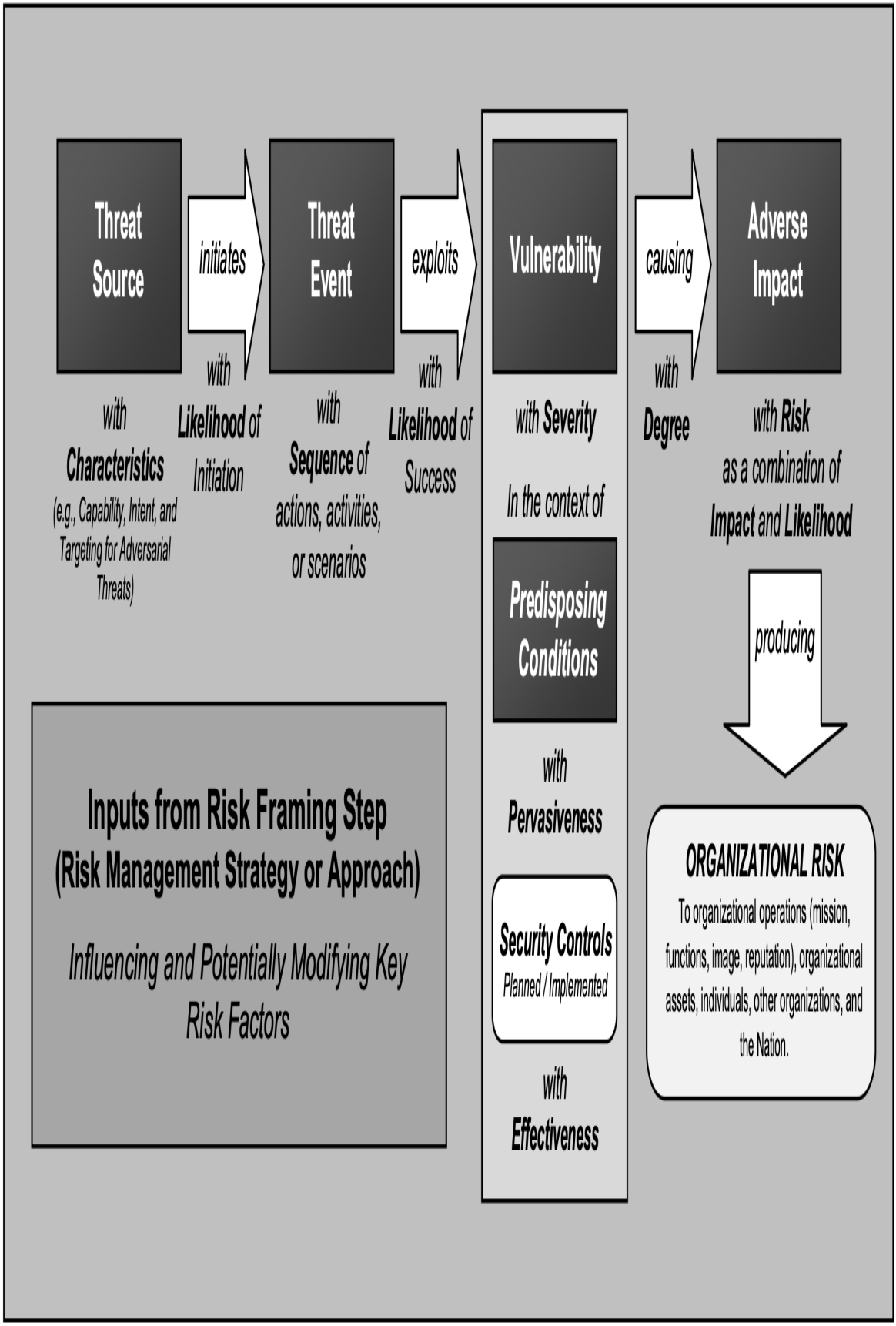
Threat Source
initiates
Threat Event
exploits
Vulnerability
causing
Adverse Impact
with Characteristics (e.g., Capability, Intent, and Targeting for Adversarial Threats)
with Likelihood of Initiation
with Sequence of actions, activities, or scenarios
with Likelihood of Success
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls
Planned / Implemented
with Effectiveness
with Degree
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.
Inputs from Risk Framing Step (Risk Management Strategy or Approach)
Influencing and Potentially Modifying Key Risk Factors

*Figure 2-6. The Risk Event Chain - Process of Adverse Attacks as per NIST SP800-30r1*

Information technology and security risk assessment begins with the identification of threat actors. A threat actor (sometimes referred to as a threat source) is an entity which poses a risk to an asset.

The risk practitioner needs to identify the sources of threats. This includes identification of the characteristics of the threat source. Is the threat source an advanced persistent threat (APT) that is highly skilled and determined, and perhaps supported by another government or criminal organization? Or, is the threat source a hacker seeking notoriety and recognition? As described in the book, *The Art of War*, it is important to know our enemy or our adversary and to understand their capabilities and intentions.

Threat actors may be internal, (employees who make a mistake), or external, (adversaries who intentionally cause harm). A threat event may be accidental or intentional, as when an external customer may unintentionally cause a risk event by entering the wrong data on a website. A risk may also be the result of a natural event, such as a storm; or the risk may be circumstantial for example when there is a fire in a building next door to ours and it interrupts our business even though we did not have a fire.

To be a good risk manager requires creativity and the ability to identify the threat actors and the tools or methods they use. In this regard, both ISO 27005 and NIST special publication 800-30 have a very good list of threat actors that the risk practitioner should review and consider.

The next step in a risk event is the threat event. Threat actors themselves are not a risk until they have a method of

causing damage. An employee that has low levels of permission is not really a threat of accidentally deleting a file because they do not have adequate permissions to initiate a damaging threat event. A hacker that would like to steal or cause damage is not really a threat until they have access to malware or some other tool used to initiate an attack. In most cases, there is little that the risk practitioner can do about threat actors or threat events. There will always be thieves and employees that cause damage, and the objective of the risk practitioner is to protect against the activities of the threat source since the threat itself cannot be eliminated.

## Vulnerabilities

The next step in risk assessment is the discovery of vulnerabilities. A vulnerability is a gap or a weakness in the security fabric protecting the asset. A vulnerability could be exploited by the threat actor causing the risk event and resulting in damage to the asset. This is shown in the diagram above.

There are many vulnerabilities that the risk and security manager need to be watchful for. When a captain of the guard is responsible to protect a walled city, the captain walks around the walls and checks if the doors are locked, the sentries alert, and the preparations ready to repel an attack. The captain will also approach the city as if they were the attacker. Where would the attack happen? The captain wants to understand what the attacking general would do if they were to attack so that any vulnerabilities can be discovered and addressed. The information security manager will look for vulnerabilities in hardware (old equipment), software (bugs), networks (misconfiguration), personnel (untrained or disgruntled), facilities (flooding),

and organizational processes (lack of roles and responsibilities). Many vulnerabilities are listed in ISO27005 and NIST SP800-30r1. These serve as a prompt the security manager can use to ensure that vulnerabilities are discovered before the attackers do. Doing regular vulnerability assessments is key to maintaining a sense of watchfulness and diligence.

## Likelihood of Attack Success

When the risk practitioner is examining the potential for a risk event, where a threat source initiates a threat event, the factor of *likelihood* is brought into the risk assessment process. Likelihood pertains to the potential frequency of an attack. The more frequently an attack is likely, the more diligent the security manager must be to thwart the attack.

Most attacks will fail. There can be thousands of attacks, and probes, every day seeking for a vulnerability to exploit. But most of these attacks are unsuccessful and blocked by security controls. An attacker may try to exploit a vulnerability that does not exist. This happens when an attack aims at a vulnerability in an application, but the organization has already patched the application. The reality is, however, that numerous studies has shown that over twenty percent of all *business* devices connected to the internet are more than a year behind on their patches, leaving all of those devices vulnerable to an attack.

When a threat is able to exploit a vulnerability then there maybe damage to the asset. The determination of risk is to determine what is that potential level of impact and the expected frequency of the attacks.

## Predisposing Conditions

But as seen in the Risk Event Chain diagram there are other factors associated with vulnerabilities. These include predisposing conditions and security controls. Ideally, security controls will be robust and effective enough to prevent or reduce the impact of an attack.

Predisposing conditions are another important consideration for the risk practitioner or security manager. The same type of risk event could happen to different organisations and yet result in a completely different level of impact.

In one case, an organization has a team of highly skilled and motivated security experts that diligently protect, detect, and respond to a risk event, thereby ensuring that the risk event is quickly contained. The same risk event that happens to another organization can have a completely different result. The other organization lacks security experts and is not monitoring systems affectively. The same type of adverse event that affected both organizations has a completely different level of impact. In the first organization the risk event was quickly identified and contained, but in the second organization the adverse event spreads rapidly causing severe damage to the organization. When assessing risk, the risk practitioner must consider the presence, and effect, of predisposing conditions that could greatly influence the impact of a risk event. Some pre-disposing conditions to be considered include employee morale, loyalty, media attention, financial strength, customer relations, and supply chain vulnerabilities.

## Likelihood and Impact

There are two parts of risk assessment that are very difficult to calculate. The first is the likelihood, or the anticipated frequency, of risk events. Every information system should expect to be attacked and built to resist the attack. But there are many types of risk events besides intentional attacks, ranging from equipment failure to loss of power. The determination of likelihood begins with a review of what has happened before - historical events. A risk event that has happened previously contains a wealth of information that can identify and improve risk management. A review of previous incidents can expose vulnerabilities, uncover problems with monitoring, and assist in the development of better incident response.

The next step in determining likelihood is to identify potential future events. This can be a challenge when performing a risk assessment on a new technology or business process where there is no historical data available. Likelihood increases when hackers are focusing on one type of target such as a specific application, or an industry sector.

Calculation of impact is equally difficult. In part, this is because impact can change every time there is a risk event. As an example, in a region of the world where there is a lot of snow, it can be quite common to become stuck in the snow. But the impact is usually minimal. In a few minutes, the driver can extricate his vehicle from the snow and continue on his way only losing a short amount of time, and with no real damage to the asset (the car). But, sometimes, when driving on an icy road the driver may hit a tree, or other vehicle, and in that case the damage can be severe. The challenge for the risk practitioner is to calculate what the level of impact of a risk event might be.

## Types of Risk Assessment

There are two methods of conducting risk assessment that are commonly used. Quantitative risk assessment is based on monetary values and mathematical calculations. Qualitative risk assessment is based on scenarios and arrange of different levels of impact and likelihood.

### Quantitative risk assessment

Quantitative risk assessment attempts to put a monetary (dollar) figure on risk. This is useful later in the *risk response* step when the risk practitioner has to recommend the selection of a risk mitigation control. Having a monetary value for risk assists in justifying the expense of the control. Quantitative risk assessment uses three mathematical formulas to calculate risk.

The three formulas used are:

SLE = AV * EF

ARO = Incidents / Year

ALE = SLE * ARO

*Single Loss Expectancy (SLE)*

This is the calculation of *impact* (consequence) of a risk event. The expected loss of a single event (single loss expectancy (SLE)) is equal to the value of the asset (AV) multiplied by the exposure factor (EF). The exposure factor is the percentage of asset value lost due to the single adverse event.

For example:

A house is worth $200,000 and experiences a fire that decreases asset value by 40%. The formula would be:

$SLE_{(fire)}$ = 200,000 * 40%

$SLE_{(fire)}$ = $80,000

This is a calculation of expected loss from this single event (a fire) – maybe based on historical data from similar houses and fires, the cost of re-building, the cost of temporary housing etc.

The single loss expectancy should be calculated for all realistic and anticipated threats – in this case flooding, theft, hail, water pipe leakage, etc. In the case of Information Systems risk this would include calculations of anticipated loss due to equipment failure, user error, malware, network failure, loss of power, etc. For each type of threat, the calculation of SLE may differ. The numbers used may be difficult to calculate since the same type of event may have different levels of impact. But using defensible arguments, the risk practitioner can provide a general value that can be used in the selection of risk response.

*Annualized Rate of Occurrence (ARO)*

This is the calculation of *frequency* (likelihood) of an event using one year (annual) as the common basis for calculations. This is useful because most security budgets are annual and the determination of the cost or impact of a risk event per year allows the comparison of impact for events that happen weekly as compared to events that may happen once in five years.

ARO = incidents / year

For example, insurance statistics estimate that there will be claim against a house insurance policy once every

twenty years (it is actually 22 years, but let's make the calculation simple).

So, the calculation of frequency is:

$ARO_{(fire)}$ = 1 incident / (in/per) 20 years

$ARO_{(fire)}$ = 1/20

Again, there are many types of incidents – all occurring at various frequencies. A fire may happen once every twenty years, whereas equipment failure may happen once every five years and a user error once a week. So $ARO_{(user\ error)}$ is greater than one and ARO of equipment failure is less than one.

$ARO_{(user\ error)}$ = 52

$ARO_{(equipment\ failure)}$ = 1/5

*Annualized Loss Expectancy (ALE)*

ALE represents the anticipated loss due to an adverse incident per year.

ALE = SLE*ARO

ALE is equal to the cost/impact of a single event (SLE) multiplied by the frequency of that event (ARO).

For example, from our earlier calculation of a house fire resulting in a claim against the insurance policy:

ALE = SLE*ARO

ALE = $40,000 * 1/20

ALE = $2000/year

This provides valuable quantitative data that can be used by an insurance company that issues a house insurance policy to determine the approximate risk/cost/liability to

the insurance company of an insurance claim on an annual basis. Some fires will cost more – and many other fires will cost much less. So, this is an average and over a large population provides the data needed to calculate how much a house owner will be required to pay per year for their house insurance coverage.

As a side note for the examination, the examination candidate may be asked to perform simple calculations like the ones shown here that should not require the use of a calculator.

Quantitative risk assessment works very well when there is a sufficient quantity of empirical data to estimate costs (impact) and frequency (likelihood). But quantitative risk assessment requires the risk assessment team to possess greater levels of experience, than qualitative risk assessment requires. And, quantitative only considers hard data – money. Its calculations completely miss the impact of damage to reputation, morale, customer confidence (all of which may come back to money or impact future earnings) but were not part of the initial quantitative calculation of risk. As has been seen many times in the past, the cost to repair a reputation can be significantly higher than the cost to repair the damage from the incident itself. Therefore, the risk practitioner should also deploy a qualitative risk assessment methodology.

## Qualitative Risk Assessment

Qualitative risk assessment works well even with inexperienced members of the risk management team. Qualitative risk assessment is often based on scenarios and levels, or a range of different tiers that measure impact and likelihood.

Figure 2-7 is an example of the comparison of likelihood and impact from NIST SP800-30r1:

| Likelihood (Threat Event Occurs and Results in Adverse Impact) | Level of Impact | | | | |
|---|---|---|---|---|---|
| | Very Low | Low | Moderate | High | Very High |
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |

*Figure 2-7. Qualitative Assessment of Risk as per NIST SP800-30rev 1*

The challenge with this process is to determine the definitions of very low. low, moderate, high, and very high in a consistent way across the enterprise. For a person like you or I, the impact of losing a hundred dollars may be

high; but for a large organization a loss of $100 may be considered to be very low. So, the risk practitioner has to define what these levels represent in a manner that is meaningful to the organization and useful for risk response and the selection of risk mitigating controls. Each level should be defined as a range of values. For example, *very low likelihood* may be defined as events that occur less than once in five years or more. *Low likelihood* many be defined as events that occur once between one to five years. *Moderate likelihood* can be defined as events that occurs less than once a month but more than once a year. *High likelihood* could be based on events happening once a month or more and *very high* based on daily events. Similar ranges can be used for levels of impact as well, based on a range of monetary costs or impact on people or operations.

For example:

The risk practitioner and security manager want to assess the risk of loss of email services. They would then create a scenario or description of an event that could impact email availability (maybe based on network problems, hardware problems, or user error) and proceed to ask the personnel in various departments what the impact on their business operations would be if email was not available for an hour? How about if email was down for four hours or a day?

The business units may review what the impact has been if there was an email outage in the past, or they may estimate the level of impact if it were to happen in the future. Maybe the last time a risk assessment was conducted, the outage of email would have been more severe than it would be now, or less, depending on how the business has evolved since the last risk assessment was conducted. The business personnel would provide a response to the risk practitioner

of whether the impact of email outage would be very low, low, moderate, high, or very high.

The responses provided by the business will vary. In some departments the loss of email would be critical – it is a primary means of communicating with customers and co-ordination of operations. For another department, the loss of email for an hour or two may have little or no impact, or, as sometimes speculated, maybe productivity would actually increase if email was down for a few hours every day.

Once the responses from the various departments have been received, the risk practitioner and security manager need to collate and analyze the results. Using professional judgement, they will determine whether the impact of this event (email outage) would pose a very low, low, moderate, high, or very high impact on the overall ability of the business to reach its goals.

The next calculation is of frequency, or likelihood, of an email outage. Historical data can be useful here. How frequently has there been an email outage? What was the level of impact?

But for a new technology there is no historical data, so the risk practitioner has to make an estimate, perhaps based on other technologies, or other incidents. As one security expert likes to say, ‘Risk management is a very inexact science – but it is the best we have to work with.’

To calculate frequency a common basis should be used to define what is a very low frequency, as compared to the other levels.

Using our example scenario of an email outage, let’s assume that, upon analysis, the impact of an email outage

across the organization was rated as moderate, and the frequency was rated as high, as shown in Figure 2-8.

| Likelihood (Threat Event Occurs and Results in Adverse Impact) | Level of Impact | | | | |
|---|---|---|---|---|---|
| | Very Low | Low | Moderate | High | Very High |
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |

*Figure 2-8. Determining Risk Prioritization*

Figure 2-9 shows a Qualitative risk assessment of the level if impact of an email outage is “high”.

| Likelihood (Threat Event Occurs and Results in Adverse Impact) | Level of Impact | | | | |
|---|---|---|---|---|---|
| | Very Low | Low | Moderate | High | Very High |
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |

*Figure 2-9. Comparison of Likelihood to Impact from NIST SP800-30rev1*

Qualitative risk assessment that the likelihood of an email outage would be high.

### *Qualitative Risk Determination*

The determination of the level of risk would be where these two factors of likelihood and impact intersect as seen in

Figure 2-10.

| Likelihood (Threat Event Occurs and Results in Adverse Impact) | Level of Impact | | | | |
|---|---|---|---|---|---|
| | Very Low | Low | Moderate | High | Very High |
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |

*Figure 2-10. Determination of Moderate Level Risk based on Likelihood and Impact as per NIST SP800-30rev1*

This indicates the anticipated severity and, therefore, the priority of the risk of an email outage is moderate. Other risk events may be very high, or high, and they should be addressed before any steps are taken to mitigate a

moderate level risk. But mitigating the moderate level of risk of an email outage would take precedence over other risks that are only rated as low, or very low.

The challenge with qualitative risk assessment is that it does not provide monetary values. When the security manager is seeking budget to be able to mitigate risk, they have to justify the cost of security through cost-benefit analysis. Justification of the budget is based on the monetary benefit of risk mitigation. It is difficult to justify or obtain a security budget based on a *qualitative* risk assessment that merely states that the risk level is moderate or high, for example.

We have addressed two primary methodologies to conduct a risk assessment: quantitative risk assessment, based on money; and qualitative risk assessment, based on levels or ranges of risk. Neither methodology is perfect. Therefore, an other way that people attempt to conduct a risk assessment is the use of a semi-quantitative risk assessment approach.

## Semi-Quantitative Risk Assessment

One method used to overcome the weaknesses of both quantitative and qualitative risk assessment is to adopt a semi-quantitative risk assessment approach. The semi-quantitative approach to risk assessment uses a bell curve that considers that most risk is at a moderate level, and risk that is either high or very high is one or two standards of deviation beyond the mean or the average level of risk. Risk that is either low or very low is one to two standards of deviation below the average level of risk this is quite often seen in a bell chart. By far the majority of quantitative values of moderate risk would be translated into a semi quantitative level of between 21 and 79 on a

scale from 1 – 100 when conducting a risk assessment. That would allow more accurate recognition of those risks that are either beyond or below a normal distribution of risk. Figure 2-11 shows the conversion from Qualitative to Semi-Quantitative Values:

| Qualitative Values | Semi-Quantitative Values | |
|---|---|---|
| Very High | 96-100 | 10 |
| High | 80-95 | 8 |
| Moderate | 21-79 | 5 |
| Low | 5-20 | 2 |
| Very Low | 0-4 | 0 |

*Figure 2-11. Semi-quantitative Risk Levels as per NIST SP800-30rev1*

## The Conclusion of the Risk Assessment Phase

The conclusion of the risk assessment phase is the generation of a *risk assessment report*. The risk assessment report lists all of the risk identified during the risk assessment and prioritizes the risk so that risk of a higher level are considered during the risk response phase before lower-level risk.

## Management Review of Risk Assessment

The risk assessment report is provided, first of all, to management for comments and review. It can be that management does not agree with the contents of the risk assessment report and sends it back to the risk assessment team for review and (possibly) correction. The reason for the rejection of the report could be an error in the calculation of risk appetite or asset value that affected the prioritization of the risk; or disagreement over threats or calculations of likelihood or impact. The senior management of the organization *owns* the risk. As the risk owners they are accountable for the risk and as risk and security professionals we provide advice. The risk and security managers are expected to provide a professional assessment and be able to justify the contents of the risk assessment report - but in the end it is the decision of senior management to act upon risk as they, as the risk owners, see best.

Once the risk assessment report has been accepted by management it provides the foundation for the next phase in the risk management lifecycle, the risk response. This

step is also known in some standards as the risk treatment phase.

### Risk Register

The risk register is an important repository that lists and preserves all the known risk of the organization in one common location. Risk is identified through many different business activities, including audits, vulnerability assessments, penetration tests, incident management, business continuity tests, security monitoring, and risk assessment. Whenever a risk is identified it should be added to the risk register. Having all risk listed in one place facilitates the management of risk and the ability to review the current risk profile of the organization.

A risk register can be created using a commercial tool or be as simple as a spreadsheet. Each identified risk is added to the register, and the entry contains a description of the risk, the source of the risk, the risk owner, the priority, and the status of the risk. As a risk is mitigated, the status is updated to show the risk as resolved.

## Risk Respond

With the completion of the risk assessment step, it is time to move on to the risk respond step. The goal of risk response is to ensure that all risk is managed to a level acceptable to management.

The risk respond step relies on the data provided by the risk assess step via the risk assessment report; and on the input and direction from management as represented in the frame step.

The risk assessment report identified and prioritized risk. This report provides the basis for making the risk respond decisions.

As seen in Figure 2-12 of the Risk Management Process, the lines of communication between all the steps are essential. What is done in one step affects the operation of the other steps.

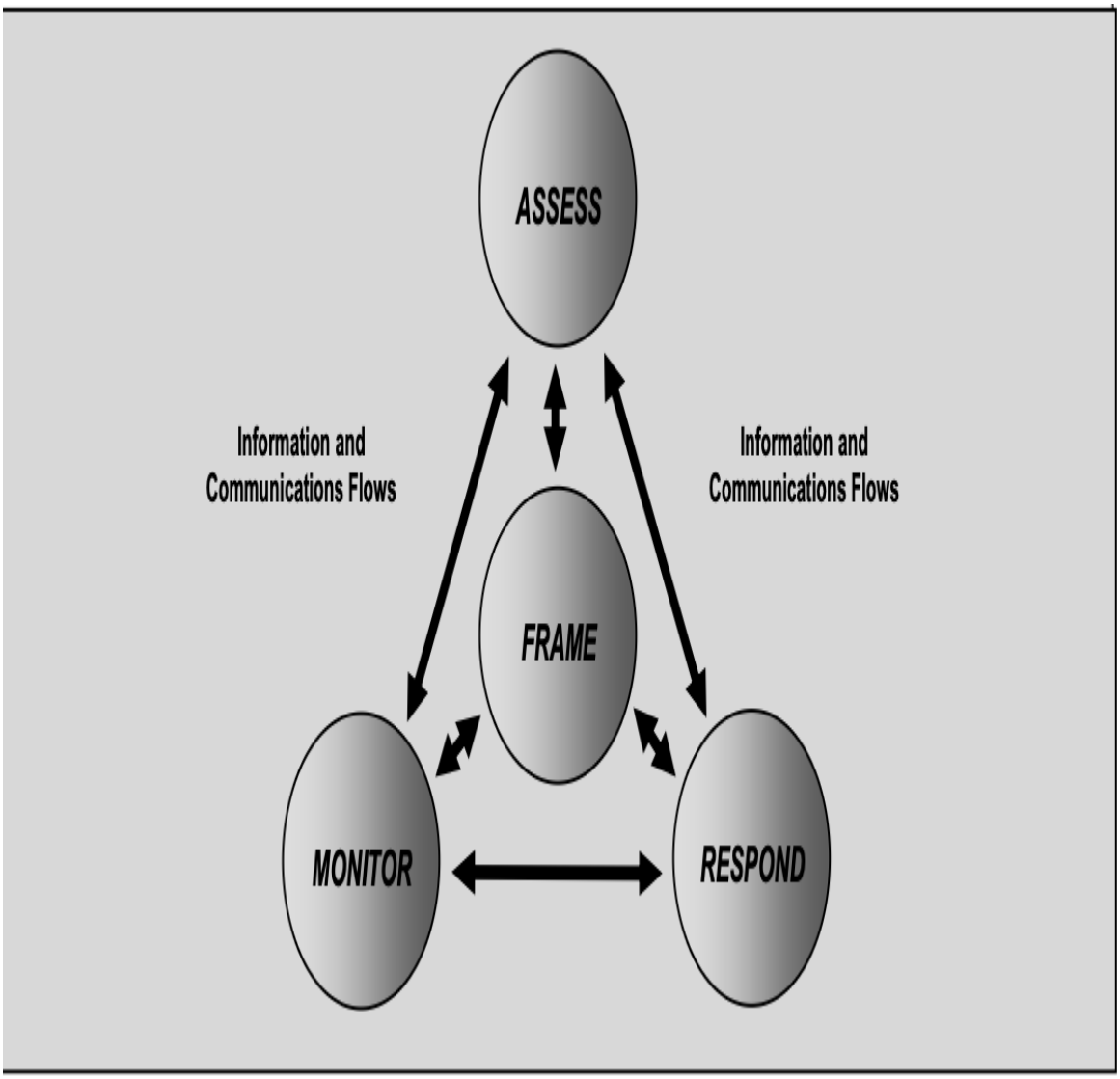


*Figure 2-12. Risk Management Process as per NIST SP800-30rev1*

The risk assessment report is represented in the information and communication flows between the assess

and respond steps. The direction and decision-making function is represented by the communication flows between management, in the frame step, and risk and security professionals in the respond and assess steps.

## Risk Ownership

The first requirement in the risk respond step is to establish or verify who *owns* the individual risks. Risk ownership must be assigned to a manager with budgetary authority, quite often from the area most affected by the risk. Risk to financial systems is usually owned by the chief financial officer, whereas risk to IT systems is owned by the chief information officer. The security professional rarely owns the risk instead the security professional must ensure that the risk owner has been adequately informed of the severity of the risk and the options available to mitigate or to address the risk.

In the end if the risk owner decides not to accept the advice of the security professional that is the manager’s right. The manager is accountable for the risk, and the security professional is responsible to provide sound (solid) and professional advice to the manager that owns the risk.

The risk assessment report listed the risks and priorities of the risks, and the responsibility of the security manager is to determine the *appropriate* response to the risk. In the end, the goal of risk management is *adequate* security. Adequate security is a term used frequently in standards to describe a level of security which is sufficient but is neither excessive nor insufficient to address the risk in a responsible and accountable manner.

## Risk Respond Options

There are usually four options considered when responding to risk. The risk owner may choose to accept, avoid, transfer or reduce (mitigate) the risk. The risk response often uses more than one of these options. The risk owner may choose to *reduce* the risk as much as they can, but then to *accept* the risk that still remains. The choice of risk response options is made by the risk owner based on the level of risk the owner is willing to accept, the availability of cost-effective controls, the prioritization of the risk, legal or regulatory requirements, and other projects or upcoming changes in the business.

The initial level of risk described in a risk assessment is known as the *total risk.* This is also known as the *inherent risk*, that is the level of risk prior to the implementation of any controls. When controls are introduced, the level of risk is reduced and the level of risk that remains after the benefit of the control is implemented is known as the *residual risk*. The residual risk is the remaining risk and is not necessarily the same as *acceptable risk*. Acceptable risk is the level of risk that the risk owner is willing to accept, whereas residual risk is the real level of risk that remains.

## Risk Acceptance

The goal of risk response is to ensure that all residual risk is less than or equal to acceptable risk. For example, a friend asks to borrow $50 because they forgot their wallet and need to buy something. If you loan them the money, then you know that that asset ($50) is the total asset at risk. Perhaps it will never be re-paid. But since it is for a friend, you are willing to accept that loss. In fact, if the friend had asked for $100 you would have lent it to them

based on your willingness to accept a risk of up to $100 for a friend. But since the amount you lent them was only $50, the ‘real’ risk was only $50.

The owner (you) of the asset (money) would have accepted any risk up to $100. So, *risk acceptance is based on a range of values* from zero to $100. This is also where *risk capacity* is a factor. A friend may ask for money, but you cannot lend it to them because you do not have any money to lend.

If the friend that asks for $50, says, “I will write a note that reminds me to pay you back,” that is a control known as an administrative control. A control addresses a risk and, in this case, reduces the likelihood of not being paid back. The control (the note) can remind them and can be used to hold them accountable for the money.

Let’s say the friend offers you a gift card that they have for a local shop for $25. This gift card would not work where the friend needs to shop today, but the friend says, “Here is a gift card for $25 you can have so that if I am not able to pay you back at least you have part of your money.” That means that you have reduced your total risk of $50 by a control that only leaves $25 at risk. The total risk of $50 has been reduced through a control (the gift card) to $25. That $25 that is still at risk is the *residual risk*, that is the risk that remains after the implementation of a control.

The goal of risk management is to ensure that the level of risk is acceptable to the manager, the risk owner. Only the risk owner can accept risk, and no one else can accept risk which they do not own. In accepting the risk, the risk owner understands that they are accepting the consequences of any risk event associated with that risk.

In some cases, risk acceptance also has to do with the availability of a cost-effective solution. It can be that there are no valid solutions to reduce the risk to the level the risk owner would prefer to accept. By doing this, the risk owner is tolerating a level of risk that exceeds their normal risk acceptance level. This is defined as *risk tolerance*, Risk tolerance is the decision by the risk owner to tolerate a level of risk which deviates from the normal risk acceptance level.

### Risk Avoidance

Another option available to the risk owner is to *avoid* the risk. Risk avoidance is to cease the activity associated with the risk. For example, to cease business operations in an location where the where the risk cannot be reduced to an acceptable level. We often see this when a country closes its embassy and withdraws its staff from an area subject to civil war.

Risk avoidance can also be chosen where the level of risk exceeds the possible reward. If we go back to our example of driving a car on icy or snowy roads, the decision might be to stay home and not drive today due to the adverse weather conditions because the risk is too high. But, when we decide to avoid the risk, we also lose any benefits we would have realized from accepting that risk. If I choose not to drive when the weather is bad, I reduced the risk of an accident, but I also lose the benefit of visiting friends, going to work, or whatever other activity I would have engaged in if I chose to drive.

This is where we see there is a different risk appetite with each individual. A younger person may be more willing to accept risk then an older person. This applies in organisations as well. Some managers are more willing to

take a risk than others, and since the managers own the risk, the security professional must adjust their risk response recommendations according to the manager who owns the risk.

## Risk Transference

Another risk response option is to transfer or share the risk. An example of this is to purchase insurance. When a person purchases insurance then the insurance company is accepting the risk based on the payment of an insurance premium. In this case, the insurance company would be responsible for a portion of the impact of any risk event in accordance with the terms of the insurance policy. But in many cases, an insurance policy does not cover the entire cost of a risk event. Instead, there is an amount of residual risk which remains to the company that purchased the insurance premium. For example, with car insurance the driver of the car would still be responsible for paying an initial cost for any claim, while the insurance company covered the remainder. In some countries, this initial amount that the insurance policy holder must pay is known as the deductible or in other countries, the excess.

The concept of transferring risk enables the organization to transfer some of the financial costs associated with the risk event to another party.

Another example of risk transference or sharing is when several companies work together to manage a risk. For example, when several banks work together to jointly provide finding for a large new project. The level of risk would be too high for any one bank to accept, but by having several banks involved the risk is spread amongst all of the banks. But the profits are also shared between all of the investors.

## Risk Mitigation (Reduction)

The fourth option for dealing with risk is to mitigate, or reduce, the risk. This is usually done through the implementation of security controls. Figure 2-13 shows the relationship where a risk justifies the implementation of a control.

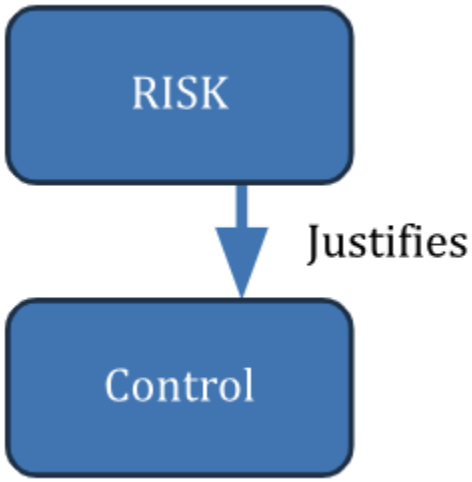


*Figure 2-13. Relationship between risk and controls*

A control is a restriction, a limitation, and a cost to the organization. A control can also pose a liability to the organization if the control were to fail. Therefore, controls should only be implemented where the control is justified based on risk. The level of control should be commensurate with the risk. In other words, the control should be appropriate to manage the risk and not excessive, or contrariwise, inadequate. We should never have a control where there is no identified risk.

Figure 2-14 shows how a risk is the result of a threat source using a threat event to exploit a vulnerability leading to damage to the asset.

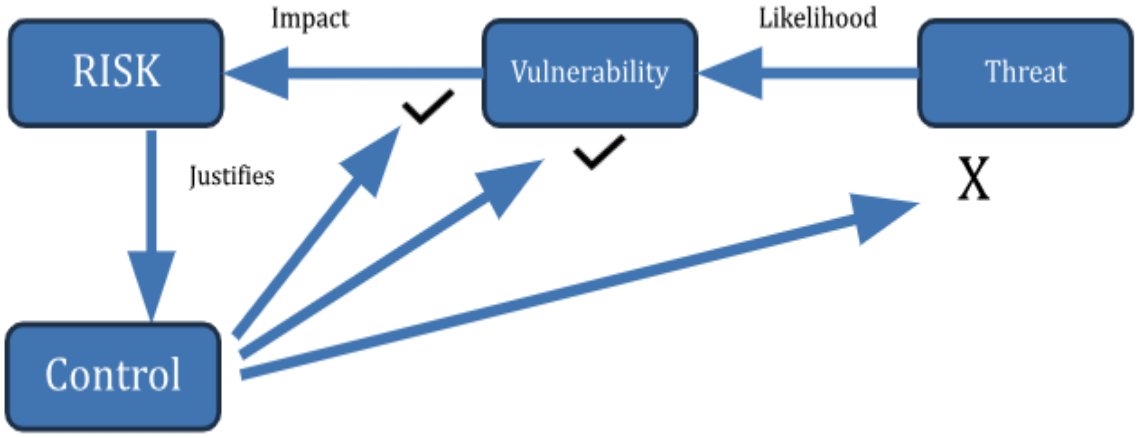


*Figure 2-14. Effectiveness of Controls to Address Risk Factors*

The identification of the risk to the asset justifies the control and the intention of the control is to reduce either the likelihood or the impact of the risk event. It is rare that an effective control can address the threat, but a control can be implemented to address a vulnerability. The removal of the vulnerability (perhaps by patching software) means that the system (the asset) is no longer susceptible or likely to be impacted by an attack.

Another objective of a control is to reduce the amount of damage or impact from the threat. This type of control minimizes the amount of the asset susceptible to the risk event. An example of this is to install fire doors in a building. In the event of a fire, the fire doors can contain the risk (the fire) and thereby reduce the impact or damage from the fire.

## Controls and Layered Defense

An example of the use of controls is to wear a seat belt as a passenger in a car. The seat belt will not prevent an accident, but the seatbelt can minimize injury if a person is in an accident. In this way the seat belt is a reactive control that is effective once a risk event (an accident) has

happened. A seatbelt is a control that reduces the impact or consequence of a risk event.

Proactive controls are controls that aim to reduce the likelihood of a risk event happening. For example, when a driver (the risk owner) purchases good tires for their car, the tires are a control that aims to reduce the likelihood of sliding on a wet road and losing control over the vehicle.

As seen here, there are two major types of controls - proactive and reactive controls. A proactive control is used to prevent a risk event, and a reactive control is used to respond to a risk event when it happens. Frequently an organization will use both preventative (proactive) and detective (reactive) controls in a series. The proactive control will attempt to stop the attack, and the reactive control will trigger and attempt to contain and respond effectively to an attack. Using controls in a series or sequence is known as *layered defense* or *defense in depth*,

They security professional has to select the controls they recommend to the risk owner. When recommending controls, the security professional has to review which controls are available and would satisfy the risk acceptance (or *risk appetite*) of the risk owner.

In some cases, the risk mitigation option recommended by the security professional is to implement a new control. In other cases, the security professional will recommend an enhancement to existing control. There can be many control options for the security professional to consider but for each option there should be a *cost-benefit analysis* (cba) calculation that determines whether the benefit provided by the control will justify the cost of the control.

## Types and Categories of Controls

Controls are divided into two groups – proactive controls are known as safeguards. They protect (safeguard) an asset from a risk event. Reactive controls are also known as countermeasures since they counter the effects of a risk event. The security manager must be familiar with the types of controls, the criteria used to select a control, the design and implementation of a control and the monitoring and reporting on control effectiveness. The knowledge and application of controls will be tested in every domain of the CISSP.

Both proactive and reactive controls can be further broken down into three groups: managerial controls (also known as administrative), technical controls (also known as logical controls), and Physical and Environmental controls.

These three groups of controls are further divided into six more categories of controls:

- Directive controls
- Deterrent controls
- Preventative controls
- Detective controls
- Corrective controls
- Recovery controls

Not all organizations use the same names for the controls, but the CISSP has traditionally used these terms, and it is relatively easy to compare the terms used elsewhere with these terms based on the purpose of the control.

Examples of many controls are listed below, but many controls fit into more than one category. For example,

auditing is primarily a detective control that would detect a problem. But an argument can be made that audit is also a deterrent because a person may not do something wrong if they know that their misdeed would be discovered by an audit. When evaluating a control or answering an exam question be aware of both the primary function of the control (such as the primary function of audit is to detect), as well as the other possible functions of the control (such as a being a deterrent).

## Proactive Controls (Safeguards)

**Directive controls** – a directive control 'directs' or mandates the behaviors or actions of an entity. For example, a policy is an example of a managerial directive control. The policy is written and endorsed by management to advice people of what actions are permitted or not permitted as the case may be.

**Deterrent controls** – a deterrent control discourages (deters) a person from doing something wrong. For example, a sign that says 'Beware of Dog' is a physical deterrent control used to deter a person from entering a protected property.

**Preventative controls** – a preventative control attempts to block or stop unauthorized activity. A password on an information system is an example of a technical preventative control that prevents unauthorized access. Table 2-1 provides an example of each type of proactive control.

*Table 2-1. Examples of Proactive Controls*

| | **Managerial Control** | **Technical Control** | **Physical Control** |
|---|---|---|---|
| **Directive Control** | Policy | Warning banner | Do Not Enter sign |
| **Deterrent Control** | Disciplinary action | Notification of Monitoring | Beware of Dog sign |
| **Preventative Control** | Separation of Duties | Password | Fence |

## Reactive Controls (Countermeasures)

**Detective Controls –** detective controls identify and alert of suspicious activity. An Intrusion Detection System (IDS) is an example of a technical detective control.

**Corrective Controls** – when an incident or risk event happens there is often a time of chaos and uncertainty. One of the main goals of incident response is to contain the problem before it enters the rapid escalation phase and causes more damage. An example of a corrective control is a fire suppression system that contains the fire and allows the organization to regain control over the situation.

**Recovery Controls -** the purpose of a recovery control is to return to normal operations. An example of a technical recovery control is to re-build a desktop if it has been infected with malware. Table 2-2 provides an example of reactive controls.

*Table 2-2. Reactive Controls*

| | Managerial Control | Technical Control | Physical Control |
|---|---|---|---|
| **Detective** | Audit | Intrusion Detection System | Smoke alarm |
| **Corrective** | Removal of Access | Isolation of Infected Equipment | Fire extinguisher |
| **Recovery** | Training | Rebuild from backups | Rebuild damaged building |

## Selecting a Risk Response

The risk practitioner and security manager use the risk assessment report to determine the recommended response to risk. The objective of risk response is to ensure that all risk is within the range of risk that is acceptance to management. In some cases, the security manager may recommend the acceptance of risk, but where the level of risk exceeds the risk acceptance level, the security manager is expected to provide management with one or more recommended responses to risk.

The recommendation may be to avoid the risk if the risk is too high and cannot be effectively mitigated. For example, the security manager may recommend delaying the implementation of an insecure modification to an external-facing application that would make it highly vulnerable to compromise. The business may argue that there are

compelling business reasons for the modification to the application, and the security manager must be able to justify why it should not be implemented. In the end, management is accountable for the decision – but the security manager is responsible to ensure that management has been given good advice.

The security manager may also recommend the purchase of insurance to cover the costs of a risk event.

The security manager may recommend reducing the risk through the installation or modification of controls. In this case, the security manager may offer several options for management to consider. The security manager may present management with an analysis of each option, comparing cost, function, interoperability with existing systems, and maintenance and training requirements. It can be that it requires more than one control to reduce the risk to an acceptable level.

The choice of which controls to implement is frequently based on cost benefit analysis (CBA).

## Cost-benefit Analysis

Cost benefit analysis attempts to provide management with a justification for investment in a security control. The security manager calculates the benefit of the control (reduction in risk) compared to the cost of the control. This is not always an easy calculation, because cost is more than the initial purchase price. The cost of a control includes the cost to maintain the control and the impact on productivity caused by the control. A password, for example, is usually not expensive to implement, it is just checking a box that says, ‘password required.’ But what does a password cost? How many calls to the helpdesk are caused by forgotten

passwords? How much does each call cost? How much productivity is lost by employees that forgot their password and are locked out of the system until they can get their password reset? How much does it annoy our customers and employees if they have to use Multi-Factor Authentication (MFA) every time they need to log in, to the point that our customers switch to another company that provides easier log in?

Benefits are also hard to justify. How many breaches were stopped when a control was adopted? Would there have been more breaches if the control was not in place? Like all of risk management, CBA is not a straightforward calculation – but we use it because it is the best methodology available.

## Calculation of Residual Risk

Total risk is the level of unmitigated risk before any action is taken to reduce the risk. Residual risk is the level of risk that remains after the implementation of controls, The goal of risk reduction or mitigation is to reduce the level of risk to a level that is acceptable to management. In this way, residual risk is to be less than or equal to acceptable risk.

If the risk practitioner has calculated, using quantitative risk analysis, that the total risk to a building in the event of a fire is $1,000,000. And the risk acceptance level set by management is $80,000, then the risk practitioner must consider various ways to reduce the total risk to an acceptable level.

The risk practitioner assesses that to install a fire suppression system will cost about $50,000 and be about 40% effective in reducing the impact of the fire. The cost benefit analysis would calculate that for a cost of $50,000 a

$400,000 ($1,000.000 total risk reduced by 40%) benefit was obtained a cost benefit ratio of 8:1 - the benefit of $400,000 is eight times greater than the cost of $50,000).

Residual Risk = Total Risk – Control Effectiveness

Residual Risk = $1,000,000 – 40%

Residual Risk = $600,000.

A residual risk of $600,000 is much higher than the risk acceptance level of $80,000 set by management. So further action is still required.

The risk practitioner suggests that the installation of fire doors to compartmentalize a fire at a cost of another $50,000 would further reduce the risk by 30%.

Residual Risk = Total Risk – Control Effectiveness

Residual Risk = $1,000,000 - $700,000 ($400,000 for suppression + $300,000 fire doors)

Residual Risk = $300.000

It is noteworthy that the cost benefit analysis of the second control (fire doors) is less than the CBA of the first control. The CBA of the fire doors is only 6:1 ($300,000 in benefit at a cost of $50,000). This is the law of diminishing returns and is a problem for security managers and risk practitioners. The law of diminishing returns states that the benefit of controls diminishes as more money is spent on controls. In the end, the security manager can end up spending more money on a control than benefit received.

The residual risk of $300,000 after the implementation of the second control still exceeds the risk acceptance level set by management. So further action is required.

The risk practitioner suggests that the organization could purchase insurance for the building. Since the building has fire suppression systems and fire doors, the annual cost for insurance it $5,000. But in the event of an insurance claim, the organization would still have to pay the first $40,000 of damage. This is known as the deductible or excess as seen earlier in this chapter.

Residual Risk = $1,000,000 – 960,000

Residual Risk = $40,000

The residual risk is now less than the acceptable risk and the risk practitioner has met their obligation to ensure that the amount of residual risk is less than or equal to acceptable risk.

This is just an example for the sake of explaining the relationship between risk mitigation and acceptable risk. There are other factors that would be brought into this calculation such as amortization of the controls, likelihood of an insurance claim and costs such as interruption to business and lost inventory, so this is not a perfect example, but it explains important risk management concepts.

## Security Awareness Training

The most effective control to mitigate risk available to a security manager is security awareness training. Firewalls and technologies are excellent tools, but a tool is only truly effective when it is used by a competent and skilled person. Many organizations have invested and relied too much on technologies only to be disappointed to discover that those technologies were easily bypassed through human error or social engineering. This is the reason that most security standards and good practices emphasize the need for

regular awareness training for all staff, and even, in some cases, customers.

## Social Engineering

Social engineering is the practice of manipulating a person to do something that they should not do. There are several techniques commonly used in social engineering and all staff should be aware of, and alert to detect, and resist social engineering attempts.

The four most common approaches to social engineering include:

- Intimidation
- Appealing for assistance
- Name dropping
- Technical
    - Phishing

Intimidation works by threatening a person. The attacker insists that a failure by the employee to do as they ask will result in a call or complaint to management. A new employee may be especially susceptible to such as attack as they fear for their job. The attacker may create a scene, and the employee just agrees to the attacker's request to avoid conflict. This is where the awareness program needs to assure each employee that management stands behind them and will not get the employee in trouble so long as the employee follows the procedures.

Appealing for assistance attracts the urge of most people to be accommodating and helpful. When someone pleads for assistance, the natural instinct of many employees that

want to ensure the success and reputation of their companies is to be helpful and ‘bend the rules.’ This is why awareness need to expose these types of manipulations employed by attackers and explain to employees the reason for various rules and the need to adhere to procedures.

Name dropping is another common exploit technique. It is often used in email compromise attacks where an email that purports to come from the CEO insists on immediate payment for an outstanding invoice or to ‘close a deal’ the CEO is allegedly working on. The recipient of the email or phone call acts quickly and sends money or complies with the demands of the attacker. There HAVE to be procedures that are followed that prohibit this type of payment and require the review of the request before action is taken.

Technical social engineering has been around as long as technology. In the early days, a fix would be sent requesting payment, now it is email, false invoices, requests to change banking information for a supplier that sends an invoice, etc. There is a saying that pertains to this. The attacker is desperate to steal so that they can ‘feed their family’, ‘keep their job,’ or get rich. So, the attacker improves their skills and refines their techniques so that they can be successful. The question is, ‘are we as desperate to keep the attackers out, as they are to get in?’ If the attackers are more driven and desperate than we are, then it is an unfair fight, and they are almost certain to succeed. We have to refine our skills and strategies to keep them out and preserve our organizations.

## Security Awareness Programs

Awareness programs should address current threats and be updated, interesting, relevant, and varied. The goal of security awareness is to draw everyone’s attention to the

need for *everyone* (managers, employees, customers, suppliers) to participate in good security practices. Security must become a ‘culture’ not just an obligation. It *is* an obligation, but the objective of an awareness program is to change peoples’ belief systems so that they *want* to follow good security practices, not just that they *have* to. The program should explain and convince the attendees of the program to embrace security – why it is important and what they can and should do to protect themselves, their families and the organizations they work for.

People learn differently. Some learn by hearing, others by seeing, others by doing. Therefore, the awareness program should be varied using different delivery techniques to suit all learning styles. It should incentivize and reward, be interesting and relevant and provide guidance and explanations for those that want to know more, or need a topic explained before they will accept it.

Posters are great. A security poster can provide a humorous way to emphasize a point, and can be easier to understand where language barriers restrict delivery techniques. But, after a few days, posters become wallpaper and no one ‘sees’ them anymore. So, a variety of delivery techniques is needed. Introducing learning through games, examples, small gifts like a lanyard or pen, or in-person sessions with a dynamic presenter are all good options for delivery of an awareness program.

## Evaluation of Awareness Programs

All security activity should be measurable. Just like any other budget item in a business, there should a method of calculating the value that was received, as compared to the money spent. Awareness is no different in this regard. Does

the security awareness program have impact? Does it increase awareness of, and compliance with, good security practices? A great security awareness program may not decrease the number of incidents – instead it may actually increase them since the aware employees are more likely to notice and report on attacks they see.

Some criteria to measure the effectiveness of the awareness program include, first of all, attendance and completion of the program, but then perhaps, surveys, observation and the increase in questions asked can help evaluate the impact and relevance of the security awareness program.

## Updating the Risk Register

As items in the risk assessment report are resolved, the risk register also needs to be updated to change the risk status to “complete.” The risk register should always be a ‘living document’ that is always up-to-date and portrays an accurate overview of the risk profile of the organization.

## Monitoring and Reporting on Risk

The fourth step in the risk management process is monitoring. This is where the processes are in place to measure the effectiveness of the controls used to mitigate risk, and the risk and security managers are actively watching for changes in risk levels.

First of all, the measurement of the effectiveness of controls is to evaluate if the controls are:

1. Implemented as designed
2. Operating correctly

3. Achieving the desired result

The review of controls starts with enduring that the controls were implemented as designed. This ensures that the control is correctly installed and configured according to the project plan that implemented the control. If some of the requirements in the design of the control were not met, then this should be highlighted in the report regarding the review of the control.

The second step is to ensure that the control is operating correctly. It could be that the control is not functioning as it should, perhaps due to misconfiguration, lack of training or procedures for administrators, lack of reporting to management, or just a defective control. The effectiveness of many controls erodes over time, and the control may not be working as well as it was when it was first installed. Management should be made aware of trends, deviations, or weaknesses in the control. The results of the monitoring can be fed back to the risk response step to adjust the configuration or operation of the control.

As will be seen in the security control testing chapter of this book, those two steps are often referred to as ‘verification.’ The assessor verifies the installation and operation of the control.

The third step in this process is to ensure that the control is achieving the desired result. The purpose of a control is to mitigate a risk, since the risk is what justifies the control. This relationship is shown in Figure 2-15.


*Figure 2-15. Measuring Control Effectiveness*

This third step is key. Controls may be operating correctly – the lights are on and the machine is working but the review of the control discovers that it is not the 'right' control for the job. This is known as 'validation.' The assessor must carefully examine whether the risk that justified the control is being effectively mitigated by the control.

## Monitoring for Changes in Risk

Some risk changes slowly, other risk can change very rapidly, but risk always changes, which is why risk management is an ongoing, continuous effort. There are both internal and external factors that can change risk and the risk and security managers need to be diligently watching for changes in risk. Internal changes in staff and changes to procedures affect risk calculations, New, inexperienced staff can increase risk of errors and older staff may not be as diligent as they once were. In addition, equipment gets older, controls become less effective and business priorities change. Changes in the business can affect asset valuation or open new attack vectors such as when new functionality is added to applications and users.

External changes in laws (especially privacy laws) and markets (including financial markets) can pose new challenges to the security team. Hackers may develop new tools and quite often will focus their exploits on specific software, hardware or industry sectors. The security manager should review whether the organization is using any of the hardware or software currently being targeted by hackers and ensure patches are up-to-date.

## Reporting

During the monitoring step, regular reports are generated that provide management with updates on risk and the effectiveness of the risk management program. Management is alerted to any areas of non-compliance with policy, procedures, laws, regulations, or good business practices. Reports should also include progress on addressing items in the risk register that has been resolved or added. The risk register provides management with a means of verifying the risk profile of the organization and evaluating the effectiveness of the risk management and security teams. Items listed in the report allow management to take immediate steps to address any unacceptable risk and supports management with the ability to ensure proper governance of the assets and operations of the organization.

## Supply Chain Risk Management

As we reach the end of this review of risk management, there is one specific area of risk that has emerged in the last decade. This is the area of supply chain risk management. Most organisations today rely on a supply chain that is both global and vulnerable to disruption. Whether the supply chain is a cloud service provider, or a

hardware vendor, the supply chain could cripple business operations in the event of a disruption.

This is where the risk practitioner has to especially investigate the reliance the organization has on 3rd party suppliers. In the past, many organisations maintained an inventory of raw materials, however that has changed with the development of just-in-time delivery and more time-sensitive business operations.

A decade ago, very few organisations used the cloud to support their data processing and storage requirements, but now most organisations have a majority of their data both processed and stored off site. In fact, many organisations use software-as-a-service applications extensively throughout the organization, perhaps without the knowledge of the risk and security teams.

As a part of risk analysis, the risk practitioner needs to discover any dependencies the organization has on external parties. Part of this analysis will include the review of whether the supplier is a single point of failure, or whether the relationship with a third party could be exploited by an attacker in a chained exploit.

NIST has issued Special Publication 800-161r1 to specifically address the supply chain risk. The focus of this standard is to highlight the risk of purchasing insecure software or hardware. The insecurity may be the result of poor design, counterfeiting, malicious functionality, and poor development practices. The risk practitioner should be alert to these types of vulnerabilities that could otherwise lead to a security breach. The risk practitioner should ensure that, as much as possible, to ensure that third-party products are designed to be secure and will support quality, resilience, and integrity of processing.

# Summary

This chapter on risk management is one of the most important chapters in the CISSP exam outline. Risk is the central point around which an information security program is built. All of the other chapters will focus on building the controls and protection of assets that risk management has highlighted. The very next chapter, Asset Security, examines the means and approaches used to protect the assets of the organization from the threats and vulnerabilities that were exposed in risk management.

As with any area of knowledge, the first major step is to be familiar with the language and terminology used. Risk management is no different. The chapter covered many terms that the security manager must be familiar with.

The next chapter is about Asset Security. Chapter 2 placed a value on assets and determined the risk to those assets. Chapter 4 will examine the process of identifying and managing all of the assets of the organization – both tangible and intangible assets, so that those assets are protected from compromise and can provide value to the organization.