

# Information Security Basics

By Brad C. Johnson

**Information security programs are built on the building blocks of information security basics. This article will describe these basics and give tangible examples of the types of topics and decisions you must grapple with to build such a program.**

## Abstract

IT information security programs are built on the building blocks of information security basics. The mortar for these blocks are the basic principles of security: *confidentiality, integrity, and availability*. The blocks that form the foundation are a variety of fundamental security topics such as risk assessments, security policies, asset management, physical security, operational management, and incident management to name a few. Understanding the concepts that define the basics of information security is critical to building a robust security program. This article will describe these basics and give tangible examples of the types of topics and decisions you must grapple with to build such a program.

## The basics

Information security means the protection of both information and information systems. We want to protect these things to ensure that access to them is controlled. We want to make sure that only authorized people and processes can access them and only at appropriate times. We want to make sure that the information is only disclosed in ways that we control, that access to it is not disrupted, and that data is only changed – created, modified, or removed – under the conditions we define.

Information, as we all know, is stored in a variety of ways: on paper, in voicemail systems, in people's minds, and on a variety of electronic technologies. Information systems can take the form of a group of people (e.g., the Information Security Group), a collection of policies, or a collection of electronic devices (routers, firewalls, security software). All in all, information security is an expansive topic that affects virtually everyone within an enterprise.

The word *basic* also needs to be put in the appropriate context. Some people assume that it means something trivial or achieved quickly or without a lot of effort. In fact, it is the exact opposite. It is about fundamentals: actions that are rehearsed,

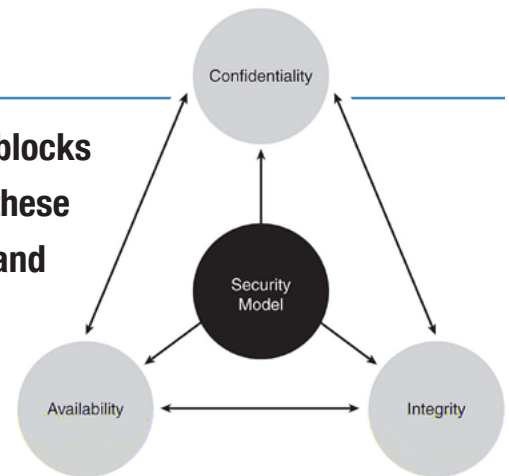


Figure 1 – CIA Triad

acted on, refined, and monitored on a regular basis. In the sport of football, blocking and tackling are considered basic skills that are necessary to succeed at any level. No matter what kinds of offense or defensive schemes are used, they can only be successfully executed with sound blocking and tackling techniques. These techniques are rehearsed continuously throughout the season. These techniques are uniquely coached to fit the special needs of the plays you are trying to run. Information security basics are the same thing. They are practiced continuously.

As we all know, security is not an end-game but an ongoing process: a way of thinking. The more ingrained that security is within the corporate culture, the more likely it is you can succeed at meeting the needs of your business. Security is an iterative process with the goal of continually improving each of your policies, procedures, or controls.

Whether you know it or not, the roots for information security within an IT organization are built on the well-known CIA triad for security policy development.<sup>1</sup> Briefly put, the CIA Triad is a security model built around three critical areas: integrity, confidentiality, and availability. Those concepts are handled within the confines of your hardware, software, and communications information systems. Those information systems and critical areas are therein executed by people, products, and procedures.

Let us take a look at these guiding principles in a little more detail.

## Principles

Trying to figure out how to start building an information security program can be a daunting task. You need someplace

1 Chad Perrin, "What is the CIA Triad?," (*TechRepublic*, August 12, 2008) – <http://www.zdnetasia.com/what-is-the-cia-triad-62044759.htm>.



to start. First, you need to decide what your guiding “lights” will be, and second, you need some type of framework to organize all of the issues you will be addressing. We will take a look at these guiding lights first and then address the framework in the section “Information Security Framework.”

The CIA Triad<sup>2</sup> was developed exactly for the purpose of identifying tenets that will help you in developing information system policies. While each of these words seems common, they have clear and important implications on what you will need to do.

## Confidentiality

Confidentiality means that information is only disclosed to authorized parties. Determining who should have access to data means you have a clear understanding of who people/resources are (authentication), an understanding of what is appropriate for them to have access to (authorization), and that you are tracking what these actions are (auditing). Also remember that we are not just talking about keeping track of electronics on a network. It includes all (human) processes that a business uses in its normal day to day operations.

Confidentiality is the area that is most tightly tied to technologies and product selection. Although you want to have a robust set of written policies that define who is authorized to access what under predefined conditions, the fact is you want mechanisms in place to ensure that those policies are followed. Let us take a look at how improper confidentiality controls can lead to problematic unauthorized access.

### Security example

A company recently deployed a Human Resources (HR) web application. The application has two primary roles: regular employees and (HR) administrators. Not surprisingly, the administrator role had significant privileges that allowed them to manage (create, modify, delete) employee benefits such as vacation and pay scale as well as access to sensitive reports like performance reviews. Unfortunately, due to a sloppy web development practice, the underlying HTML code used to perform actions for either role – employee or administrator – was embedded in the client-side code but only “revealed” if the current user had the correct privileges. For example, if you used your browser to perform a *View Source* function, you could see that pages sent to an employee actually had function calls for the administrator but they were disabled (hidden) since the current user was not logged in as an administrator.

By using a web browser proxy, one could intercept the client-side code before it was passed to the local browser and make those administrative functions visible (enabled) which allowed a regular employee to call administrator-level functions and have access to functions and data not intended for him. In other words, the web application as-

---

## We do not develop information security programs and policies to support themselves; we do it within the context of our business.

---

sumed that only administrators would make administrator-level calls and did not have the appropriate authorization checks on each individual function call. To resolve this problem, the underlying file system structure had to be modified to support the ability for user-level authorization checks to be made for this web application. This example highlights that decisions about confidentiality technologies have to be thought of in many different places to ensure they all support and implement the formal policy.

## Integrity

Integrity means that information cannot be updated (that is, created, modified, or deleted) without authorization. To authorize an update means that you have policies, procedures, and mechanisms in place to ensure that you know who is trying to update something and that it is being done using the approved processes and at the appropriate time.

When you think about the controls you need in place to ensure this level of access control, you can appreciate the depth of what it means to have integrity.

## Availability

Availability means that people or applications have access to information in a timely and reliable way: simply put, it is available when it is needed. In most cases, one needs to identify both a primary and a secondary method for granting access just in case something goes wrong.

When all is said and done, we need to ensure that our information system program is singularly focused on ensuring that we can execute our business and develop strategies that allow that to happen. Making sure a resource is available or can be available is critical to support that business goal.

## Focus on business

The issue we just addressed in “Availability” is potentially the most important principle of them all. We do not develop information security programs and policies to support themselves; we do it within the context of our business. Too many organizations become a slave to technology and develop processes to support the technology which can be at the expense of actual business operations. Here is an example to highlight this.

### Security example

Let us say that we have a mission-critical trading or sales operation that requires 2-factor authentication and that one of the credentials used is supplied by technology that

2 Yusuf Bhaji, “Chapter 1: Overview of Network Security,” *Network World*, July 25, 2008 – <http://www.networkworld.com/subnets/cisco/072508-ch1-net-security-technologies.html>.

runs on the local protected network. If we focus too much on technology we might have a security requirement that states that no trades or sales can be completed without successfully performing this 2-factor authentication. So what happens if that credential technology is somehow not available? Do we stop making trades or sales?

The answer, of course, has to be – no. The better solution is to have a security requirement that stipulates that strong authentication is required and then describe the primary and secondary means by which it should occur. The 2-factor method is the preferred (automatic) method, but in the event of some type of network or service disruption, there is an alternate (manual) method so that business can continue.

Keeping the focus of our information security program on the business will allow us to develop sensible basic policies, procedures, and mechanisms.

### Information security framework

Earlier we said that one needs to define the guiding lights of the information security program and that we also need a

## The ISSA Store Is Open Order Your ISSA Shirt Today

Stand out at your next chapter or regional event by wearing the navy blue polo shirt featuring the embroidered ISSA logo. The stainless steel Thermos makes a statement and is the perfect beverage companion. Each tumbler holds 16 oz. of your favorite beverage.

Our logoed pens with fraud-resistant ink are a popular choice. Paired the fraud-resistant pen and ISSA notepad make for the perfect chapter or industry event door prize/giveaway, thank you gift for speakers, welcome gift for new members, or to express appreciation to volunteers.

To find out more about purchasing these or other ISSA promotional

products, contact Dana Paulino, 1-866-349-5818, U.S. toll-free; 206-388-4584, international; extension. 103.

framework. The ISO 27002 standard is a good model to use for such a framework because it is an enterprise-wide definition of the types of resources and controls that one needs in place to develop an information security program. It encourages a program that integrates business and technology and helps to identify specific tasks to improve security.

In addition, using the ISO 27002 standard as a framework helps to meet the needs or requirements of other compliance initiatives like Sarbanes Oxley, Gramm-Leach-Bliley, and HIPAA. Using this standard as a framework is an excellent way to build your information security program and cover the basics that are essential to your environment.

### ISO 27002

There are 12 major sections of ISO 27002:

- Risk Assessment
- Security Policy
- Information Security Organization
- Asset Management
- Human Resources
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information System Acquisition
- Incident Management
- Business Continuity Management
- Compliance

The ISO 27002 standard is a rename of the ISO 17799: a code of practice for information security.<sup>3</sup> In it, there are about 130 control objectives which can be implemented.

Let us review some of those 12 sections as a way of highlighting some of the important information security areas you need to think about.

### Risk assessment

On the face of it, a topic like risk assessment is worthy of its own article. In fact, there are entire books, courses, and conferences dedicated to risks and risk assessment. Interestingly though, it is somewhat fortuitous that the very first section of the ISO standard is such a lofty topic because it forces you to develop a practical strategy for dealing with complex parts of your information security program. You might think it would be better to start with something easy, but tackling this helps set the stage for other areas. Here is how that happens.

Many people make the mistake of trying to go from scratch to a finished product too quickly. When you are forced to think about risk assessments and the incredible breadth of issues that topic might entail, it is better to not try and solve the whole thing at once.

<sup>3</sup> <http://www.27000.org/iso-27002.htm>.

# Connect Learn Advance



For less than \$10 a month  
become an ISSA Member and  
take your career to the  
next level through:

Local Chapter Meetings

Face-to-Face Networking

The ISSA Journal

ISSA Web Conferences

Trusted Online  
Member Community

Continuing Professional  
Education (CPE) Credits

Certification  
Study Courses

## Join Today!



**Information Systems Security Association**

*The Preeminent Trusted Global Information Security Community*

**[www.ISSA.org](http://www.ISSA.org)**

A good starting point for thinking about risk is to do the obvious: identify a policy that states the kind of events that would trigger a risk assessment, define who would be responsible for it, and define the documentation that would be required to support it. How do you decide what events would be trigger points? I cannot tell you exactly what they would be, but if the COO, or CSO, or any manager sat down and asked themselves “What events would the president, the board of directors, or our customers worry about?” you can easily identify a small set of high-priority events; and just like that, you have the beginnings of a risk assessment policy.

## Security policy

Again, much like risk assessment, the right way to lay the groundwork for this work is to start with first-tier issues and accept that this policy will grow in breadth and depth over time. The key is to start with an information security policy document that has been approved by management and distributed to appropriate staff members. In addition, you need to make it clear that this policy will be reviewed and updated periodically (e.g., annually), and that when material changes to the policy are implemented, they have to be reviewed.

What goes into a security policy? To start with, think about the following. You are trying to give guidance and a sense of priority. If you hired somebody to deal with your security issues, what are the types of things you would verbally describe to him as important parts of his job description? Chances are many of these things are exactly what you would want in your security policy.

## Information security organization

Here we want to make sure we have good organizational clarity for both internal and external groups. For within the organization, the key items to document and get agreement on are:

- Decide who is responsible for what information or information systems (data owners)
- Decide the process that each of these people should use when granting authorization
- Ensure you have confidentiality agreements in place for those who have access to (sensitive) information
- Make contact with local or federal authorities and make sure your processes can provide the data they need in case of some type of breach or emergency
- Have periodic independent reviews of your information security program and policies

For external parties, you want to make sure your security risks are explicitly called out both in how you deal with them and the agreements (legal documents) you have with them.

## Asset management

This is one of those tangible topics that may require a fair amount of time to execute but should not be hard to figure

out. Most companies have a pretty good idea their assets. You need to make sure there is a clear understanding of responsibility for all assets and that there is a system for keeping track of them.

For each asset you need to identify a unique owner and define what the acceptable use characteristics are for it. For all assets, you need to identify the different classes of information that exist (e.g., public, sensitive, secret) and then make sure you have a clear understanding of how each type should be handled. All of these steps are critical in that the assets you are protecting are the intellectual property of your company. Categorizing these assets allows you to ensure that the systems containing the personal and corporate identifying information are properly identified and protected.

Asset management is very much like incident management (to be discussed later) in that it is an important area, a topic that is easy for the entire organization to understand; and yet, despite being very solvable with simple but hard work, it is often an area that languishes. Maybe the following will help motivate you to tackle it sooner and better.

## Security example

One of the problems for any manager in the IT arena, and especially within the area of security, is that there are not a lot of business tools or models to help define good return on investment or life-cycle costs. How much did you “save” by performing an Internet penetration test? Why is it “worth it” to have DNS, email, and file transfer services on separate systems instead of having them all on the same one? Why does the organization have to pay for licensing for virus and malware software when there are public domain programs for free? The life of justifying costs without the availability of good cost tools is a hard but typical one for security professionals. Asset management is one area that allows you to have realistic life-cycle costs because you can uniquely identify all of the resources you have. The more detailed and thorough your asset identification process is, the easier it is to demonstrate that your house is “in order” to other managers and supervisors.

For those in governmental positions, having a tight rein on asset management is essential for identifying short- and long-term costs as these costs are tightly tied to budgets and grants. In addition, identifying these costs is required for full-disclosure to public evaluation forums.

The bottom line is having a good information classification system allows funds to be defended. That is important because protecting sensitive systems and information often requires elaborate policies, procedures, and technology. Having a detailed catalogue of your assets allows you to more easily defend those costs.

## Physical and environmental security

This is another tangible topic that also is not hard to grasp but yet can be time consuming. The good news, however, is that it covers the most obvious resources: physical resources.



There are two basic areas that need to be addressed: secure areas and actual equipment.

For the equipment, there are some standard issues that have to be dealt with. I will put those in the form of questions that would need to be answered.

- How do you protect your equipment to reduce risks from threats and unauthorized access?
- How is your equipment protected from power failures or failures in supporting utilities?
- What are the guidelines for performing maintenance on your equipment?
- How is your equipment protected when it is off-premises?
- How do you securely dispose of or re-use equipment?

Depending on how your company is setup, the issues dealing with secure areas can either be quite straight forward (for example, you rent space from a company that provides physical security within your lease and you outsource your IT infrastructure which is also handled by SLA documents) or worthy of its own serious and extensive analysis, such as you have state-of-the-art redundant and terror-proof controls, buildings, and facilities.

Regardless of where on the spectrum your company lies, you need to outline the controls you have in place for the perimeter and entrance to your physical locations, a statement of how these facilities are secured, a description of how you have protected these places from external and environmental threats, and how you control access to public points and delivery or loading areas.

## Communications and operations management

This topic and the next one (access control) are quite large within the ISO standard (although we are not going to cover access control within this article). There are over 30 control objectives for this one and 25 for access control, accounting for over 40% of the standard.

The reason there are so many is that while all of the ISO topics are important and help to paint a complete picture of your information security program, these areas tend to cover issues that cross important organizational boundaries (with Communications and Operations Management) and identify specific actions for controlling access to information on your network (Access Control).

Here are the main areas that you need to think about:

- Defining and documenting operating procedures: critical topics include segregation of duties and separation of the development, test, and production environments
- Defining and monitoring the delivery of services and information from third parties
- Documenting the terms for system planning, such as capacity management and system acceptance
- Developing a plan for handling malicious and mobile code

---

## All too often, people wait until after they have had an incident to figure out a plan for reacting to one.

---

- Developing a plan for handling removable media, disposal of it, and a back-up strategy
- Designing the controls for network management and the security of the networked services

## Incident management

Oddly enough, this is probably one of the easiest parts of your information security basics toolkit to prepare for and yet the area most organizations are least ready for. All too often, people wait until after they have had an incident to figure out a plan for reacting to one. The normal outcome is that they are woefully unprepared for the first incident, gather the wrong information, do not know who to contact or who is responsible for managing the situation, and taint the evidence because of the lack of well-documented procedures.

In a nutshell, there are only two general areas you have to define: what to report and how to manage the incident. For reporting an incident or weakness, you need to assign responsibilities for accepting and responding to an event and articulate the instructions for what each person should do. The rule of thumb is that there are normally three people involved in an incident – a technical person to do the reconnaissance, the manager of the information or information system affected, and somebody from the legal department for contacting authorities. In most cases, the basic instructions of what each person should do will fit on one page.

For managing the event you need to clearly state the chain of command for making decisions, define a policy for how your organization will respond, learn, and improve your procedures for future incidents, and make sure you have spoken with appropriate authorities to understand what evidence needs to be collected.

Incident management is one of the most important job responsibilities of information departments and often the one most organizations are least prepared to handle. Here is one way you could prepare for such an event.

## Security example

Very similar to a lot of other emergency response teams – such as firefighters, policemen, emergency medical teams, SWAT teams, etc. – one of the best ways to prepare for an event is to simulate it and practice the very steps you would need to perform if the situation were to happen.

The first step is to develop a (small) list of real-case scenarios that you need to be prepared to handle, for example:

- A virus somehow enters the internal network and is infecting systems
- The corporate website has been defaced

## The more ingrained that security is within the corporate culture, the more likely it is you can succeed at meeting the needs of your business.

- An unauthorized mobile device has connected to the corporate internal wireless infrastructure

For each of these events, you would want to document the exact steps that each person involved would perform and identify specific people (and their backups) that would execute the work. After you have defined the default actions, you want to initiate the simulation as if that very event were actually happening and make sure everyone can perform the work and successfully recover from the incident. Our experience has shown that you will find that there are important steps that have not been documented, that not all of the appropriate people have been identified that need to be involved, and that you have invalid assumptions built into your understanding of what it will take to be fully recovered. It normally takes a number of iterations through the process to fine tune the game plan for a quick recovery.

Every time you run through this incident response process, whether in a simulation or for real, you need to also gather the parties after-the-fact and determine what parts of the process need modification to be better prepared in the future.

### Putting it all together

Understanding information security basics is really about knowing what to do to build a good information security program. The ISO 27002 standard provides an excellent framework for methodically thinking about the various basic

areas that you will need to address. In this article I have highlighted some of the key topic areas and a number of specific questions or issues you need to think about, document, and make decisions on. Of all the things I have discussed, remember a few of them in particular.

First, security is an iterative on-going process to continually make things better; it is all about evolution, defense-in-depth, and maturity; it takes time.

Second, *availability*, *confidentiality*, and *integrity* are the key technical pillars for your program.

Third, document the policies, requirements, and responsibilities that people have and you will be on your way to creating a successful information security foundation. A foundation, built on time-tested information security basics.

### References

- Bhaji, Yusuf, July 25, 2008, “Chapter 1: Overview of Network Security,” *Network World* – <http://www.networkworld.com/subnets/cisco/072508-ch1-net-security-technologies.html>.
- International Organization for Standardization, ISO/IEC 27002:2005 – [http://www.iso.org/iso/catalogue\\_detail.htm?csnumber=50297](http://www.iso.org/iso/catalogue_detail.htm?csnumber=50297).
- Perrin, Chad, August 12, 2008, “What is the CIA Triad?” *TechRepublic* – <http://www.zdnetasia.com/what-is-the-cia-triad-62044759.htm>.

### About the Author

*Brad C. Johnson, Vice President, SystemExperts Corporation, is a well-known authority in the field of distributed systems. At SystemExperts he has pioneered innovative methodologies to improve customer's effective security. Brad holds a BA in Computer Science from Rutgers University and a MS in Applied Management from Lesley University. He may be reached at [brad.johnson@systemexperts.com](mailto:brad.johnson@systemexperts.com).*

## ISSA Connect Survey

### Is Cloud Computing secure enough for your critical business application/data?

I have no idea what to do. I need more education, time, and money! (0%)

It is against company policy to go outside my data center walls for any SaaS offerings. (0%)

I will let early adopters go ahead of me and work out all the “kinks” then decide. (25%)

Increasing datacenter costs have forced us to move to the Cloud as quickly as we can. (50%)

Data Security is better with over 50% of breaches occurring from within. I believe the risk is low. (25%)

**Cast Your Vote Today:** <http://connect.issa.org/poll.jspa?poll=1040>.

