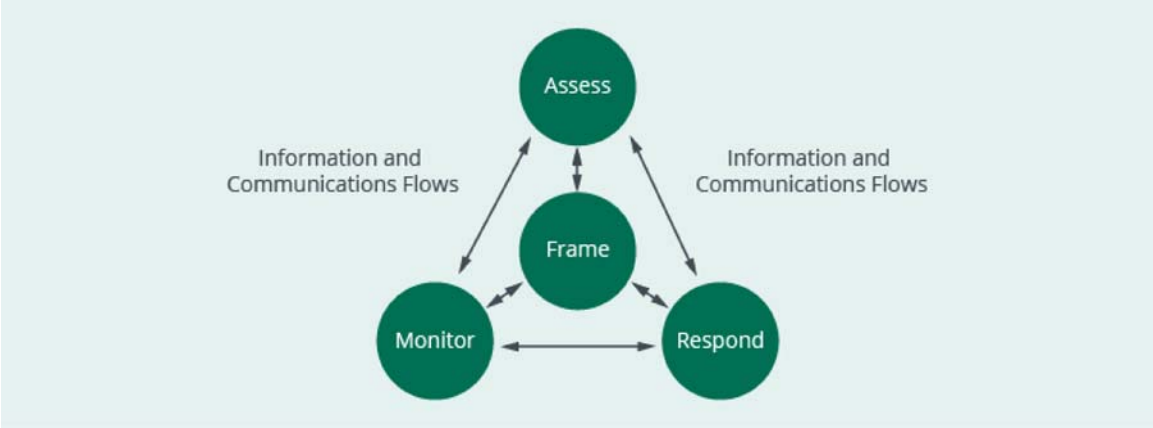
Risk Treatment Overview

We have now completed the first two steps of the Risk Management Framework. We saw this diagram earlier from NIST SP800-39:



The first step was to frame the risk (or as ISO/IEC 27005 calls it to establish the Context) of the risk management effort. This set out the scope and identified internal and external factors that could influence the risk management effort. Then we performed the process of Risk Assessment where we identified and evaluated risk based on threats, vulnerabilities, likelihood, and impact of risk events. The final result of the Assessment step was a Risk Assessment Report (RAR) that was provided to management. The RAR documented the identified risks and also may have included some ideas or recommendations for how management might respond to the risk listed in the report.

Now we come to the Respond step, where management must decide how to respond to risk. Management's response to risk is based on management's attitude toward risk. What is management's risk appetite or tolerance? People have different appetites; some people enjoy spicy foods while others do not. It is the same with risk, some people enjoy the thrill and challenge of taking a larger risk in hope of gaining a larger reward, while others are more cautious and will give up a larger reward in exchange for accepting a lower level of risk and having a more stable operational environment. The challenge for the security practitioner is to gain an understanding of

management's appetite for risk and set out a risk response strategy aligned with that appetite.

There are four usual responses to risk:

- Avoid risk: cease the risk-laden activity
- Accept risk: take no action to reduce risk and instead accept the consequences of a risk event
- Mitigate (reduce) risk: implement or enhance controls
- Share/Transfer risk: pass some of the risk to another party, such as purchasing insurance

Note: ISO/IEC27005 refers to the four risk response (treatment) options as: Risk Reduction, Risk Retention, Risk Avoidance, and Risk Transfer.

The decision of the 'best' risk response option can be difficult since there may be many possible alternate solutions and each alternative may have advantages over the other solutions in one way or another.

Discussion: Risk Factors

What are some of the factors that need to be considered when deciding on the best way to respond to risk?

Cost-Benefit Analysis

One of the harsh realities faced by information security teams is that there will never be enough time or money to do everything that needs to be done. This creates conflict related to priorities and tasks to find the correct balance between what has to be done, what to spend money and time on, and whether the resources are available to do everything to the best possible standards.

The justification for many projects is return on investment, what will be the return or benefit from an investment in a new technology or a modification to a business process. Calculating return on investment for investment in security can be a challenge because if the investment is successful then ideally nothing will happen! This is the same with risk management—how can we justify the cost of a control? We try to use cost-benefit analysis where we compare the cost of the control with the benefit obtained through the control. In some physical cases this can be easy.

For example, a company installs a new fire detection and suppression system that will reduce their insurance premiums, reduce the damage caused by a fire, and allow for faster resumption of operations following a fire. The benefits can be fairly easy to quantify and then they can be compared with the cost of the new system. If the benefits outweigh the cost of the system, it is probably a good investment. (But again, this does not factor in the problem of likelihood. One organization can spend a lot of money on fire suppression and never have a fire—never need the system—while their neighboring company spends nothing on fire suppression and also does not have a fire. One company spent money on a system they did not use and the other saved the money and made additional profit from saving the money.) Who said risk management was easy?

One of the key requirements for a security program today is the need to make security accountable for its budget. Management may see security as a "black hole" where money sinks into darkness from which nothing ever seems to emerge. Instead management needs to see the benefit of a security program—how security is utilizing its resources and supporting and benefiting the business.

If a risk assessment report indicates that the organization should invest in new equipment, for example, a new firewall, then management wants to see the cost/benefit analysis of this recommendation: the cost of the firewall compared to the way the firewall will benefit the organization. This is one reason why a quantitative risk assessment (where the risk was measured in monetary values) was so important. Management will rarely be convinced to spend money because a qualitative risk assessment categorized a risk as a "Level 5 Risk". You want to spend money on a firewall—show the monetary benefits from that firewall.

Calculation of Cost

There is an old story of a man walking into a car dealership and asking what the fuel efficiency was on a high-end car, to which the salesman replied, "If you have to ask that, then this is not the car for you." This is recognition of the complexity of calculation of cost. The calculation of the cost of a control, such as a firewall, is based on much more than just the initial price of acquisition. In some cases, a vendor may even give the initial product away for free, such as a printer, because they know that their real profit will come from the ongoing support for the product (toner cartridges, licensing, maintenance agreements, etc.).

The security practitioner should include these ongoing costs in the cost-benefit analysis. After all, no one wants to be given money to purchase a firewall only to find there is no budget for training, support, licensing, or repair.

Discussion: Benefits of Security Investment

How can we calculate benefits—what are some of the ways to convince management of the benefits of investment in security?

Review: Benefits of Security Investment

Risk Acceptance Levels

The goal of risk management is to ensure that all risk is within the risk acceptance levels set by management. We have already discussed how management may determine what is an acceptable level of risk and, in the end, only management can accept risk on behalf of the organization.

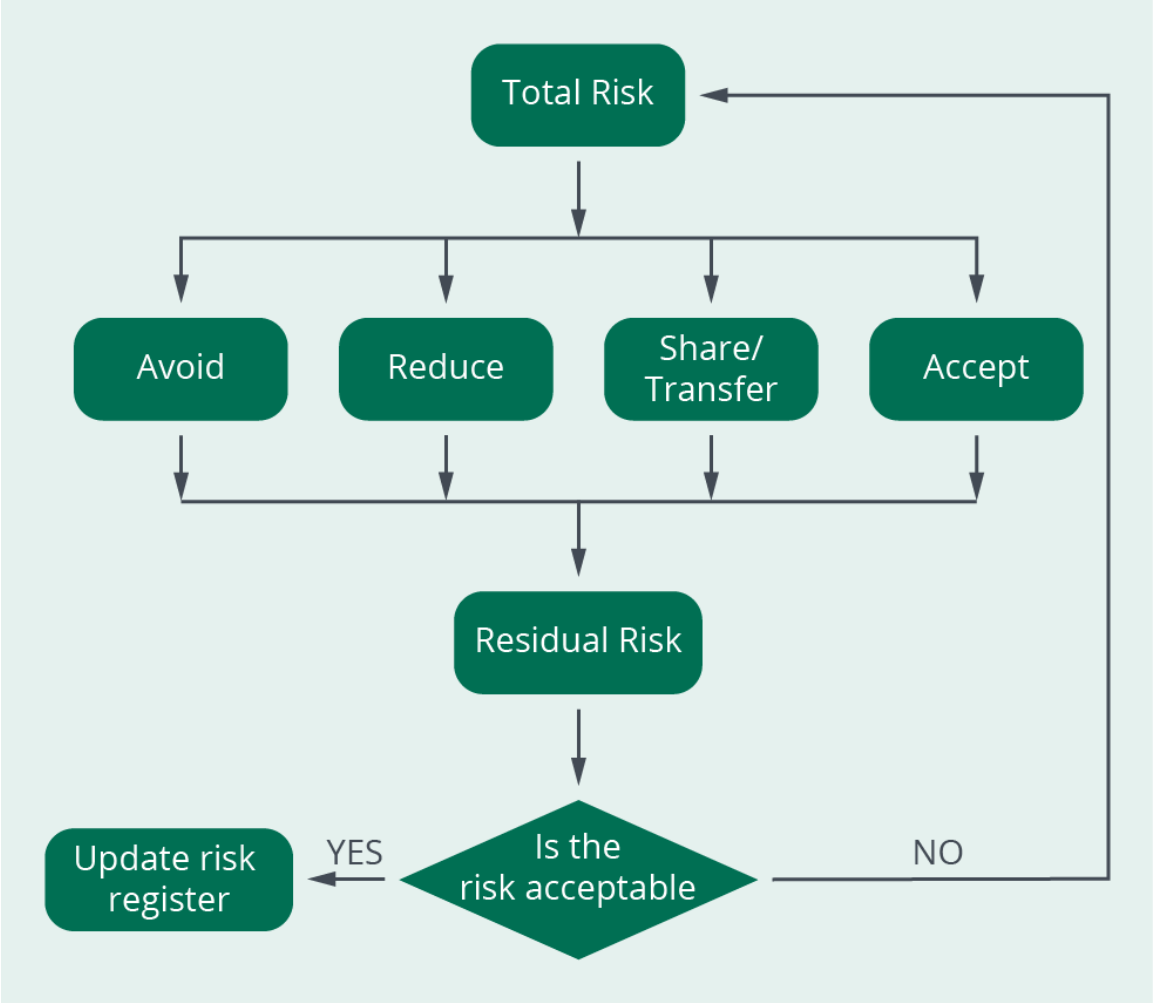
As per the risk assessment report, some identified risk may already be acceptable, but other risk may still remain that requires some form of risk response.

This is where the decisions have to be made of what is the best response to the identified risk. Each of the risk response options is examined in more detail next.

Risk Response

Risk may be shared, avoided, reduced, or accepted; which is the best solution? In some cases, more than one risk response may be required: to implement technology and, in addition, to purchase insurance. In the end, the implementation of controls will determine residual risk, the level of risk that remains after a control is implemented.

For example, a person purchases car insurance. This response shares or transfers (most of) the risk to the insurance company in exchange for an annual insurance premium that must be paid by the owner of the car. The insurance company ensures that they charge each insured person a premium for the insurance that would be enough to pay for any claims made against the insurance company, but even the insurance company shares the risk. They often purchase re-insurance so that if there are excessive claims, their re-insurance will pay for the amount of the claims above a certain limit.



For the owner of the car, they are not protected from total loss of the asset—the car. However, the owner of the car is still liable for the first part of a claim, often called the deductible, or excess. If the owner makes a claim, they know they have to pay for the first $500 of the claim, and the insurance only covers the amount in excess of $500. This deductible is the residual risk—it is the amount of risk the owner of the car still faces even after the implementation of the control (insurance).

Risk Avoidance

Risk avoidance is to cease the risk-laden activity. For example, an organization may close a branch office in a region that it considers unsafe. The choice to avoid risk protects the assets of the organization from a level of risk that cannot be effectively mitigated (based on cost or available solutions). This also means that the organization would also lose any potential benefit from continuing that business operation.

Risk Acceptance

Risk acceptance is the decision by management to take no (further) action in regards to an identified risk. This decision may be based on cost—the cost of

further controls would outweigh the benefits of the controls—or on the calculation that the level of risk is within acceptable limits, and management is willing to accept the cost of the event should it occur.

The challenge with risk acceptance is whether the calculations of cost are accurate. It could be that management has accepted a risk of a certain declared value, but if that event ever happened, it is discovered that the real cost is far in excess of the original expectation.

The end goal of risk management is to reach the point where all risk to the organization is at a level that is communicated and accepted by management.

Share/Transfer Risk

If the level of risk to the organization exceeds an acceptable level, management may decide to transfer the risk to another organization, for example, through the purchase of insurance. The other situation is where an organization is working on a large project that may exceed the capabilities of the organization. In that case, the organization may partner with other organizations that can provide the necessary skills or support to meet the project requirements. This means that both the risk and the profit are shared by the partnering organizations.

Reduce or Mitigate Risk

The fourth option to consider in responding to risk is to reduce the risk through the use of new or enhanced controls. The controls should reduce the risk to an acceptable level. In the next chapter, we will examine this process in more detail.

Remediation Overview

The goal of risk management is to manage risk by ensuring that the risk facing the organization is within acceptable limits. This often requires the use of controls to mitigate or reduce risk. The purpose of a control usually is to address a vulnerability in a system or process. It is rare that an organization can address the threat itself—for every thief that is caught, another will still rise up to take his place. There will always be threat agents determined to take advantage of the assets of someone else. So instead of focusing on the threats, we remediate attacks by working on the areas that we can control—weaknesses, gaps, or vulnerabilities that could be exploited by an attacker. Remediation of vulnerabilities will often provide the greatest benefit through reducing the likelihood or impact of a breach. Remediation will frequently improve the ability of the organization to prevent an attack, detect an attack sooner, and respond more effectively to the attack.

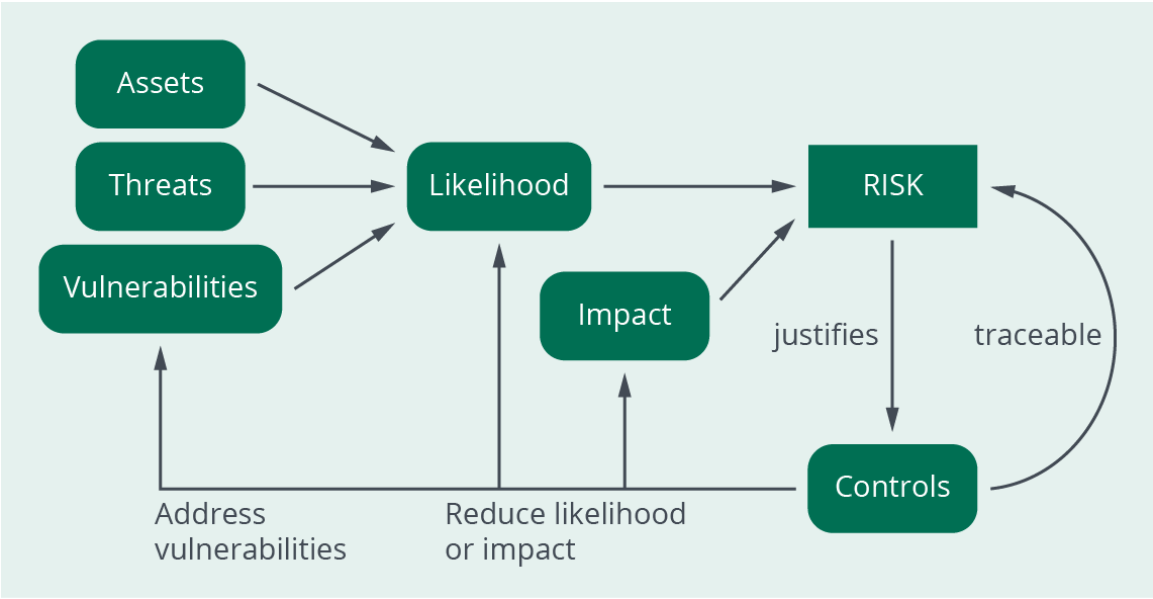
We can see in the Risk Response diagram the objective of the risk response effort. Based on the identified risk, we need to implement an appropriate response until the residual risk has been reduced to an acceptable level. The risk register is updated to document the changed status of the risk.

The implementation of a control addresses a vulnerability. Usually a control will reduce either the likelihood of a successful attack or the impact of an attack. A firewall may reduce the likelihood of an attack by blocking the threat agent and closing any vulnerable points of entry into the network. This does not mean the attacker does not continue to try, but the firewall has made the likelihood of the attacker successfully getting into the network less likely.

On the other hand, a control may address the impact of an attack. A fire extinguisher, for example, does not prevent fires (reduce the likelihood), but it is very effective at putting the fire out before it spreads to other areas and does more serious damage.

A control that is proactive and tries to stop something before it happens is often call a safeguard.

A control that is reactive and attempts to limit the effect of an attack (fire extinguisher) is called a countermeasure.



Remediation of risk is done through the implementation of controls. Risk justifies the need for controls, and each control should be traceable back to the exact purpose (the risk mitigation) that that control was put in place to address. It would be a waste of resources and an unnecessary burden on the organization to have controls that are not needed and cannot be justified, and it would be a false sense of security to have a control that is not effective to mitigate the risk.

When assessing a control, therefore, the effectiveness of the control should always be measured in relation to the risk that justified that control.

Whenever there is a risk that exceeds the acceptable level of risk set by management, the risk practitioner should seek out a reasonable or appropriate way to mitigate that risk.

The challenge is find a control that is cost-effective to purchase, implement, and maintain.

A control is a limitation, a restriction, a chokepoint that affects business operations. A control can affect network speeds, system performance, and response times; therefore, the control must be justifiable in the eyes of the business. If the users believe that a control is unreasonable or unnecessary, then it can be amazing to see how inventive the users are in finding ways to bypass the control. The result of this is that the organization may find that by implementing an unreasonable control, the overall level of risk actually increased instead of decreased. And, in addition, the attitude soon spreads that security is irrelevant and controls are optional instead of mandatory.

What are Controls

We will look at this in more depth in the next module but for now let's look at the primary types of controls:

- Managerial (sometimes called administrative)
- Technical (also known as logical)
- Physical (formerly called operational)

Controls do not work in isolation, instead they work together. For example, a network firewall is an example of a technical control. It provides excellent risk management by controlling network traffic. However, what good is a firewall if it not configured correctly or maintained by skilled staff? How effective would the firewall be if someone could unplug it (physical security)? Controls need to be implemented and maintained using a combination of all three types of controls. In fact, it could be said that an effective security program is where, "the right people are using the right tools in the right way." The "right people" requires managerial controls such as training and oversight. The "right tools" is critical since a person cannot be expected to do a good job with poor quality tools. The "right way" can refer to operational controls and ensuring the physical infrastructure is in place to support the reliable operation of the controls.

Controls may also be a single point of failure or compromise. Putting in place a control may open a new attack surface for the attacker. The firewall may be a target that could cause a network outage if the attacker can compromise the firewall. This is where controls must be maintained and operated according to best practice. This often requires patching the control, hardening the control (disabling all unneeded ports, functions, services or other possible points of attack), monitoring the control, and having an incident response plan in case the control is damaged or disabled.

This is why many organizations deploy a "defense in depth" approach to security. Instead of relying on one device to protect the organization (i.e., a firewall), the security practitioner also implements an Intrusion Prevention System (IPS), network segmentation, and anti-spam tools to ensure that even

if one device fails or is not effective to mitigate a specific risk, other controls in behind the initial control can step in to contain the attack.

Risk Reduction/Mitigation Process

When management has been provided with the Risk Assessment Report, then they need to initiate the process to respond to the identified risks in the manner they feel is appropriate, depending on their tolerance for risk.

The first step in risk response is to determine the owner of the risk. Is this a risk in a business process? A risk in IT operations? The owner of the risk will be responsible to ensure that the appropriate risk response decision is made and, if necessary, oversee the deployment of the risk mitigation activities.

The risks in the Risk Assessment Report should be prioritized according to their severity. Some risks may need immediate attention while others may be able to wait to be addressed in the future. Management may wish to review the justification for the recommendations made in the Risk Assessment Report. Management may also want to confirm the effectiveness of the existing controls and review ongoing projects or major changes that may be pending in business operations. It may be that existing controls may be adequate or there are compensating controls in place that would effectively stop an attack. A major change in business practices or the pending deployment of a new business process or technology may make it infeasible to address a risk to a process that is about to be replaced anyway. In this case, management will usually accept the risk and increase the monitoring of the risk, pending the rollout of the new business process.

Cost-Benefit Analysis

The general rule is not to pay more to protect an asset than the asset is worth. Spending $10,000 on a $5,000 problem is probably not wise.

Therefore, the risk analyst and security practitioner have to investigate which risk treatment options are available and then perform a cost-benefit analysis on the various available solutions. Is it better to drive an expensive car or a cheaper one? Does quality save money in the end? These are hard questions that plague the risk analyst who has to determine whether to recommend a more expensive control that may have additional features over a cheaper option that may meet basic requirements.

Sometimes budget constraints may force the selection of a cheaper option—even though everyone knows that the more expensive option would be better. If you have a limited budget, then you have to work effectively with what you have.

In some cases, new legal requirements may force an organization to implement certain controls. Such requirements often require monitoring and regular reporting on the status of the controls.

Action Plan

The selection or choice of the risk response strategy drives the development of an action plan to roll out the chosen controls and enhancements. In many cases, a risk may be addressed through the enhancement of existing controls. It is often the case that an organization already has everything it needs to improve its security; it is just that many of the controls are not configured correctly or properly managed. The owner of the risk is also responsible to ensure that the controls implemented to mitigate the risk are also working correctly.

An action plan is important with allocated resources, delivery dates, milestones, and reporting requirements. Without such details, it is questionable whether the project will ever reach completion.

A single control may not be adequate to mitigate risk. In this case, more than one control may be required. If there are no cost-effective controls available to reduce the risk to an acceptable level, the organization may choose to purchase insurance to cover the remaining risk.

In the next phase of the risk management framework, the security practitioner may be required to support the monitoring of, and reporting on, risk. This may require that a control is configured to support the gathering of audit data and create suitable logs.

Residual Risk

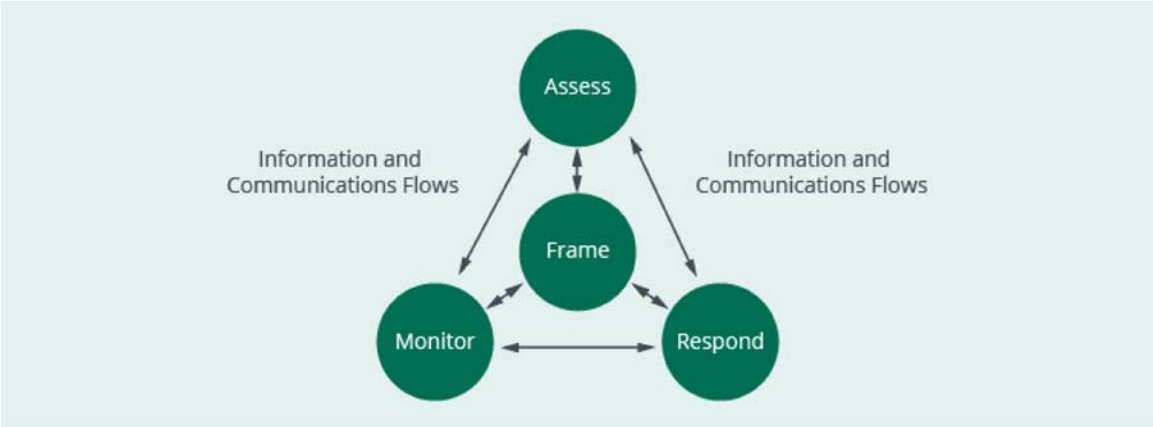
Total Risk – Control Effectiveness = Residual Risk

The challenge with calculating residual risk is the challenge of determining how effective a control will be. Some controls are 100% effective, such as applying a patch to a vulnerability. If the patch works, it will stop an exploit of that vulnerability (but of course we all know that some patches don't work). Other controls, such as a firewall are partially effective. They will block some attacks but may miss others. A fire extinguisher is also partially effective in that it puts the fire out, but undoubtedly there is still some damage from both the fire and the residual from the extinguisher.

As we saw before, a control will usually reduce either the likelihood of an adverse incident or the impact of the incident. This leaves us with a level of residual risk. Our objective is to ensure that all organizational IT-related risk is within the limits accepted by management, therefore, our risk remediation objective is to reduce risk that is unacceptably high to a level that is equal to, or less than, the level of acceptable risk.

Residual risk is the measure of the level of risk that remains after the implementation of the controls (the risk response). Residual risk may not be exactly the same as acceptable risk since residual is the level of risk that does remain and acceptable is the theoretical level that would be accepted by management.

Monitoring



Let's go back to the diagram we reviewed earlier that described the risk management framework. As we can see, everything is centered on the core step of framing the risk. During that phase, we determined the scope of the risk management effort, the internal (cultural) and external factors (laws) that affected risk, and management's attitude toward risk acceptance. This drove the actions taken during the risk assessment and risk response phases. The risk response was based on management's direction and acceptance of risk. As a result, we now should see that the level of risk has been reduced to an acceptable level, and any other areas that still need mitigation are listed in the risk register with an action plan to address those areas according to the agreed-upon schedule.

The reality is that risk management is a cycle—a never-ending effort—and even though the best steps have been taken to respond to risk, there are many risk factors that change. This means that we need the next step in the framework, monitoring.

In the monitoring phase, we will:

- Evaluate the effectiveness of the controls
- Watch for changes in risk
    - Asset value
    - New threats
    - New vulnerabilities
    - New legislation

- Report (Communicate) risk levels to management
    - Comply with legal reporting requirements
- Support audit
- Trigger a new risk assessment when necessary

Evaluate the Effectiveness of Controls

Many controls will lose effectiveness over time. Perhaps the control was effective to mitigate risk when it was first installed; however, over time, the control becomes less effective as users respond automatically to warnings without thinking or find ways to bypass the control altogether.

The security practitioner is interested in providing effective protection from risk, not just creating an illusion of security. This requires the careful examination of risk and controls to ensure that the controls are working correctly. For example, an organization may have a policy that requires users to lock their screens when they are not at their workstations. Just having the control (the policy is a managerial control) is not enough to protect the systems from unauthorized access. Instead the security professional has to evaluate whether the control is actually effective to mitigate the risk. This means that the security practitioner will review for compliance with the policy.

When monitoring for the effectiveness of a control, there are three questions that should be answered:

1. Is the control present (in the above example, is there a policy in place)?
2. Is the control operating correctly (if a user locks their screen does it prohibit access)?
3. Is the control accomplishing the desired result (reducing the risk)?

Having a policy does no good if no one complies with the policy, and the security practitioner should not be content with finding that there is a good policy in place if it is not followed. We want effective risk management, not just an illusion.

Watch for Changes in Risk

Asset Value

Risk assessment was influenced by impact, and impact is based on the value of the asset affected by the risk event. As asset values change, so also does the level of impact change. A system that may have been critically important a few years ago may now be at end of life, while a new system has increased in value to the organization. Remember that we are basing the level of impact by the impact of an IT outage on the business as a whole not just on the impact to the IT department. This means that controls that were not justifiable when the system was just a minor system a few years ago are now essential and should be implemented as soon as possible.

New Threats

As security practitioners continue to win the battle against hackers, the hackers must continuously develop new methods of attack. You can imagine how frustrating this must be to some hackers who spend months discovering a new attack only to have it shut down a few days after it is released. But hackers will never quit because for many of them, this is the way they are feeding their families, or they are being paid to compromise systems. This means we have to be just as motivated, and attentive, to keep them out as they are desperate to get in. Risk management requires constant vigilance to be aware of new threats that could affect us.

Discussion: Monitoring Information

What are some sources of information about new threats that the security practitioner should monitor?

New Vulnerabilities

It is strange to say “new vulnerabilities” since most vulnerabilities are not new, just newly discovered. We know that many of our systems and applications may contain vulnerabilities that will be found and publicized. Vendors are usually quick to create a patch for a serious vulnerability, but there are always the questions of:

- Will the patch work?
- Will the patch affect other functionality?
- How quickly can we test and rollout the patch?

We will examine the important process of change control and patch management later in the course, but obviously we need to integrate patch management into our risk management process.

When we implement new technologies, we may also introduce new vulnerabilities. A new technology may introduce a new attack surface and angle of attack we did not have before. An example of this could be a new firewall that we implemented to protect our network communications that could give an attacker a new way to disable our communications by attacking the firewall itself.

New Legislation

New laws and regulations may also affect risk. This is especially difficult for an organization that operates in multiple jurisdictions. It may be nearly impossible for an organization to keep up and comply with different and conflicting laws. Laws also tend to be subject to interpretation, and there is no clear set of rules the organization can use to ensure compliance.

Report (Communicate) Risk Levels to Management

Perhaps one of the most important parts of the risk monitoring phase is to report on the status of risk to management. Management needs to be aware

of the level of risk facing the organization and be alerted to changes in risk as they happen. This is necessary in some cases where the organization is required to report to government agencies regarding compliance with laws or regulations.

Management may also communicate back to the security practitioner to increase the frequency or level of detail of monitoring.

Management reports should be consistent and follow the same format to allow management to detect trends or patterns in risk levels.

The risk register should always be kept up to date with the status of risk, and as risk mitigation efforts are completed, the risk should be shown as resolved.

Support Audit

Both internal and external auditors may want to evaluate the effectiveness of the risk management program. The security practitioner may be required to provide access to data used in the risk assessment, the justification used in risk response, and the logs or reports generated in risk monitoring.

Trigger a New Risk Assessment

Risk monitoring is an ongoing process; however, there will come a time when it is advisable to initiate a new risk assessment. This may be a scheduled effort (must be done every three years, for example), or it may be driven by a substantial change in the organization. Examples of events that could trigger a new assessment when necessary are:

- Merger
- Re-engineering
- New business process
- New laws
- Time
- New threats

Summary

Risk management is an important part of security management, and it is important that the security practitioner is familiar with the components of risk management.

Document and Operate Security Controls Overview

In this module, we are going to start looking at the pieces that make up a security program. Now that we have examined the process of risk management, we have the information needed to justify the controls and other actions taken to secure and protect the assets of the organization.

The core principle of information security must be remembered – that is that security exists solely for the purpose of supporting and enabling business mission. Our goal as security practitioners is not just to be secure but rather it is to secure the business. Our organizations do not hire us because they are really interested in security – they hire us because management realizes that security is necessary in order for the business to survive. But when the security practitioner forgets this principle then the business quickly begins to isolate and cut back on the security budget and the influence of the security team.

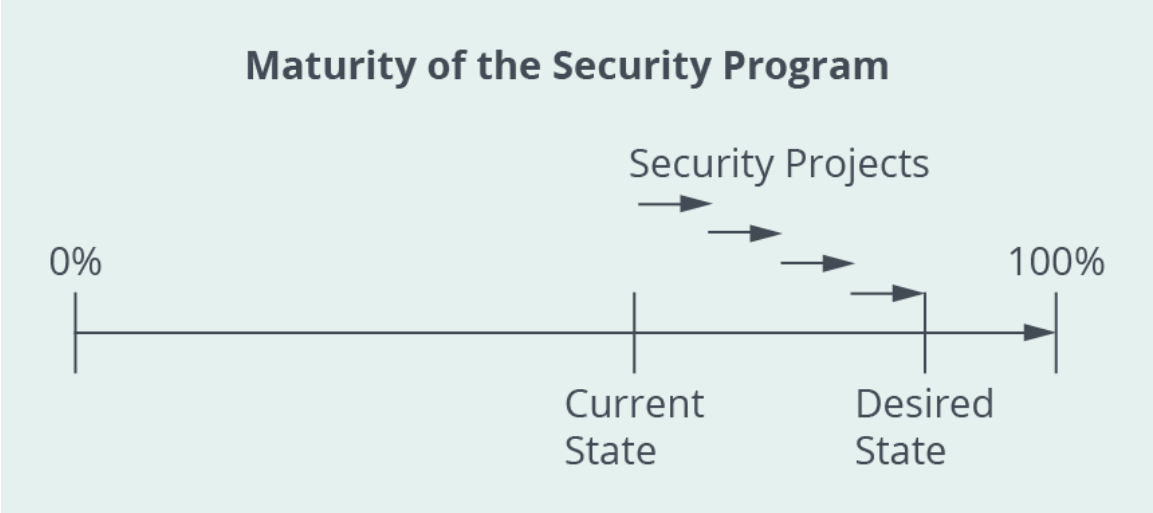
Security by its very nature has often been reactive – following along weeks or months later to try to secure technologies or business processes that have already been implemented. Security is often late to respond to emerging threats and new technology, and is speechless when asked by management for an opinion on how to secure a new business process or technology.

Strategy

We need security strategy not just security operations. We need a plan that has a vision for the future and has an eye on how to protect the world as it will be in a few years – not just to react to what is happening now, or has already happened. But that strategy must be aligned with the strategy of the business. Security must not be aiming in one direction while the business is headed along a different road. Then we will witness that security becomes more and more distant from the business and will be seen as irrelevant by management. Instead our goal to is understand the business, listen to management, watch for changes in business and technology and demonstrate to management the value we bring. Then we may 'have a seat at the table' and will be much more effective and working with management to integrate and weave security into business processes.

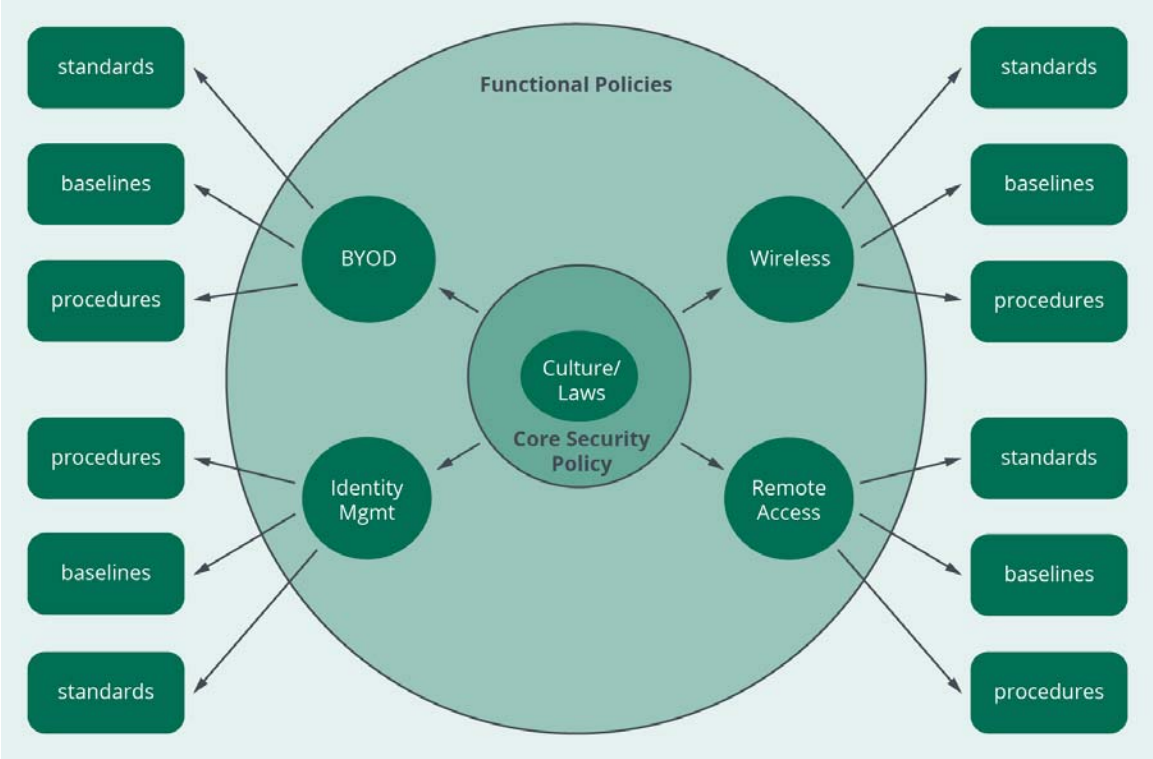
So, the first step in security is to have a strategy – a plan for the future. But a strategy is only words and must lead to actions – a strategy should result in a security plan – the roadmap to implement the goals of the strategy. For most organizations, there is a large gap between their current security state and where they want/need to be (the desired state), this will mean that the security plan is comprised of several projects that work together to reach the desired state.

> State is defined as the condition an entity is in at a point in time. Therefore desired state is the desired condition – and state changes as the organization moves from one state to another as it progresses towards the desired state



As can be seen in this diagram, the security program matures as various security projects move the organization from its current security state to its desired state. We see that the programs often work together and integrate the pieces of the security program into an enterprise security solution. We can also see that the desired state of security is not usually going to be 100% security – depending on management, there may be a determination of what is an adequate level of security for this organization.

Policies



This diagram shows the relationship between many parts of an information security program. At the core of any security program are the laws and regulations that direct the behavior of the organization. The next factor in the development of policy is the culture of the organization – the ethics; the attitude of management toward employees, customers, regulations, suppliers and risk. This culture should be reflected and supported through the policies that the organization adopts.

Policies are what are called ‘directive’ controls. They ‘direct’ or mandate the behavior of the employees of the organization. Policies are signed by management and are the statement of what management intends and proclaims as the core principles of the organization.

Policy is the heart of an information security program. Policy itself is defined as the 'Aggregate of directives, regulations, and rules that prescribe how an organization manages, protects, and distributes information.'

As seen in the diagram, policies are often a collection of documents. At the core, should be a high-level policy that sets out the primary direction for the security strategy. This document should reflect management's attitude towards security and demonstrate the commitment of management to sound security practices.

Discussion: Characteristics of Policies

What are the characteristics of “good” policies?

Review: Characteristics of Policies

Creation and approval for a high-level information security policy may take a period of months. Therefore, you do not want this policy to have to change often. It should be short and visionary, but not technical since technology changes and you do not want to have to update the policy every time technology changes.

Functional Policies

Functional policies are the technical side of the policy framework. Since the high-level policy is not technical, an organization needs policies to address specific areas of technology or specific business processes. Functional policies are targeted and specific, and easier to change or replace than a high level, general policy.

Examples of functional policies would be policies regarding remote access, acceptable use of the Internet, Bring Your Own Device (BYOD), Portable media and incident handling policies.

Policies are words – but words should be followed up with action. Policy should direct actions and those actions will be written in procedures, standards and baselines.

Procedures

Procedures are the step-by-step actions taken to accomplish a defined task. For example, every organization should have a change control procedure to oversee the implementation of changes to systems, projects and networks. The advantage of having a defined procedure is that it ensures that a task is consistently completed in the same manner. Any deviation from the procedure could be noticed and lead to an investigation. If a procedure is documented, then it allows other personnel to fill in for an ill co-worker.

Standards

There are two different ways to look at standards:

- International Standards such as ISO/IEC 27001
- Standards related to software or hardware implementation

ISO/IEC 27001 is entitled **Information technology — Security techniques — Information security management systems — Requirements.** This is an excellent standard that can be used by an organization to help them establish a credible information security program. Many organizations

struggle with the challenge of how to build a good security program. Using the ISO27001 as a standard or framework for their security program can ensure that the organization bases their program on globally recognized best practices. It also ensures that all the main areas of information security are addressed and that nothing was missed. Another advantage of using the ISO27001 is that the organization can now be certified by a third party as compliant with the standard – thereby providing assurance to their clients, shareholders and vendors that they are meeting internationally recognized industry best practices in information security.

ISO27001 mandates the practices that an organization must do to be compliant with its requirements. Therefore, it uses language like "shall" when it describes what an organization must do. However, most standards are not prescriptive enough – they tell what must be done, but not how to do it. The requirements can often be interpreted in different ways – which means that there is an element of subjectivity in how the standards are applied.

To help an organization to set up a strong security program that would be in compliance with ISO27001, a separate, supporting document was created named ISO/IEC 27002. This document helps an organization to build the security framework mandated in ISO27001. This can be seen through the naming of ISO27002 as: **Information technology — Security techniques — Code of practice for information security controls.** We can see that this is only a guideline – a code of practice rather than a requirement (as seen in the naming of ISO27001). The language used in the ISO27002 standard also differs in that it uses the term 'should' instead of the more proscriptive 'shall'. ISO27002 lists the controls that an organization should consider in building, implementing and improving their information security program.

There are many other standards available as well that an organization could use as the standard for their security program. These may be national standards (such as NIST or BSI standards), or industry standards (such as the Payment Card Industry – Data Security Standard (PCI-DSS)).

The other use of the term standards can refer to the adoption of hardware or software standards that an organization selects. The adoption, for example, of a standard operating system or the choice to purchase equipment from one vendor (e.g., Dell) can provide significant advantages to the organization. If an organization only has to support one product, that can ensure greater consistency in the configuration and security of the organization's systems, and can reduce the cost of training and support. Standards also can result in better cost control through bulk purchasing and licensing. On the other hand, standards can pose a risk to the organization

through ‘having all your eggs in one basket’ where a flaw in the product would now affect the entire organization. Other risks with enforcing a standard is the problem of a lack of flexibility – the standard product may not be the best for all departments, and the vendor may increase prices and maintenance costs that are difficult to avoid without a complete change of standard.

Baselines

It is common to see situations where an organization has purchased an excellent product (device) that can provide a wide range of services (benefits), however, the product is not configured correctly and is only providing minimal benefit. This can be a result of a lack of a defined baseline configuration for the device. A sound security practice is to define a minimal security baseline (configuration) for a product so that when the product is deployed in multiple locations it will be properly configured and secured. This baseline may include the hardening of the device (turning off services and functionality that are not required), setting of security controls, enabling security functions, or other configurable items that would ensure the device is adequately protected.

By setting a security baseline the organization can conduct security compliance scans to ensure that all devices on the network, for example, are configured correctly in accordance with the baseline. A baseline often represents the minimum acceptable configuration, in other words, no device may be connected that does not meet this minimum standard at the very least. However, it does not restrict a department from implementing an even more secure configuration where needed. In other words, everything on the network is secure to at least a minimum acceptable level – but some devices may be even more secure.

Important tips from this section:

So as can be seen, the foundation for a security strategy is the development of, and approval of, policy. Policy is that high-level document that states management’s commitment to the information security program and mandates the behavior of the employees. The high level policy is often supported through functional policies that address individual areas of technology. All policies are supported through standards, procedures and baseline to ensure that the intent of the policies is carried out in action.

Controls

Earlier in this course we examined the development, implementation and maintenance of controls. Controls are used to place a limitation on risk and restrict the ability of a threat to exploit a vulnerability. But the selection of controls must be done with prudence and awareness of the impact of the control. A control may impact performance or productivity, it may be expensive to maintain, and it may introduce new vulnerabilities if the control itself can be attacked.

We know that there are usually three types of controls:

- Managerial controls (sometimes called administrative),
- Technical controls (sometimes called logical),
- Physical (environmental) controls (sometimes called operational)

Each type of control is important in that a technical control requires the physical infrastructure and physical security in order to operate, and the support of managerial controls to manage and monitor the effectiveness of the technical control.

We can further subdivide all three of these types of controls in sub-categories. Each sub-category provides a specific benefit.

Directive Controls:

> Controls that direct or mandate operational procedures or behavior.

Examples of directive controls include:

- Managerial – policy
- Technical – warning window about a potentially dangerous website
- Physical – “Do Not Enter” sign

Deterrent Controls:

> Controls that discourage a person from committing an improper act.

Examples of deterrent controls include:

- Managerial – disciplinary policy
- Technical – Warning banner regarding prosecution for entering prohibited systems
- Physical – "Beware of Dog" sign

Preventive Controls:

> Controls that try to stop improper behavior.

Examples of preventive controls include:

- Managerial – separation of duties
- Technical – password
- Physical – fence

All of the above controls are precautionary controls that proactively try to stop bad events from happening, therefore we often hear proactive controls referred to as safeguards in that they attempt to safeguard an asset from attack. However, we need to move on to reactive controls – controls that come into effect once an undesirable event has taken place. These controls are often called countermeasures since they 'counter' or respond directly to an attack.

Reactive Controls

Examples of reactive controls include:

Detective Controls:

> A detective control is one that would identify an attack and alert administrators. The problem in many cases today is that organizations have been attacked and compromised, but they are not even aware of the attack. This leads to a failure to respond to, contain, and eradicate the attack.

Examples of detective controls include:

- Managerial – balancing reports
- Technical – Intrusion Detection System
- Physical – motion sensor

Corrective Controls:

> Corrective controls attempt to regain control over the incident. In many cases this does not resolve the incident but rather it contains and identifies the nature and scope of the incident.

Examples of corrective controls include:

- Managerial – removal of a suspect from the area
- Technical – isolate a system
- Physical – fire suppression system

Recovery Controls:

> Recovery controls restore the affected area to normal, whatever 'normal' is. In some cases, normal may be a new building in case of fire or replacement of a system. For example, an organization attempts to protect its building and equipment through a managerial directive control that prohibits smoking near an area where explosive materials are stored. It enforces that policy through a managerial deterrent that states that a violation of the policy could lead to a fine or disciplinary action. It attempts to prevent fire through the managerial preventive control of monitoring and physical preventive control of removal of fire-causing materials. However, since a fire could still start, the organization installs physical detective controls such as smoke detectors to detect a fire. The organization then has the physical corrective control of a fire suppression system to put out the fire and stop further damage. Now the organization has an area that has been damaged by both the fire and the fire suppression system, and it needs recovery controls.

Examples of recovery controls include:

- Managerial – training of new employees
- Technical – recovery from backups
- Physical – rebuilding the damaged area.

It is clear to see how controls often work in layers. One control provides a layer of protection at one level, but that control is supported by other controls. This is one example of defense in depth or layered defense. This will be examined in more detail in the networking section where defense in depth is commonly used to provide multiple obstacles to an attacker attempting to gain unauthorized access to assets of the organization.

One common control that was not used as an example above is closed circuit television (CCTV). That is because CCTV is an excellent example of a control that fits into numerous control categories. While CCTV is a physical control (supported by the managerial control of monitoring and technical controls of passwords and secure communications), it can be seen as:

- A deterrent – the very presence of a camera may discourage crime
- A detective control – it can observe unauthorized behavior
- A corrective control – it can identify the type and scope of the incident to facilitate better response.

A recovery control – it can record the previous state of the systems to enable rebuilding

Compensating Controls

There is one more category of control that should be reviewed – compensating controls. Compensating controls are additional controls that attempt to compensate for, or address a vulnerability that is not effectively addressed through other controls. For example, a user is usually prevented from doing administrative functions on their desktop. This prevents the user from installing unauthorized software or deleting system critical files. However, that control would not work for privileged users such as system administrators that need privileged access in order to do their job. They cannot be prevented from performing administrator functions on the system. Therefore, normal preventive controls would not work. So, management deploys additional controls to compensate for that vulnerability through the use of additional controls. In this case, compensating controls could include 'dual control' where separation of duties is enforced through the managerial and technical controls are requiring two people to work together to complete a task. The organization also may require additional supervision or monitoring of activity by privileged users. All actions taken by privileged users may be written off to an external system that cannot be overwritten or deleted by the administrator. Compensating controls are additional layers of control of all types and

categories used to protect vulnerable assets of the organization that may not be adequately protected by other control.

Discussion: Examples of Controls

Provide an example of each of the following without using the examples listed above:

- **Managerial deterrent control**
- **Technical corrective control**
- **Physical directive control**

What type of control is an identity management system?

Implementation/Assessment

When an organization designs and implements a control, it does so with care and careful consideration. It wants to deploy controls that are effective, but moreover, cost-effective. The most expensive control is not always the best fit for the organization. It can be assumed that most controls are designed and implemented with the best of intentions, but not everything works out according to plan. Once deployed, a control may not be as effective as originally thought, and, over time, the control may lose some of its effectiveness so that it no longer provides the expected benefits.

When controls are designed, they should be designed to facilitate monitoring and testing. The controls need to facilitate access, generate logs, and have testing capability to allow management, auditors and regulators the ability to examine and assess whether the control is working correctly.

When controls are implemented, they should conform to the security and operational baselines mandated for the control – if a firewall is implemented in a remote location it still should be implemented according to the configuration required by the central IT management or security department.

When testing a control, the assessor should test all the aspects of the control – management of the control (training of users, monitoring, change control, etc.,), the technical operations of the control (it is working correctly), and the physical controls supporting the control (power, physical security, etc.,).

The results of testing and monitoring should be provided to management to allow management to be aware of any problems with the control environment and take corrective action when required. This corrective action may include replacing a control, enhancing a control, or implementing additional layers of control.

Access Controls

It could be argued that access controls are the heart of an information security program. Earlier in this course, we have looked at the foundation of security through risk management and policy and the leadership of information security through management involvement and strategic planning, but in the end, security all comes down to “who can get access to our assets (buildings, data, systems, etc.,), and what can they do when they get access?”

Access controls are not only about restricting access, but also about allowing access. It is about granting the correct level of access to authorized personnel and processes but denying access to unauthorized functions or individuals.

Access is based on three elements: subjects, objects, and rules.

Let’s take a look at those elements.

> A **subject** can be defined as any entity that requests access to our assets. The entity requesting access may be a user, a client, a process, or a program. A subject is the initiator of a request for service, therefore, it is called active. In some cases, a subject may have a defined level of privilege. This is often known as a clearance level.

A subject is:
A user, a process, a procedure, a client, a program etc.,
A subject is:
Active — it initiates a request
It requests a service from an object
A subject often has:
A level of clearance (permissions)

An **object** is a device, process, program, server, or other entity that responds to a request for service. While a subject is active in that it initiates a request for a service, an object is passive in that it takes no action until called upon by a subject. When requested, an object will respond to the request it receives, and if the request is wrong, the response will probably not be what the subject really wanted either. An object has an owner, and the owner has the right to determine who or what should be allowed access to their object. Quite often the rules of access are recorded in a rule base or access control list.

An object is:

A building, a computer, a file, a database, a printer, a server

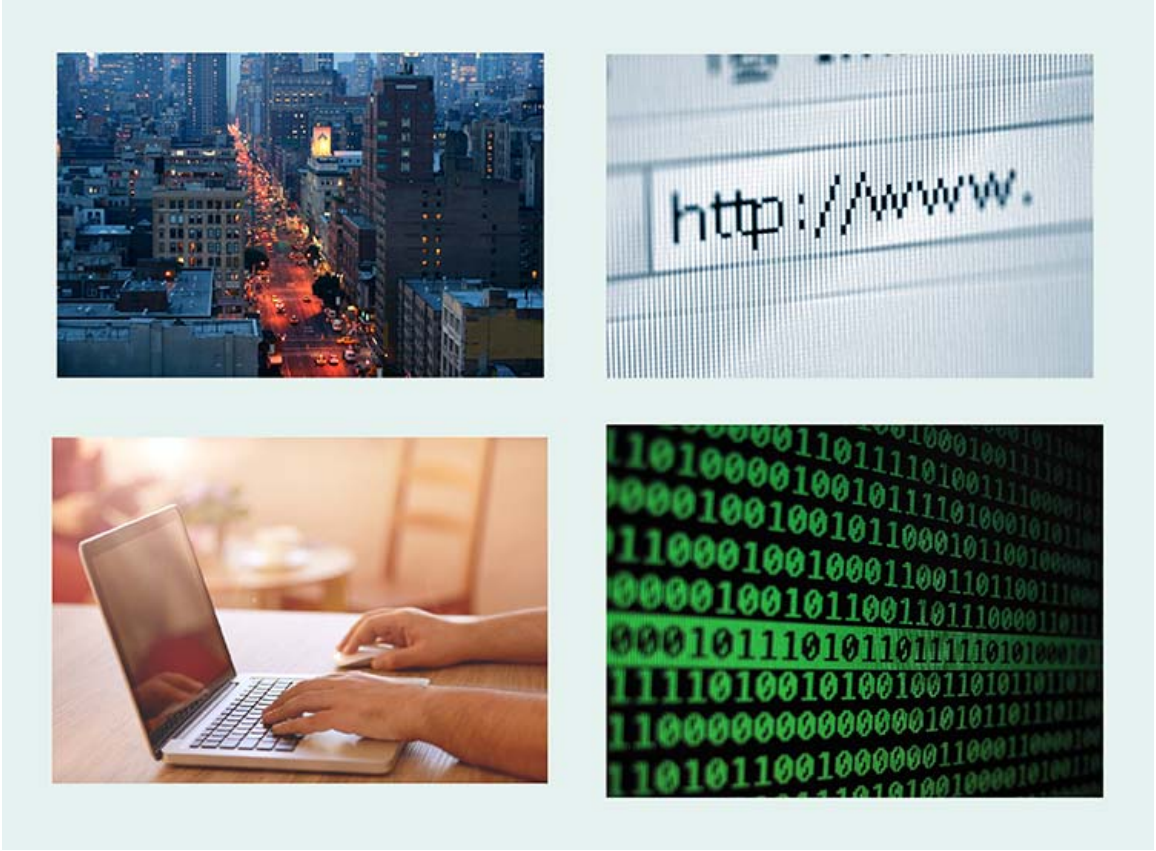
Anything that provided service to a user

An object:

Is passive

It responds to a request

An object may have a classification



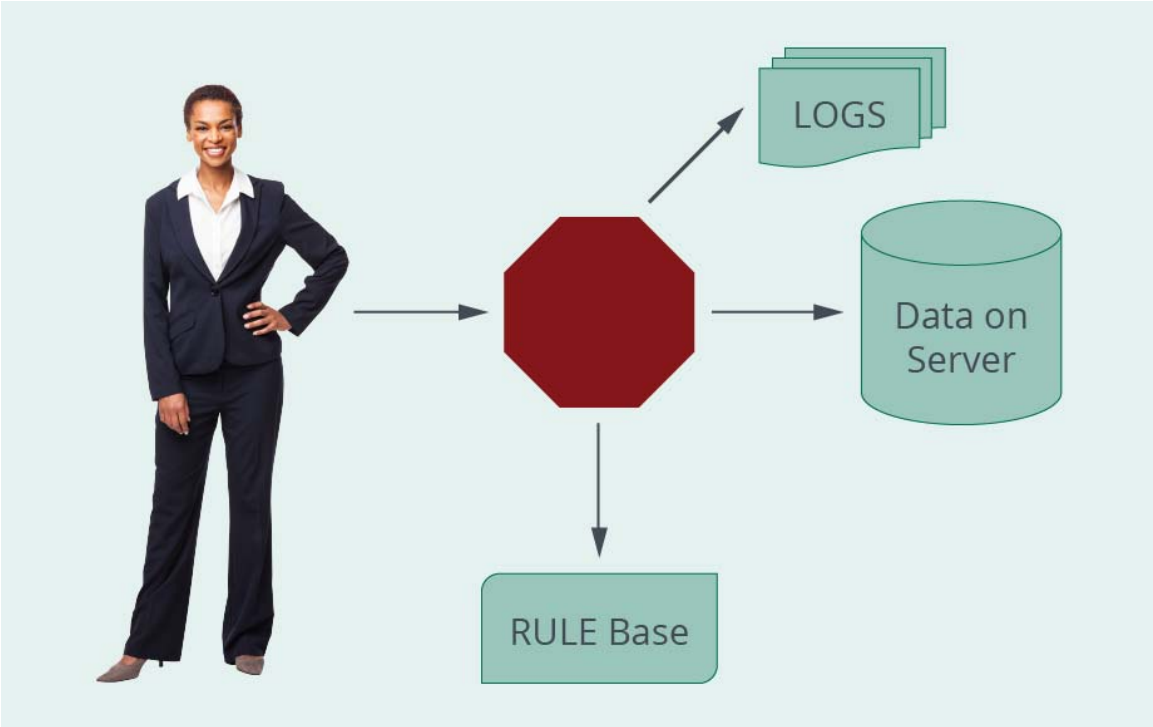
As you can see here, we are not just looking at system access. We are looking at all access permissions including building access, access to server rooms, access to network, applications, and utilities. All of these are implementations of access control and are part of the layered defense strategy developed by the organization.

The Reference Monitor

Now we will look at the mechanism that enforces access controls between a subject and an object. This is known as the reference monitor. The reference monitor is a conceptual idea of how access controls operate. The reference monitor describes the process of access control by demonstrating the regulating of access granted to a subject through the mechanism of intercepting the access request and then granting or refusing access based on the rules mandated by the owners of the object (the asset).

In actual fact, the reference monitor does not in itself exist. It is the concept of access control that is enforced through a mechanism such as a security guard, a lock on a door, or, in a computer system, by the security kernel. In all of these cases, we can see that the lock, the guard, and the security kernel do not decide who should have access, instead, they grant access to a person with the right credentials—the correct key or password. The security kernel enforces the decision of the data owner. The reference monitor should also have the ability to log all access requests, whether the access was granted or

denied, so that the owner can review the logs later as a part of monitoring to ensure that the access controls are set and operating correctly.



A subject wants to get access to data on a server.
The request is intercepted by the reference monitor that must determine if the access has been permitted by the owner of the asset - the data owner - it does this by checking the rules in the rule base set out by the owner

If access is permitted, then the subject gets access. The request (whether permitted or denied is logged)

The Information Management Model

Access to the assets of the organization, whether those assets are buildings, networks, applications, databases, or personnel, should be carefully designed, implemented, and maintained. The design of access controls can be facilitated through the use of an information management model (IMM). The IMM is simply a list of the three elements of access control: the subjects, the objects, and the rules that govern the access a subject should have to an object.

The first step is to identify all the potential subjects that may require access. This may include employees, managers, guests, customers, and auditors to name a few, but it also will include processes and programs that could access the systems and other processes within the organization. Quite often, the subjects will be grouped into roles of subjects that would require a similar level of access.

The next step is to identify all objects. That would include everything that could be accessed by a subject, including physical systems and technical systems. Once all objects have been identified, the third step can commence.

The third step is to determine the rules of access. That is, how will subjects be permitted to interface with objects. The rules of access are recorded and implemented onto the systems to restrict access according to the level of access required. This is often based on least privilege, where an entity requesting access is only granted the minimum level of access required to do their job, often only for the time they require that access.

User-Based versus Object-Based Access Control

There are two ways to view access control permissions. The first perspective is that of the user, or, "what is the user permitted to do?" The second is from the perspective of the object, or, "who is allowed to access this object/application?"

To manage access controls from the perspective of the user facilitates the oversight of user permissions and regular review to ensure that the permissions currently granted to the user are in line with their current job responsibilities. This review should be done at least annually to update and correct user permissions.

To manage access controls from the perspective of the object is also important. For example, an auditor may want to know who currently has access to the server room. In one case when I asked the security manager this question, the answer was quickly provided as a verbal list of a few names. In reality when a printout of the list of personnel that had access was generated, over thirty names were on that list—many of whom no longer even worked in that department or for that organization. This lack of review of access permissions has led to many security breaches over the years.

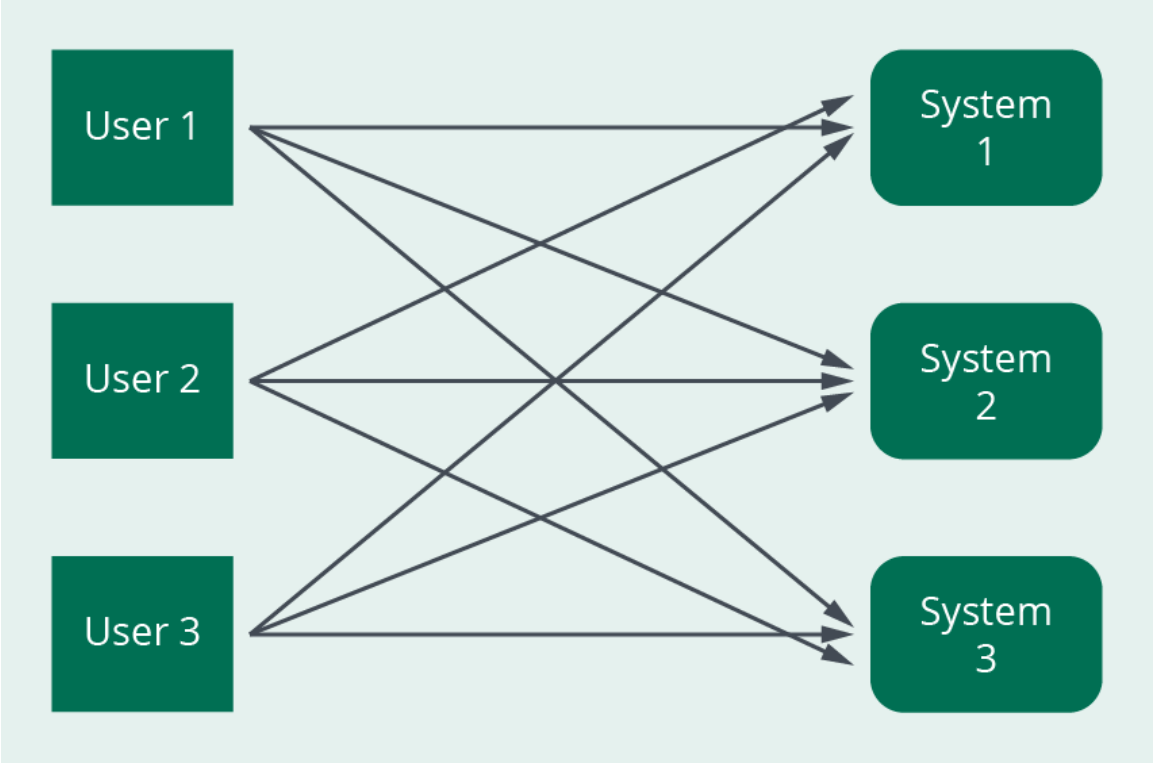
Temporal Access Control

Temporal, or time-based, access control is an important part of an access control implementation. Let's say an employee of an organization works from Monday through Friday from 8:00 AM to 5:00 PM. The employee is given an access card that grants them access to the building they work in and an identification (ID) on the systems they log into for work. Temporal access control would restrict that employee's access so that their access cards and ID would not work outside of normal business hours. This means that even if an unauthorized person stole the employee's ID or access card, they would

still be denied access outside of normal business hours. This can prevent misuse of the employee's access by cleaning staff or other personnel working after hours.

Rule-Based Access Control

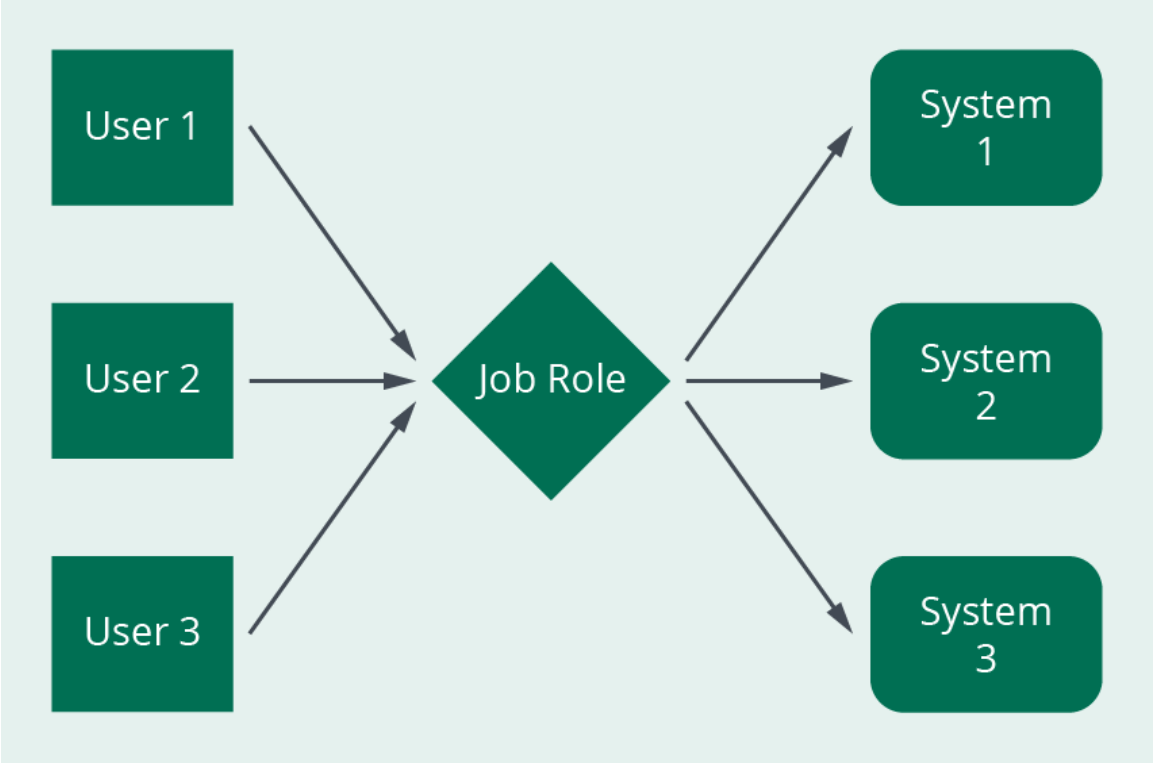
Rule-based access control is based on defined rules for each subject that controls what the subject can do. In a rule-based access control system, each subject is granted explicit access to an object by a rule that specifies that access right. In a large organization with many users and multiple changes in permissions, this can become an administrative nightmare. The administrators need to copy or create the rules for each user and maintain those rules as the roles and privileges of the users change. This can lead to a large number of users having access to systems they no longer require. In the world of compliance of today, where access to sensitive data should only be granted on a need-to-know basis, this can be a difficult system to maintain.



Role-Based Access Control (RBAC)

Role-based access control, or RBAC for short, sets up user permissions based on roles. Each role represents users with similar or identical permissions. A role is created that is assigned the access required for personnel working in that role. Then when a user steps into that role, all the administrator has to do is enroll him or her to make them a member of that role. If a user leaves

that role, the administrator only has to remove that one rule, and then all access associated with that role is removed. This works well in an environment with high staff turnover and multiple personnel with similar access requirements.



Attribute-Based Access Control (ABAC)

Attribute-based access control goes beyond the limitations of the access control models described above. Those models used a fairly simple relationship of user to object, whereas ABAC adds attributes (descriptors) to the subjects and the objects that can enhance the granularity or precision of access controls. For example, a user/subject may be a nurse working in a hospital cardiology department. There are many nurses in the hospital, but the access for each one is not only dependent on their job function of a nurse, but also on their placement within the hospital. A nurse in one department should not be able to access medical records for patients in another department, so each nurse is assigned attributes that describe their role within the nursing function, and each patient record is assigned attributes according to which hospital department it is in.

With ABAC, the attributes associated with the nurse will be compared with the attributes associated with the patient's medical record to ensure that access in only granted in accordance with laws and policy of the organization. This would ensure that only a nurse in cardiology could access the records of a patient in the cardiology department, and the nurse in cardiology would

not be able to access the records of patients in other departments. This is further explained in the NIST SP800-162 at nvlpubs.nist.gov.

Discretionary Access Control (DAC)

Definition: An access control policy that is enforced over all subjects and objects in an information system where the policy specifies that a subject that has been granted access to information can do one or more of the following: (i) pass the information to other subjects or objects; (ii) grant its privileges to other subjects; (iii) change security attributes on subjects, objects, information systems, or system components; (iv) choose the security attributes to be associated with newly created or revised objects; or (v) change the rules governing access control. Mandatory access controls restrict this capability. [Source CNSSI 4009]

Most information systems in the world are discretionary access control systems. In a DAC system, a user that has access to a file is usually able to share that file with, or pass that file to, someone else. This grants the user almost the same level of access as the original owner of the file. Rule-based access control systems are usually a form of DAC as per CNSSI 4009.

Mandatory Access Control (MAC)

Definition: An access control policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: (i) passing the information to unauthorized subjects or objects; (ii) granting its privileges to other subjects; (iii) changing one or more security attributes on subjects, objects, the information system, or system components; (iv) choosing the security attributes to be associated with newly created or modified objects; or (v) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints. [Source CNSSI 4009]

In a mandatory access control system, the user who has been granted access to a file cannot share that file with anyone else, and they cannot change the security attributes of the file unless they have been specifically identified as a trusted user.

Non-Discretionary Access Control

CNSSI 4009 defines NDAC as another name for Mandatory Access Control.

Summary

Access controls are a critical part of the information security program. They need to be carefully designed, implemented, and maintained to ensure continued protection of sensitive data and systems.

The Identity Lifecycle Overview

In this part of the course, we are going to look at the process of identity management. This includes the establishment, maintenance, and removal of identities on our systems. This area has changed almost in its entirety over the past few decades. Originally the only people on our systems were employees, and not many employees even had access to computers. Access was mostly granted at a system level to people in one building. In the 1990s, if you went to another building, you often had to find the Local Area Network Administrator (LAN Admin) and ask them to set up access for you in their building. But then came the world of the Internet and e-commerce. Now for many organizations, the majority of users on their systems are customers or other outsiders that they will never meet. This has moved identity management away from manual processes to automated systems, since there is no effective way to manage identities for all those external users through a manual process. It has also brought an increased requirement for network and systems architecture to isolate external users into safe areas, such as a Demilitarized Zone (DMZ), and keep them away from sensitive internal systems and data.

Identity management is often described using the IAAA model (or sometimes called the AAA) model. This represents the steps of identification, authentication, authorization, and accounting (sometimes called audit).

Identification

> Identification is the process of establishing a unique way to identify or distinguish one user or process from another.

FIPS 201-1 defines identification as:

> The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

The importance of identification is to establish accountability so that the actions of a person can be associated with the individual that committed those actions. This is important for reasons of non-repudiation and investigation.

Identification may be done in many ways including UserIDs, Social Security Numbers, Account Numbers, email addresses, biometrics, and DNA. These are often good identifiers since they are more likely to be unique than a person's name.

A challenge faced by many organizations is to allow people to register their own accounts and set their own identities. This removes the overhead of administrators trying to manage identities on behalf the users but also presents the opportunity for misuse. We often see that CAPTCHAs and other techniques are used to try to ensure that identities are only granted to real people and not to some type of bot attempting to create multiple IDs on the system. The process of establishing identities on a system should be a secure process so that only legitimate users are able to obtain a UserID.

Another form of identification is using a location or device to establish an identity. This is often called node authentication and uses a MAC (Media Access Control) address, IP (Internet Protocol) address, CPU serial number, or other device authentication technique to identify the location an administrator or user is using to log in from. Many wireless devices used to

use MAC filtering to restrict users to being able to log in only from registered wireless devices.

Authentication

Once a person has stated their identity, we need to validate that they are the rightful owners of that identity. This process of verifying or proving the ID is known as authentication. There are three common methods of authentication:

- Knowledge
- Ownership
- Characteristic

Knowledge

Knowledge-based authentication has been in use for thousands of years. Ensuring that someone is authentic and asking them for a passphrase or secret code has been used to differentiate between authorized and unauthorized personnel. Today we use knowledge-based authentication through the use of a PIN (Personal Identification Numbers), a password, a passphrase, or some other secret value that only authorized personnel should know. The problem with this type of authentication is that it is often vulnerable to shoulder-surfing or sniffing, where an unauthorized person can capture the password by looking over the shoulder of a person (perhaps using a camera at an ATM banking machine) or sniffing the communication during the login process. Since passwords and other knowledge-based systems often use the same password for a period of time (perhaps 30 days), the capture of the password would allow an attacker to log in as if they were the authorized user by performing a replay attack, where they replay the stolen login credentials.

Knowledge-based passwords are also subject to attacks such as brute force, dictionary, and rainbow tables, which will be explained later in the course once we have examined hash values.

A common problem with a knowledge-based system is a forgotten password. Within the organization, a password may be reset by the helpdesk, but the challenge is always how to ensure that the passwords are only reset for the correct user and not someone else calling in pretending to be another user and having that person's password reset.

Discussion: Protecting Passwords

What are some ways to ensure that passwords are only reset for the correct people?

Passwords

There are many opinions about what makes a strong password. Most often a longer password is considered stronger than a shorter one, and the use of special characters, numbers, and upper- and lowercase letters may provide additional strength, although we saw recently a breach where an organization allowed upper- and lowercase letters but actually converted everything to lowercase.

The other question is how long a password should be used before it must be changed. The main point to remember is the need to balance security with functionality and if the password rules are too stringent, then the users will almost certainly begin to work around the access controls and write passwords down or use the same password on multiple systems.

When a user has entered a password incorrectly multiple times, then it may be advisable to lock out the UserID being accessed. The point at which the account is locked is called the threshold or clipping level. The clipping level is set to allow for normal human error but to lock the account if the account is subject to a brute force attack.

Ownership

Another authentication factor is based on ownership. This has also been in use for many decades where a person could authenticate their identity through a letter, passport, driver's license, or badge. Today we also see ownership through the use of tokens (hardware- and software-based), smartcards, key fobs, and other hardware or software mechanisms.

Many tokens and smartcards are used to create a dynamic, or one-time password—a password that is only valid for a single login and then is not subject to a replay attack. The creation of a one-time password may be based on timing, where the password changes every minute or two; or the passwords may be based on events, where the password changes every time the user pushes a button on the device or uncovers a hidden value (scratch card).

Some ownership-based systems are synchronous (such as the timing- and event-based systems described above), while others are based on a challenge-response scheme (asynchronous). A challenge response scheme

operates on the principle that the access control server sends a challenge to the user. The user must then reply (respond) back with the correct response to the challenge. This response could be generated by a token or may just be the challenge encrypted using the user's password.

Ownership-based systems have the weakness that the loss or failure of the device may result in denial of service for the user; or a stolen device could be used by an unauthorized person to log into the organization.

Characteristic

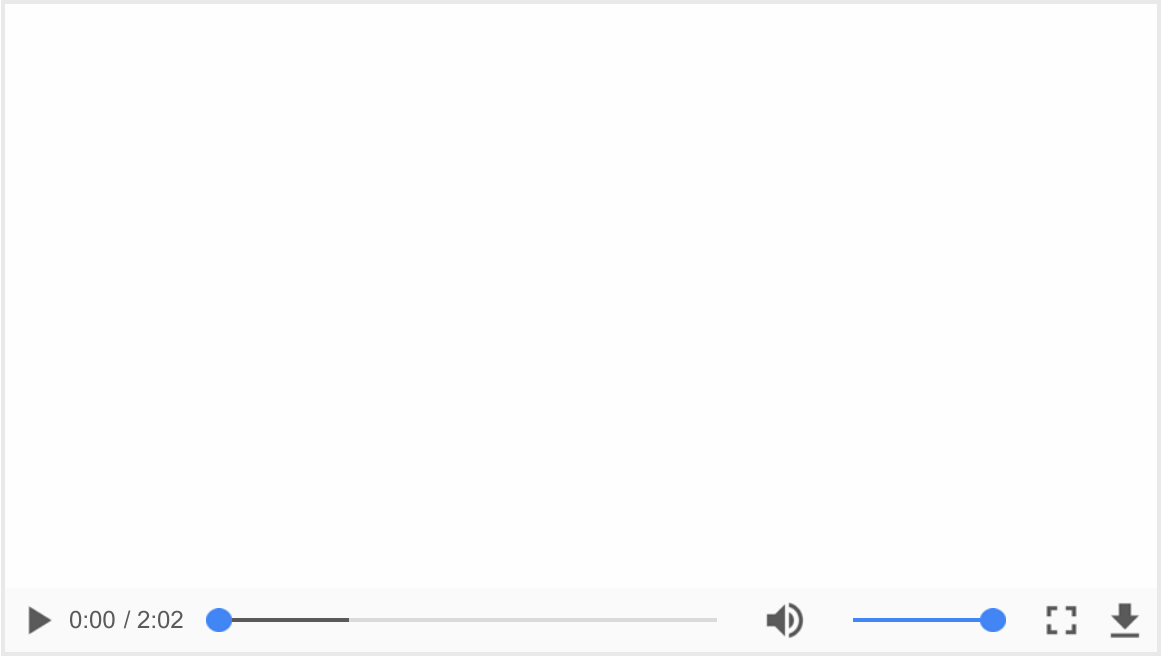
Characteristic-based authentication has also been in use for thousands of years as fingerprints were used to validate contracts in ancient Mesopotamia, just as they are used to log onto smartphones and laptops today. This form of authentication is commonly called biometrics from the Greek words *bio* for life, and *metrics* for measures. Biometrics today takes two primary forms—physiological and behavioral.

Physiological systems measure the characteristics of a person such as a fingerprint, iris scan (the colored portion around the outside of the pupil in the eye), retina scan (the pattern of blood vessels in the back of the eye), palm scan, and venous scans that look for the flow of blood through the veins in the palm. Some of the biometric devices will actually combine processes together to resist counterfeiting, such as checking for pulse and temperature on a fingerprint scanner.

Behavioral systems measure how a person acts by measuring voiceprints, signature dynamics, and keystroke dynamics. These systems measure behaviors such as the delay rate (how long a person holds down a key) and transfer rate (how rapidly a person moves between keys) as a person types.

Biometric systems are considered to be quite accurate, but they are also plagued by challenges. Biometric systems are rather expensive to implement and maintain due to the cost of purchasing equipment and registering all the users. Users may also be uncomfortable with the use of biometrics, considering them to be an invasion of privacy, a risk of disclosure of medical information (retina scans can disclose medical conditions), and the challenge of sanitization of the devices.

The implementation of biometric systems can also be a good example of the challenge of finding the ideal setting or "sweet spot" for the device. The sensitivity of biometric devices can usually be adjusted, and this will affect the accuracy of the device. This can be seen from the diagram below.



▼ Transcript

It is possible to adjust the sensitivity settings on biometric devices. A higher sensitivity setting would indicate a higher degree of precision or accuracy. We see the effect of increasing the sensitivity since this would increase a number of authorized personnel that would be rejected by the biometric system even though they should have been accepted.

This is known as a type one error and is defined as the false reject rate. In many cases, this would just require the person to try to authenticate once again. But, in some cases, it would require a secondary form of authentication perhaps using a security card to validate the person's credentials. The problem with a low sensitivity is the number of unauthorized personnel that may be able to gain access if the system is not precise enough to differentiate between different users. This is known as a type two error or false acceptance rate. This is far more dangerous than a type one error for an organization since it could lead to an unauthorized person gaining access.

We can see that as we adjust the sensitivity of the device, the false acceptance rate decreases and the false reject rate increases. These two types of errors will intersect at what is known as the crossover error rate. This is the point at which the biometric device is most accurate. However, this may not be the setting chosen by the implementer of the device. If the device is protecting a secure location, the implementer may choose to set the sensitivity higher to ensure that the false acceptance rate is very low.

Strong Authentication

Each of the authentication techniques we have looked at has advantages and disadvantages, and no one method is good enough on its own to protect the assets of the organization. So, the solution is to use a combination of several authentication techniques together, for example, a smartcard with a pin number to combine ownership with knowledge. This use of two different factors is what is called 2-factor or strong authentication. An implementation of two of the same factor—facial recognition software with a fingerprint—is not usually considered to be 2-factor since both authentication techniques are the same. Most security solutions today recommend the use of at least 2-factor or 3-factor authentication.

Denial of Service

The problem with access controls is that the controls affect legitimate users a lot more frequently than they stop unauthorized users from gaining access. The organization's helpdesk has to deal with forgotten passwords on a daily basis, and this costs the organization time and money both for the helpdesk personnel and the loss of productivity for the user locked out of the system. Organizations have also been the victim of attacks where the attacker would cause a mass lockout of all the accounts of the users of a system.

An attacker who knew that many users select weak or predictable passwords conducted an intriguing attack on a bank in China. He selected a word that was quite possibly going to be used as a password and then tried to log into a user's account at the bank. He knew that if he tried several times then that user's account would be locked out, so instead of trying multiple passwords on one account, he wrote a script that would try to log into each account number of the bank using the password he had chosen. As a result, he found that several dozen users of the bank's online banking system were using that password he chose. Each time he was able to log in, he transferred money from the victim's account to his own.

Authorization

The process of authorization refers to the rights, permissions, and privileges granted to an authenticated user. Once the user has been identified and their identity verified through authentication, the user should be granted the appropriate level of access to the resources of the organization.

This is where the principles of least privilege and need-to-know apply. These principles both have a common theme, although they are slightly different. Least privilege only grants a person the minimum level of access required for them to perform their job function—perhaps read-only or guest level access.

Need-to-know is often based on classification of information that only grants access to information when required or according to the user's clearance. An example of this is to display only the last four digits of a credit card number to a person working for a merchant that accepts credit card payments. This prevents theft or misuse of the credit card by the employee.

A core element of authorization is the principle of separation of duties (also known as segregation of duties). Separation of duties is based on the security practice that no one person should control an entire high-risk transaction from start to finish. Separation of duties breaks the transaction in separate parts and requires a different person to execute each part of the transaction. For example, Bill may submit an invoice for payment, but it has to be approved by Sam prior to payment; or Bill may submit a proposal for a change to a system configuration, but Sam will review and need to approve the change before it can be implemented. These steps can prevent fraud or detect an error in the process before implementation.

It could be that Sam will sometimes input an invoice for payment, but he would not be able to approve the invoices he inputs. This is mutual exclusivity; Sam can perform both operations—input and approval—but not on the same invoice. However, if Sam and Bill work together to bypass the separation of duties, they could collude to commit fraud. This is called collusion.

Another implementation of separation of duties is dual control. This would apply at a bank where there are two separate combination locks on the door of the vault. Some personnel know one of the combinations and some know the other, but no one knows both combinations. It would require two people working together to open the vault, this is an example of dual control.

Accounting

Accounting (sometimes called auditing) is not the last step in the process since it happens throughout each of the previous steps. Accounting is to create a record or log all activity on the system. Each time a person logs in or out, attempts to access an application or a customer record, a log entry is created for later review. This is one reason that a UserID must be unique since that is the only way to associate a particular action with the person or process that initiated that action.

Logs should be protected to prevent the deletion of log entries or the deletion of the log file entirely. Sometimes writing a log off to a separate system that even the administrator cannot access does this. These logs may

be needed in case of an investigation or to prove compliance with laws or regulations.

Reviewing logs can be a mundane, boring process, and it can be hard to justify log review when there are other more pressing issues, but logs can be reviewed using tools to filter out critical data, and log review may alert the organization to activity that may be ongoing as part of an attack, even if the attack has not yet been successful. The challenge is to log the correct data and in the correct place to enable identification of a problem. As one Security Manager told me after a breach that had lasted for six weeks, they found that the logs contained almost nothing of value since they were logging the wrong things.

Feeding log data into a Security Information and Event Management (SIEM) system may also facilitate the capturing and analysis of log data by correlating data from many sources and gaining a larger perspective of the relevance of the log data.

Privileged Access

One of the challenges of access control today is that there are many different levels of access that need to be managed. It was much simpler to manage access when the only people on our systems were employees, but now we need to ensure that each user has the level of access they should have and that they do not have access permissions beyond what they should have.

There are some users of our systems that require privileged access: administrators, maintenance personnel, and management. These people require a level of access that poses a risk to the system itself or the data it manages. Misuse of privileged access can disable the system, delete data, remove security controls, and lead to a security breach. Least privilege for such personnel is still a high level of privilege.

Discussion: Privileged Access and Associated Risks

What are some steps that can be taken to reduce the risk associated with users that have privileged access to systems or equipment?

Review: Privileged Access and Associated Risks

As too many organizations have discovered, the failure to remove vendor default accounts and passwords has frequently led to the compromise of systems. Vendor accounts are almost always privileged accounts and must be carefully monitored or disabled to prevent system compromise.

Summary

In the next module, we will look at Identity and Access Management and some of the issues related to the implementation of access control. The materials covered in this module are critical to understanding how we will implement access controls on applications, networks and equipment throughout the rest of the course.