KnowBe4
Human error. Conquered.

WHITEPAPER

How to Run a Risk Assessment Program

by Roger A. Grimes

Table of Contents

Asset Inventory 2
Identify Threats 3
Risk Analysis 4
Identify and Implement Offsetting Controls 7
Evaluate and Update 9
KnowBe4's KCM GRC Platform 10
Additional Resources 10

Risk management is the identification, evaluation, prioritization, and mitigation of risks to maximize goals. Individual risk to an organization is most often shown as:

Risk = Likelihood of Threat x Estimated Damage From Theat if it Occurs

Or even more simply:

Risk = Probability x Severity

A risk assessment program is about identifying threats to assets, the likelihood of the threats occurring in a given time period, estimating the potential damage if the threat is exploited, and implementing appropriate controls to offset the biggest and most likely risks first and best.

All of this is made far easier on an initial and ongoing basis using a digital risk assessment or Governance, Risk, and Compliance (GRC) program. A risk assessment program can help you keep track of the various assets, threats, calculated risks, implemented controls, and accepted risks – on an ongoing basis. Calculations can be tweaked as assets, risks, and controls change over time. Here is a summary of the phases in any risk assessment program:

- Asset Inventory
- Identify Threats
- Risk Analysis
- Identify and Implement Offsetting Controls
- Evaluate and Update

Each of those phases will be covered in more detail below.

Asset Inventory

You can't protect what you don't know about. You need to get a detailed account of every significant asset in the company, starting with the grounds and buildings, vehicles, computer equipment, software, and everything that the company officially designates as an asset (with the notable exceptions of depreciation and goodwill). Your inventory should not include office supplies and minor items that are easy to replace. A good place to start to gather an inventory is in Accounting, if you have an Accounting department. If not, start going around and taking a physical inventory. Your physical inventory may exceed the official accounting inventory. Things not owned by the organization, but used by them, such as building and vehicle rentals, may be included in your inventory depending on the scope of your risk assessment. But in general, if you're unsure if the asset is used by your organization, include it in your risk assessment.

Collect the following information about these assets (not all inclusive and could vary by organization):

- Name
- Description
- The purpose (or mission) and criticality of the asset
- Type
- Cost/value
- Location
- Who owns and/or supports the asset
- User information (number of users, type of users, etc.)
- Security requirements
- Storage information and protections
- Physical security
- Environmental security
- Miscellaneous
- Other

Identify Threats

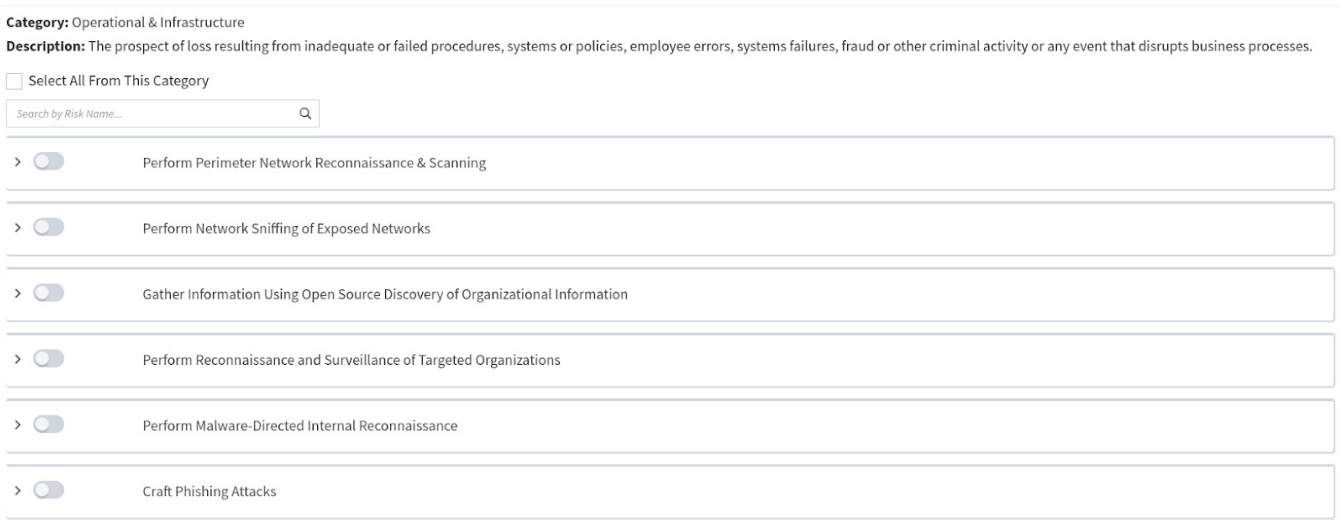
Next, threat model the asset. What are the different threats and risks that could compromise, destroy, or disable wanted access? Understanding how to perform good threat modeling can help you with this part of the risk management program. Start by brainstorming to identify likely threats against the asset. It could be natural events (e.g., weather, floods, pandemics, etc.), or unnatural events (e.g., war, bombing, hacking, etc.). You need to focus on both physical and logical threats and attacks.

Sometimes, it helps to identify particular categories of likely attackers, say malware, ransomware, nation-state attackers, script kiddies, financial thieves, physical criminals, insider threats, hacktivists, etc. Then create likely exploitation pathways. For example, attacks against computer assets are usually from one or more of the following categories:

- Programming bug (patch available or not available)
- Social engineering
- Authentication attack
- Human error/misconfiguration
- Eavesdropping/MitM
- Data/network traffic malformation
- Insider attack
- Third party reliance issue (vendor/ dependency/watering hole)
- Physical attack
- Brand new attack vector (w/o current/default mitigation)

While you don't have to think of and identify every possible threat and risk, you are trying to capture the most likely and most potentially costly threats and risks. The more you capture, the better. No one ever got in trouble for identifying too many threats and risks.

The screenshot below shows an example of sample risks listed in the KCM GRC program.



Risk Analysis

Determine the likelihood of the risk and threat occurring in a particular time period (most organizations use a year) and the range of likely resulting damage for each occurrence of a particular risk/threat happening. This is one of the most important and difficult parts of risk assessment. There will be times when you believe you are making a guess. When you do, try to make it an educated guess.

In the best possible case, you can use your organization's own experiences and data to help calculate risk (i.e., a data-driven risk management defense). Every organization existing for a set period of time has experienced some successfully exploited risks and threats, even if it is only malware that made it past anti-malware defenses for a limited period of time or petty theft. A good risk manager focuses on the most likely threats, especially those that are actively occurring or have recently happened and successful 100% mitigation has not yet occurred.

Concentrate on, in order of decreasing importance, the following types of risks:

- Risks and exploits actively and successfully used against your organization right now
- Risks and exploits likely to be used against your organization successfully in the near future
- Risks and exploits used successfully against your organization in the recent past without effective mitigations applied
- Everything else

The best risk managers focus on real risks from their own local data, and don't just rely on the risk rankings of others. For example, in a given year, there are over 10,000 distinct hardware and software vulnerabilities publicly announced. And in general, one-fourth to one-third of those potential threats and risks are ranked with the highest criticality. But in a given year, the average organization will only face a handful or two of those threats. The vast majority of those overall threats (98%) will never be attempted against any organization. A good risk manager separates real, most likely threats (2% of announced attacks) and separates them from the most likely "theoretical" highest risks.

In the computer security world, for example, most attacks against unpatched software involve, internet-facing software types (separated by client- and server-hosted):

Clients

- Browser add-ons
- Network-advertising services/daemons
- Operating Systems
- Productivity apps (Microsoft Office, etc.)

Servers

- Web server software
- Operating systems
- Database
- Server management software

This is to say that malicious hackers are not normally attacking unpatched accounting and video editing software. They can. And there are instances in which malicious hackers have attacked all sorts of software. But, in general, year in and year out, the above categories are what malicious hackers attack most often. A good risk manager realizes that patching the most likely to be attacked software first and best is more important than trying to patch all software, because you will never patch all software 100%. It's better to concentrate on better patching, with a goal of 100%, the most likely to be attacked software. Then apply that sort of training to all asset risks and threats. If your organization is located in South Florida, it's more likely to be threatened by hurricanes than earthquakes and tornadoes, even though there are chances of all those weather events occurring. Focus on the most likely things that would be damaged first.

The best risk management strategies focus on:

- Better risk ranking the most-likely threats
- Local threat and attack experiences
- Root causes of initial breaches
- Asking the right questions
- Getting and using good data
- Selecting the right defenses

Note: KnowBe4's Data-Driven Defense Evangelist wrote a book called A Data-Driven Computer Defense (https://www.amazon.com/Data-Driven-Computer-Defense-Way-Improve/dp/1092500847) on this subject, if you are interested in more details.

For many events, such as disasters, there are usually actuarial tables which can be accessed to help determine likelihood. Insurance companies are quite familiar with how often particular events, such as hurricanes, tornadoes, floods, fires, falls, crimes, and human disease events happen. The computer security world hasn't formalized the likelihood of different threats, but there are some base

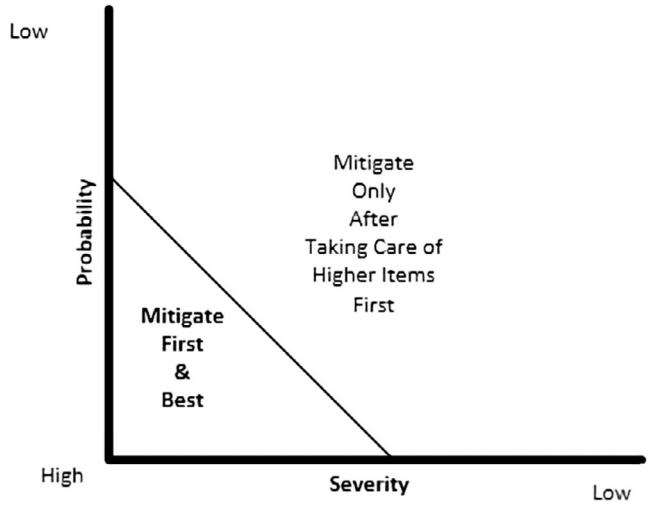
commonalities that have withstood the test of time and remain fairly consistent as far as likelihood. For example, social engineering and phishing are responsible for 70% to 90% of all malicious breaches. Unpatched software accounts for 20% to 40%, with overlap because both unpatched software and phishing attempts occur together. All other types of computer threats and risks account for less than 10% of malicious breaches (based on sheer numbers alone, and not including damage calculations).

Note: To read more about cybersecurity incident risk calculations see:
https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks

You need to calculate the likelihood of a particular risk or threat. It could be that a single occurrence could result in huge damages (for example, from a fire, flood, or other big weather event), but the likelihood is very low. For example, the odds of a hurricane impacting the central United States is fairly rare, but floods and tornadoes are not as rare.

Other events, such as ransomware, will be hard to determine as far as both likelihood and damage. I don't think anyone knows exactly when their organization will experience a ransomware event. Some organizations may have past experience with ransomware, but can't predict when it will occur in the future. Other leaders may believe that their organization is ripe for a ransomware attack and can't believe it has not happened. The key is to take your best risk management guess. If your organization has no experience with a particular threat, look to industry trade groups or national reports for data.

You want to mitigate the risks and threats that are likely to cause the most estimated damage (based on likelihood x severity) in a particular time period. Normally, as shown by the figure below, you want to first mitigate items with the highest likely potential damages (even if low likelihood) and highest probabilities (even if lower cost per incident).



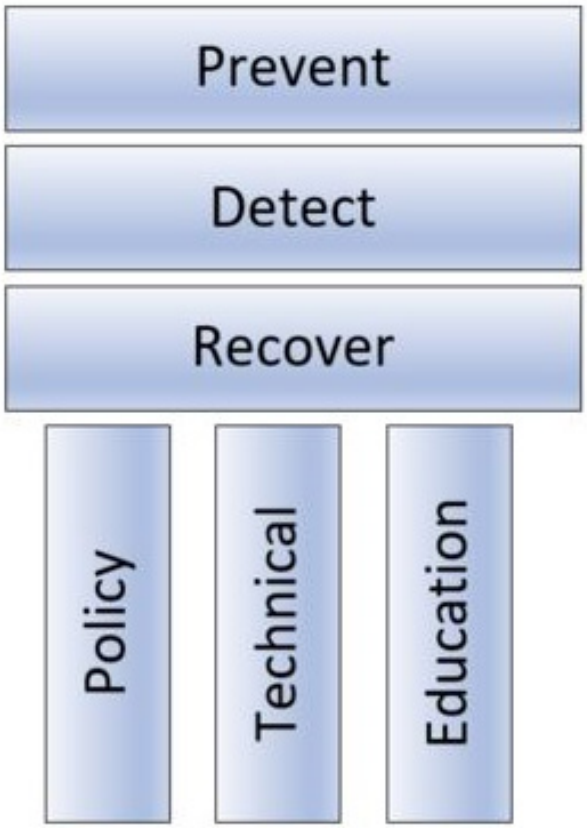
Risk assessment estimations are not an exact science, even in the world of actuarial tables. Usually, there are definite long-term trends, such as phishing and unpatched software causing the most malicious breaches, and heart issues and cancer causing a significant portion of human deaths. But then you have relatively unexpected events showing up, like COVID-19 did in 2020. Infectious disease experts have been predicting an infectious pandemic for decades, but no one knew when it would show up. Same with ransomware. Most people cannot predict when it will happen to them or if the impact will be wide ranging or impact just a few computers. But as a risk management assessor, you must simply take your best guesses and estimates—put a line in the sand, so to speak, and adjust as you learn more information over time.

Note: You always want to put numbers to your severity and likelihood assessments, even if your initial assessments are more general descriptions (such as unlikely, likely, very likely, etc.), because it makes the world of comparative risk assessments easier to perform and see.

Identify and Implement Offsetting Controls

Once you have identified the risks and threats that you want to concentrate on, it's time to identify and implement offsetting mitigation controls. The ultimate goal usually isn't to remove all potential risk for something happening, but to lower risk to an acceptable level. This isn't always the case, because in some cases, such as "Don't let enemies control nuclear bombs", the risk and threats damage consequences are so severe that the threat and risk must absolutely be prevented from happening at nearly all costs. But these types of binary scenarios are less likely than ones in which you attempt to significantly mitigate the risks and threats to an acceptable level.

The potential to offset controls includes all things that can prevent a particular exploitation event from happening, or if that fails, detect as soon as possible that a successful exploitation event happened, followed by methods to quickly recover and prevent the next event. Controls are made up of policies, technical safeguards and education. These three by three control pillars are graphically represented to the right.



Policy controls include anything written or verbal administrative controls which help to reduce risk. Examples are security policies, acceptable use agreements, rules, procedures, and documentation. Administrators verbally communicating and enforcing the policies is considered part of the policy tier. Technical controls include any physical or logical control that mitigates a risk to an asset. Examples include physical and environment protections, access control, firewalls, anti-virus software, security logs, and alerting systems. Education references all the teaching materials (e.g., policy documents, classes, videos, posters, human educator, etc.) that an organization uses to mitigate a risk. An example is educating employees to hover and inspect URL links to verify their legitimacy before clicking on them.

Note: You can read more about the three by three control pillars here: https://www.linkedin.com/pulse/3-x-security-control-pillars-roger-grimes

Every risk manager should consider all the controls necessary to mitigate particular risks and threats, including the cost, length of time to deploy, and how much estimated residual risk is left over after applying the control. Most controls are not 100% effective. That's why most defenses and risk management strategies use a "defense-in-depth" strategy where multiple overlapping controls help reduce the risk. In many cases, even with all possible, reasonable controls implemented, there is some sort of "residual risk" left over. The residual risk will have to be accepted, transferred (like with insurance), or otherwise further mitigated.

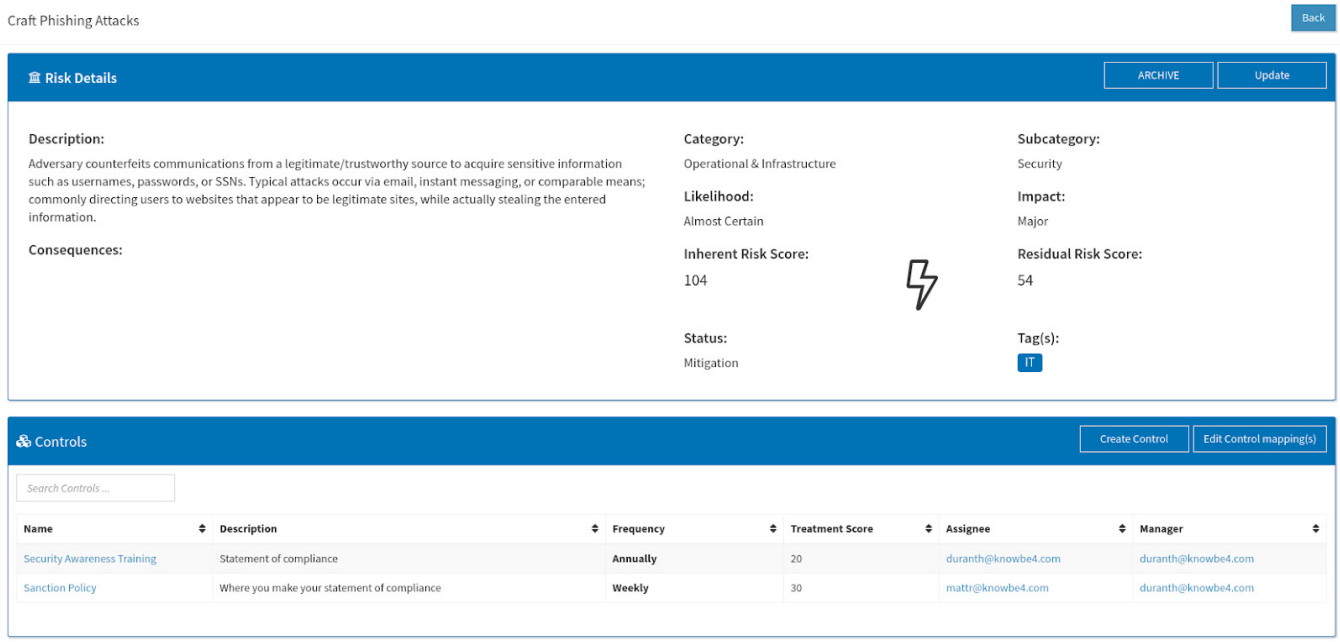
Note: You don't want to spend more on your mitigations than the estimated potential damage.

If you don't know where to start on mitigation controls, check out any of the popular guides (e.g., NIST, HIPAA, PCI-DSS, SOX, CIS Controls, Microsoft baseline security recommendations, etc.). They often have very comprehensive advice. Here are links to some of them:

- NIST Cybersecurity Framework (https://www.nist.gov/cyberframework)
- PCI-DSS (https://www.pcisecuritystandards.org/)
- Center for Internet Security (https://www.cisecurity.org/controls/)
- HIPAA (https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html)
- Microsoft Baseline Security Controls (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines)

Select, document, and implement the desired controls.

The screenshot below shows an example of a particular risk and selected offsetting controls from a sample from the KCM GRC program.



Evaluate and Update

During the period after implementing the desired controls, monitor threats and risks to see if any successful exploits happened, and if so, why? Successful exploits mean gaps in controls. Update your controls to handle the threats and risks you want to further mitigate. It could be that you expected and accepted that some successful exploitations will get through. Again, the goal of risk management is to significantly reduce risks to an acceptable level, not to necessarily remove all risks. It's not only very costly to remove all risk, but oftentimes impossible.

Determine how you will evaluate the effectiveness of the controls or even if they are in place and being used. Many entities perform an audit, where an auditor performs an assessment or does spot checks. Other organizations use self-reporting and questionnaires, or a mixture of the two approaches. But it is clear that without regular evaluation of whether security controls are in place and being effectively used that risk management becomes simply a paperwork exercise that doesn't reduce real risk. In order to have an effective risk management program, there must be ongoing evaluation and auditing of some sort. Some organizations use internal teams, some use external auditors, and others, again, use a combination. Everyone in the organization needs to understand that controls and auditing of those controls are to benefit the organization and everyone working for it.

Overall, you want to determine what controls were cost-effective and adequately reduce the risk they were designed to mitigate. Ineffective controls should be redesigned to become more effective or removed and replaced. You must decide on cadence and rhythm for future analysis and evaluation. Do you only do it once a year or continuous as additional risks and threats present themselves?

As stated in the beginning, risk management is the identification, evaluation, prioritization, and mitigations of risks to maximize goals. Picking a good GRC system which helps with that process can save you a lot of time, money, and resources.

KnowBe4's KCM GRC Platform

Most old-school, on-premise compliance applications require months of implementation and outside consulting help to deploy, as well as a commitment to yearly maintenance and support fees. Small, mid-sized organizations, and many divisions of multi-nationals can't afford this high cost, nor do they need an enterprise compliance platform. There are affordable, cloud-based alternatives, however. KnowBe4's KCM GRC, a pure SaaS platform, provides you with Compliance, Risk, Policy and Vendor Risk management modules to help you save tons of time getting through audit requirements. KCM GRC has a simple, intuitive user interface, easy to understand workflows, a short learning curve, and deployment that takes days, not weeks or months. It's also affordable for any size organization. KCM GRC makes it easy to get rid of spreadsheets and manual processes and efficiently manage risk and compliance both internally and for third-party providers.

Finish your audits in half the time and half the cost. Finally, affordable GRC for the rest of us.

Click here for more information »

Contact us at: Sales@KnowBe4.com, 855-KNOWBE4 (566-9234)

Additional Resources

- Osterman Research and KnowBe4, *The Critical Need to Improve Compliance Practices*
- *Costs of Non-Compliance with Privacy Laws*, September 2019
- CIOReview, *Enhancing Compliance Automation Efforts Step-by-Step*, Amy Matsuo, Principal, global leader for compliance transformation solutions, KPMG and Todd Semanco, partner, banking and consumer compliance risk, KPMG
- Shared Assessments and Protiviti, *2019 Vendor Risk Management Benchmark Study: Running Hard to Stay in Place*
- KnowBe4, *Starting Your Vendor Risk Management Strategy From Scratch*
- KnowBe4's *KCM GRC Platform*