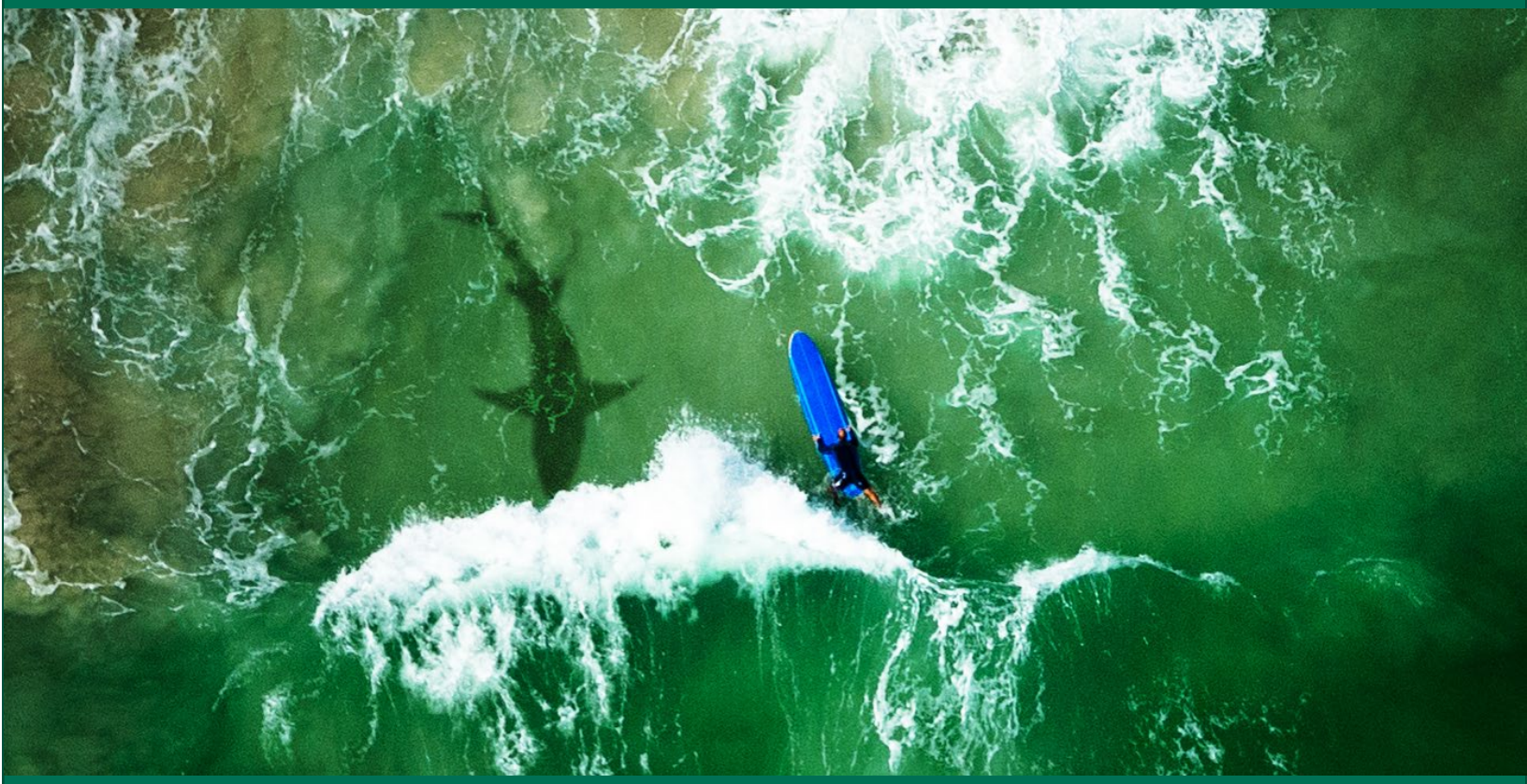


Collective Risk Model (CRM)

(2021 Version – May 2021)

EDITED BY JAMES TARALA & KELLI K. TARALA

“

Why should every organization be alone in their risk management? By collaborating on pragmatic risk management practices, we are free to focus on defending ourselves against the common threats that face us all.”

The 2021 version of the Collective Risk Model (CRM) is a community driven project. It is the result of numerous conversations between cybersecurity professionals over video conferences, dinners, in the hallways of security conferences, and over countless email exchanges. This is the first official and formal release of a simple, practical model that the community can use as a model for managing cybersecurity risks.

Scott Adams, of Dilbert™ fame, warns – never be the creator, always be the criticizer. Creators open themselves up to attack and criticism. It is better, he says, to show your moral and intellectual superiority through criticizing someone else's work than to create something yourself. With this project, we are violating that principle by organizing those conversations, cocktail napkins diagrams, and email exchanges into a repository for the community.

This effort is a work in progress. We believe that the 2021 version will be soon replaced with a more valuable version, along with future updates and improvements cycle that will follow. The community needs a risk model with straight forward language and a readily accessible roadmap to begin managing cybersecurity risks. We hope this is a starting point in that direction.

If you have suggestions or want to help, please contact us at the email address below. This will continue to be a community effort. This model is designed to evolve over time, and we hope this document will for years to come.

James Tarala
Kelli K. Tarala
Security Researchers, Enclave Security
research@enclavesecurity.com

Table of Contents

Introduction: What is the Problem?

Daily, organizations are faced with limited resources and competing priorities in their ongoing cybersecurity programs. Rarely do organizations have unlimited budgets, personnel, and time resources to invest in *any* aspect of their operations, let alone cybersecurity. This means that organizations must define methodologies for prioritizing their resources and their focus to those areas of operations in order to bring the organization the best return for their investments that align with their overall business priorities. The program activities of cybersecurity are no exception to this dilemma.

Add to the issue of competing priorities, the highly visible threat of cyber-attacks and data breaches are grabbing the attention of business executives and lawmakers around the world and these attacks and breaches are often times the result of misunderstanding of cybersecurity risks. Senior leaders in organizations from every industry are asking themselves if they have prioritized the appropriate activities to protect their organizations from cyber-attacks and data breaches. To add to this confusion, regularly self-proclaimed experts in cybersecurity offer competing advice on how organizations should best prioritize their defenses against this growing threat. Confusion and delays in implementing appropriate safeguards seems to be universal result.

Many generic risk management methodologies exist, and organizations can customize them to fit their cybersecurity needs. However, many of these generic standards are overly vague and do not provide organizations with specific, practical ideas they can use to create a defensive strategy to address this confusion and uncertainty, this Collective Risk Model (CRM) proposes a methodology to prioritized cybersecurity activities and provides guidance on how best to implement a cybersecurity risk management lifecycle.

Contributors

No project of this size is ever the work of just one person. Thankfully at the time of publishing this version of the Collective Risk Model (CRM), we have had numerous international organizations contributing to the effort.

The early work was performed by many of the same people who contributed to the Center for Internet Security's Critical Security Controls (CIS Controls). And this project was created from an urgency for a formal way of determining how to prioritize control selection based on threat priorities. As such, many of the contributors to that original project have been instrumental in the development of this risk model.

Work on this Collective Risk Model (CRM) has been an international effort. Representatives from numerous countries and international groups have contributed their time and resources to the development of this effort. In the future, we hope to continue to receive such broad support to help ensure that the information produced can be useful to any member of the global internet community.

People have often asked whether this model is specific to a particular industry. The answer is no, it has been correlated by a diverse group of organizations seeking to develop a broad understanding of risk. However, whether an organization works in the energy sector, financial services, or healthcare, if they are utilizing a Linux server or network router, then the risks to each system often overlap, regardless of the industry.

That being said, over the past few years there have been a number of dedicated contributors to this project, along with the Collective Threat Taxonomy and Collective Control Catalog, represent organizations such as:

- The SANS Institute
- The Institute of Applied Network Security (IANS)
- Black Hills Information Security (BHIS)
- The US Department of Homeland Security & other US Federal Agencies
- The US Federal Bureau of Investigation (FBI)
- NATO, the European Union & other International Governments
- US State & Municipal Governments
- Information Technology & Security Vendors
- Banks, Private Equity, Monetary Funds and others in Financial Services
- Energy Sector & others utilizing Industrial Control Systems
- Clinical Healthcare & Insurance Providers
- Universities and other Educational Institutions

We sincerely thank all of the people who spent their time to make this project a reality and hope to continue to see more organizations engage the project in order to make this a more helpful resource in the future.

Definitions

To begin it is important to define the terms that will be used throughout this risk model. In the field of risk management there is a great deal of confusion regarding the terms organizations choose to employ. In fact, no word carries with it a greater sense of vagueness and confusion than the word "risk" itself. The authors of this model often wonder if organizations should ban the word from their lexicons altogether and begin to use more specific terminology in its place.

Throughout this document there will be a number of terms, which are elements of risk, which will be utilized. To ensure organizations do so in a consistent manner, each of these terms should be clearly defined, as simply as possible, to ensure consistency in language. The following terms are terms that shall be used throughout this model, with a definition provided:

Asset

"A component of an overall information system or data."

Control or Safeguard

"A process or technology implemented to help ensure an organization is able to achieve a business objective."

Criticality

"The business value of an information asset."

Cybersecurity Risk

"The potential that harm to information systems or data will prevent an organization from achieving their overall business objectives."

Cybersecurity Threat

"The potential for something to cause harm to an information system."

Cybersecurity Vulnerability

"A weakness that could allow a cybersecurity threat to be realized."

Likelihood of Threat

"The probability of a cybersecurity threat being realized."

Risk Remediation or Mitigation

"Minimizing or eliminating the potential of a risk being realized."

A Two-Phased Approach to Risk Management

In modern cybersecurity risk management strategies, there is a large amount of confusion as to the *purpose* of risk management. Without a clear purpose, the methodology or steps of cybersecurity risk management remain unclear. Organizations struggle with clear definitions for terms like risk, threat, or vulnerability. Without clear definitions, an organization cannot build a clear process. Too many risk models are focused on the academics of risk rather than the practicality of understanding and limiting risk. We have simplified the cybersecurity risk management lifecycle into two primary phases – risk management for the purpose of control selection and risk management for the purpose of identifying gaps in a cybersecurity program. The assumption in place is that organizations have already prioritized the idea of reducing cybersecurity risk and are now ready to implement a methodology to reduce cybersecurity risks. Each of the other steps of risk management fall under one of these purposes.

Phase One: Risk Management for Control Selection

Phase One of risk management is to assess an organization's risk for the purpose of choosing the appropriate controls or defenses that the organization should implement in order to achieve their overall goals. Technology systems or business processes should always be implemented to achieve a specific goal. Normally this goal will be for greater efficiency, managing large amounts of data, collaboration, or other similar goals. Technology systems enable businesses to achieve these goals and are often relied upon exclusively to achieve these goals. In fact, many organizations rely so heavily on these technology systems that without these systems the organization may be unable to achieve even larger business goals.

In order to ensure that these business systems continue to function as intended, security controls must be implemented to protect these systems. The goal of these controls or defenses is to control or limit the potential for risk being realized. To ensure that these business goals are achieved, organizations must implement a process by which they appropriately decide which controls are the most appropriate for ensuring that their overall goals are achieved.

At a high level, a process of threat inventory and threat modeling can be used to select and prioritize the controls an organization chooses to ensure their goals are achieved.

Phase Two: Risk Assessment for Gap Analysis

The second phase of the risk management process is evaluating an organization in light of an agreed upon set of controls. Once an organization has determined the control library they believe is appropriate for defending their information systems, then they can perform a gap analysis to identify the controls that have not yet been implemented from their library. By understanding where an organization has not actually implemented their agreed upon controls, they can identify where risks may exist in the form of control gaps which could lead to harm to the organization. Such gaps could come in the form of completely missing a control or only a portion of their systems not meeting the determined goal.

This approach to risk management is the most common approach that organizations perform. Often organizations will even skip the first phase of risk management and move directly to this phase. Ideally organizations would take the time to document threat inventories, perform threat modeling, and use that information to prioritize the controls that they should implement. However due to resource constraints, most organizations will simply choose a pre-defined control list and perform their assessment against this list instead. In fact, very few organizations put in the effort to do the first phase. Organizations that take this approach will most often look to established standards or regulations as the foundation for such an assessment. The assumption is that the standards or regulatory bodies responsible for creating and maintaining the control library are performing the modeling efforts on behalf of their readers.

Examples of some of the more popular standards that are used for this purpose include:

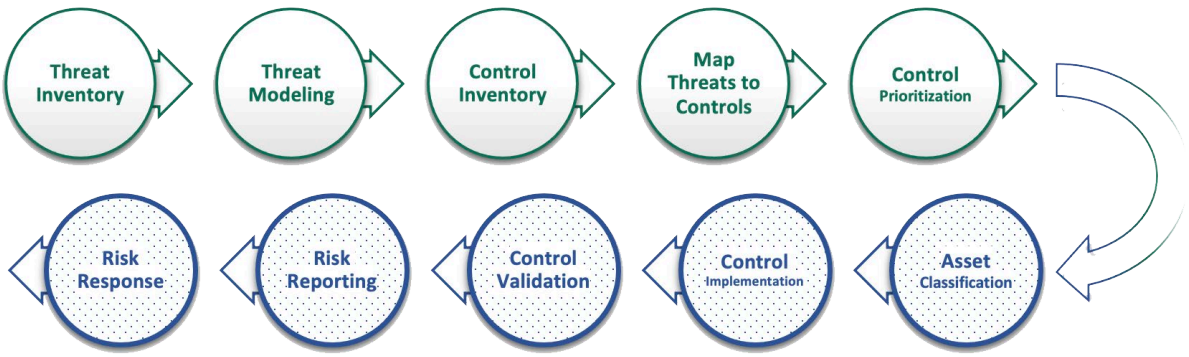
- The Collective Control Catalog (CCC)
- The Center for Internet Security Controls
- NIST Special Publication 800-53
- The NIST CyberSecurity Framework (CSF)
- ISO 27001 / 27002
- Cybersecurity Maturity Model Certification (CMMC)
- The Payment Card International (PCI) Data Security Standard (DSS)
- Other government or industry specific standards

If organizations decide that outsourcing the control selection process is most appropriate to achieve their business goals, then they should clearly define which of these standards will be used as the foundation for their security program. Typically, an organization will define a program charter, which defines the security program's goals, business requirements, stakeholders, and leadership structures. As an organization defines their goals for the program, they should formally document the standards, regulations, or contractual requirements that they will be working towards. This will help to ensure clarity in which controls the organization intends to implement as a part of the program.

Risk Management Lifecycle: Overview

As mentioned earlier, at a high level, the cybersecurity risk management lifecycle can be broken into two phases – control selection and gap analysis. However, as organizations begin to dive deeper into this process and examine which specific steps are necessary, a more complete picture begins to emerge. Within those two phases are a number of other steps that should be addressed. These steps should be followed in order, with the results of the earlier steps being used as inputs into the later steps. Information collected during each of the steps will be crucial for making better decisions during later parts of the lifecycle.

The following diagram illustrates the stages in the risk management lifecycle. Each of these steps will be considered in greater depth later. Once an initial pass through the lifecycle has completed, an organization can then edit the data from any of the steps, as long as the subsequent steps are then re-evaluated using the information collected.



Risk Management Lifecycle: Threat Inventory

The first phase of the risk management lifecycle is to create an inventory of existing threats that could potentially cause harm to information systems and data. The goal of this phase of the project is to create a *comprehensive* list of the threats that could cause harm to the organization's information systems. By identifying each of the items that the organization believes could cause them harm, it gives the organization an opportunity to define defensive controls to prevent, detect, or respond to such threats and the ability to prioritize each control. The more complete an organization can make this inventory, the more likely they will define a comprehensive strategy to addressing all relevant risks.

When defining threats, organizations should consider that there are different classifications of threats that can be defined. The four primary categories of threats are:

- Threat actors
- Threat actions
- Threat targets
- Threat consequences

The focus of this inventory should be the actions that a threat actor could take to cause harm to the organization. These will be the events that an organization will attempt to prevent, detect, or respond to with their defensive controls. While it may be interesting to groups, such as law enforcement, to define who is threatening an organization, it is likely not actionable intelligence for most organizations.

Existing research does exist in this field. Government entities and community research groups have documented inventories of threats that organization should consider as a starting point for documenting their own threat inventories. The following threat inventories are some of the commonly used libraries available:

- The Open Threat Taxonomy[1]
- ENISA's Threat Taxonomy[2]
- MITRE's ATT&CK® Framework[3]
- OWASP Top Ten[4]

Organizations should feel comfortable utilizing one of these inventories if their risk management resources are limited or they may choose to develop their own.

[1] https://www.auditscripts.com/free-resources/open-threat-taxonomy/
[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view
[3] https://attack.mitre.org/
[4] https://owasp.org/www-project-top-ten/

Risk Management Lifecycle: Threat Modeling

Once an organization has created an inventory of each of the potential threats that could cause harm to their information systems, they must find a way to prioritize those threats. The process of prioritizing a list of threats is also known as threat modeling. By prioritizing the threats with the potential to cause the organization harm they will eventually be able to prioritize the controls that are necessary to prevent such harm from occurring or to detect it if it occurs. However, that will be a later step in the process.

In order to create a prioritized threat list, each organization must determine the criteria by which they will prioritize each threat. Therefore, in addition to documenting an inventory of potential threats, the organization will need to decide the criteria that they will use to score each threat's relevance and overall importance. Finally, once the inventory and criteria are established, a weighting or scoring system will need to be established to consistently score each threat in the model.

The following criteria are examples of weights that an organization may use when creating their threat model:

- Threat Probability
- Damage Potential
- Business Impact / Severity
- Weights Assigned by Third Party Threat Analysts

When establishing a scoring system, the organization will need to document a consistent method by which they will rate each criterion for threat. It is not necessary that each threat criterion be scored the same as all the other criteria. However, each individual criterion should be scored the same way for each identified threat. For example, when scoring the probability of each threat occurring, the same scale should be used. However, the scale used when scoring the threat's probability versus damage potential do not necessarily need to be scored in the same manner. Typically, organizations will assign words that are meaningful to each score but translate each verbal score to a numeric system behind the scenes that can be used when calculating the score for each threat.

Risk Management Lifecycle: Control Inventory

After completing the threat modeling process, an organization should have a prioritized list of the events or actions with the potential to cause harm. This helps the organization better understand what events could happen that would stop them from achieving their business goals. This begs the question, what can the organization do to stop these threats and their harms from being realized?

An organization must begin by identifying a list of the controls or defenses that they could implement in order to address these threats. Just like with threats, organizations must then create an inventory of the controls they could potentially implement to better defend themselves. This list should also be as comprehensive as possible to give an organization the best chance of ensuring comprehensive coverage of identified threats.

As discussed earlier, numerous documents have been published to give organizations a starting point for inventorying potential defenses. Organizations will likely want to utilize these standards when creating a list of the controls they are considering. Once common place to start is with the laws and standards most relevant to an organization's industry group or demographics. For example, a small retailer will likely want to consider a different control library than a large, international defense contractor.

Risk Management Lifecycle: Mapping Threats to Controls

After inventorying and prioritizing the potential threats to the organization and identifying potential defenses against such threats, the next step in the risk management cycle is to map the threats documented in the threat model to the controls listed in the control library. By mapping or identifying which threats each control has the capability to address an organization will gain a more practical idea for what action items to take to address each threat in the inventory.

Since each threat has already been effectively prioritized in the threat model, once an organization maps controls to threats they will also have a prioritized list of controls as a natural result. Normally this process is most effective if the organization begins with the threat inventory as the primary field in the mapping and then links effective controls to each threat as they work their way through the inventory. Organizations will likely notice that each control may be used to address multiple threats and that not all controls in the control library are utilized. That is normal and to be expected during this stage of the cycle.

One of the more difficult aspects of this part of the risk management lifecycle is determining the completeness or coverage of each control as it relates to each threat. Organizations will likely realize during this mapping that multiple controls are often necessary in order to stop a particular threat. This is often referred to in the defense in depth model of information security. For example, to protect computer workstations against malicious code, an organization will likely want to implement application control restrictions. However, as effective as the control is, other controls will likely be necessary to completely address that particular risk. Unfortunately, judging the potential completeness of any control to address any specific threat is often an art as much as it is a science. Organizations should assume, however, that most often multiple controls will be necessary in order to address any specific threat.

Risk Management Lifecycle: Control Prioritization

The natural result of mapping prioritized threats from a threat model to controls is a prioritized list of defenses or security controls that an organization can implement in order to defend themselves against the identified threats. This stage of the risk management lifecycle is more the organic result of the previous stages than a dedicated set of actions that needs to take place. It is listed separately to illustrate the importance of these results, but organizations need not designate large numbers of resources to this effort. Rather, organizations should simply be able to take the results of each of the previous stages to naturally assemble a list of the most important controls necessary to defend themselves, prioritized via the above threat models. The resulting prioritized controls are often said to create an information security hygiene model for defense.

At the conclusion of this stage in the lifecycle the organization should have defined a prioritized set of controls and conclude the first stage of the risk management lifecycle.

Risk Management Lifecycle: Asset Classification

To begin the second stage of the risk management lifecycle, an organization should define the scope of what they are planning to defend. Most risk management models attempt to be granular in their approach and define this scope at the individual asset level. By asking specific control questions at the asset level, the result will be a richer and more detailed view of the specific risks in the organization. But the tradeoff to this approach is the time required to maintain the control status on individual assets.

This step in the lifecycle should both inventory and characterize each of the organization's information assets. This classification or characterization will allow the organization to determine where it is appropriate to implement the controls identified earlier in the process and prioritize which systems should implement specific controls before others.

There are specific data points an organization will want to gather, some of which include:

- Logical computing asset
- Data assets on each logical asset
- Data owner of each data asset
- Data custodian of each data asset
- Criticality of the data asset
- Sensitivity of the data asset

Performing a logical computing asset inventory is most often the result of running technology tools against a network environment. Asset inventory tools will provide the ability to determine which nodes are on any given network segment. Once these assets are inventories, an inventory of the data sets present on each logical asset should be performed. This is often a more manual process, although more and more tools are being released to help organizations to automate this process and identify network shares, databases, or other data sets that may be present on a logical asset. Organizations should also consider data managed by third party business partners or cloud service providers as a part of this inventory.

Once a data inventory is complete, data owners (business process owners) and data custodians (technical analysts) for each data set should be identified. These individuals should generally identify themselves as responsible for each data asset, rather than being assigned the responsibility. Data sets that do not have data owners should be questioned as to whether they are actually necessary for business operations. Once these individuals have been assigned then they should take the responsibility to define the criticality and the sensitivity of the data sets they are responsible for defending. Technical tools are also available to help facilitate this process (generally host based data loss prevention or cloud access security brokers).

For the sake of expediency, many organizations in their initial program maturity may choose to skip this step and simply perform a controls-oriented assessment against the organization as a whole. Rather than asking control implementation questions against every individual asset, they may choose to simply ask a higher level, subjective question against the organization as a whole. In other words, rather than asking, "Does this specific server have application controls enabled," they might ask, "What percent of our servers have application controls enabled?" This is a scoping question for every organization to consider, however as an organization moves closer to an automated, data driven approach to risk, this step will be vital in the process.

Risk Management Lifecycle: Control Implementation

Once an organization has agreed upon a prioritized library of controls that can be used to defend themselves, the next step is to the implementation those controls. It is time for the organization to actually do the things they have strategized to ensure their information systems continue to achieve the goals for which they were designed. The reality for most organizations is that resources are limited, however, and as much as they would like to do every possible thing to defend themselves, these resource constraints will limit what they are actually able to accomplish. Therefore, a project management approach to implementing these controls, in accordance with the established priorities noted earlier, would be most judicious.

As with any program an organization establishes, realistic goals and timelines must be established to achieve their goals. Although it may sound simple to do the things agreed upon, there are often competing priorities and disagreements about the importance of particular controls that may threaten to take the process off track. Leadership may also struggle with the concept of accepting risk for periods of time as security debt is addressed over the longer term. It is important that organizations stick to the fundamentals or project management as they work towards implementing their security control library. Following industry standards for project management, such as those established by the Project Management Institute[5], will help to ensure that each control implementation (project) is accomplished in a timely manner and in accordance with the organization's overall goals.

Organizations may also want to consider implementing a technical tracking tool to facilitate the project management lifecycle. Many organizations new to project management may consider simple spreadsheet-based tracking tools, while organizations with additional resources may consider utilizing a Governance, Risk, and Compliance (GRC) system to tracking control priorities and implementation progress. This will also assist with the validation and reporting phases later in the process. An example of a tracking tool that an organization may consider can be found at AuditScripts.com[6].

[5] https://www.pmi.org/

[6] https://www.auditscripts.com/free-resources/

Risk Management Lifecycle: Control Validation

After an organization has taken the time to implement their selected control library, it is important to introduce quality management into the risk management lifecycle. In the context of cybersecurity risk management, the idea of quality management is often referred to as control validation or information system auditing. More simply stated, once an organization has decided what they should do to defend themselves and have done the things they believe are right to defend themselves, then they should put a process in place to validate that they have actually done the things they believe are proper cyber defense. It is important that every organization regularly performs checks to ensure they are doing the things they have decided to do and that those actions are performed consistently.

Organizations may choose different types of audits to help ensure that the appropriate controls are being implemented in a timely manner. Most commonly organizations should consider external audits, internal audits, control self-assessments, and automated reporting tools. Organizations should remember that each of these different types of assessments has their place in an overall validation process. Each has a different set of resource requirements and output quality or assurance that should be considered when deciding which type to utilize and when. But likely a comprehensive approach of each is most appropriate as a part of a holistic approach to an organization's quality management program[7].

Risk Management Lifecycle: Risk Reporting

The next step in the risk management lifecycle is that the appropriate business stakeholders are educated on the risks that their information systems are exposed to – also known as risk reporting. Each of the earlier steps in the risk management lifecycle led to this point. The goal of any measurement program (metrics) is to help an organization to make better decisions. Therefore, once an organization has performed each of the following steps, the data obtained from the previous step (control validation) should be shared with the appropriate stakeholders so they understand the risk their systems face and can make better decisions on how to address the risk identified.

The presentation of risk is most often done by the reporting tools mentioned earlier (spreadsheets, GRC, etc.) and should be presented to all appropriate stakeholders. Stakeholders may include the business owners benefiting from a particular information system all the way to senior board level leadership in an organization. Any person effected by a risk being realized should have the opportunity to engage in this process.

[7] More information on the information systems audit process can be found at the Institute of Internal Auditors (https://www.theiia.org), the SANS Institute (https://www.sans.org/), and ISACA (https://www.isaca.org/).

Risk Management Lifecycle: Risk Response

Finally, once the appropriate business stakeholders have been educated regarding the risks facing their data assets, it is time for stakeholders to decide what to do with what has been presented to them. In a practical sense, when a risk is reported to stakeholders it is most generally in the form of gaps in security defenses (controls or safeguards) that should be in place to defend an asset. Early stages of the risk management lifecycle exist to define which controls are appropriate for an organization. Later stages exist to show the organization where they have not implemented the controls which they decided were appropriate for their environment. Therefore, when deciding how to respond to an identified risk, the organization is actually deciding how to respond to the reality that a control they believe should exist, does not currently exist.

In most organizations it is generally agreed that there are four potential responses to risks that have been identified:

- Ignore the Risk
- Accept the Risk
- Remediate the Risk
- Transfer the Risk

Ignoring the risk, is certainly not ideal response. However, it is by far one of the most common responses. Organizations often choose not to respond when they are faced with an identified risk. While results of ignoring a risk or accepting a risk are the same, the difference lies in how the organization reaches the destination.

Accepting the risk involves following a defined process to delay the implementation of a control until a later date – and should be documented and reviewed on a regular basis to validate the business' intentions in the future as well.

Ideally organizations would choose to remediate the risk and actually improve their defensive state. But resources do not always allow for this choice.

Often organization will attempt to transfer the risk via insurance or outsourcing the risk to a third party. However, transferring the risk generally only involves transferring some of the responsibility. Residual risk will always exist for the original organization as well.

Risk Management Maturity Levels

The reality is that most organizations will have the resources to implement each of these components of the risk management lifecycle immediately. Most organizations will need to take a phased approach to implementing each of these steps. It is appropriate for organizations to take advantage of resources that the cybersecurity community has collaborated on, rather than reinventing the wheel for themselves at each phase. In that light, and in light of observations made of numerous organizations, a phased approach to implementing the components of risk management has been developed to guide organization on where to prioritize their resources when implementing a risk management program. This model overlays the phases of risk management with the maturity levels defined by Carnegie Mellon University Software Engineering Institute[8]. The following table illustrates the priorities that organizations at different levels of risk management maturity should consider:

	Initial	Managed	Defined	Quantitatively Defined	Optimizing
Threat Inventory					X
Threat Modeling					X
Control Inventory	X	X	X	X	X
Map Threats to Controls					X
Control Prioritization	X	X	X	X	X
Business Impact Analysis			X	X	X
Control Implementation	X	X	X	X	X
Control Validation	X	X	X	X	X
Risk Reporting		X	X	X	X
Risk Response		X	X	X	X

[8] https://www.sei.cmu.edu/

Concluding Thoughts

An accurate understanding of threat can lead to better information security controls. Better information security controls can lead to better assurance of the continued confidentiality, integrity, and availability of information assets entrusted to our organizations. This project was created to fill a gap in the security community and provide a better understanding of threat. If organizations misunderstand or misinterpret threats, this will lead to inappropriate defenses and potentially a waste of valuable resources that could be used to better defend these assets. We hope this risk model is a step in the right direction towards understanding and creating programs for managing risk.

For this information to be useful, it must be accurate, and it must be current. As a community we can work together to make this more accurate. If we share our ideas and collaborate, then we can use this information to prioritize how we respond to the threats we collectively observe. We hope that as someone benefiting from this project, you will consider contributing to the effort as well. Please reach out to us if you believe you have information you can contribute that will help make this resource even more useful to others.

Please remember that this is a continuously evolving document. We hope to release many more versions in the future and on a regular basis. Expect the model to change and to grow. Eventually the need for quick updates will slow, but especially in these early phases, we expect there to be a number of regular updates that are released.

We look forward to your feedback and even releases ahead.

Enclave Security

1435 East Venice Ave, Suite 133

Venice, FL 34292

Enclavesecurity.com

Auditscripts.com