RISA Framework

Risk–based Information Security Approach

White Paper

A practical, risk based approach to Information Security

Curtis L. Blais
CCNA, CCNP, GCIA, GCFW, WCSP, CISSP
Savant Advisory Inc.

October 14, 2010

Version 1.0

Disclaimer:
All views expressed in this white paper are solely that of the author and may not represent the views of the company or companies with whom he is associated now, in the past or in the future, or any of his professional affiliations. This white paper looks into the application of a practical risk based approach to Information Security that is believed would help today's global businesses take a structured approach to Information Security through the application of a framework entitled RISA, developed by the author.

The author disclaims all warranties, expressed or implied.

About the Author:
Curtis L. Blais, CCNA, CCNP, GCIA, GCFW, WCSP, CISSP is a freelance information security, risk management, compliance and strategic consultant in Edmonton, Alberta, CANADA. He is also the Founder and Executive Consultant with Savant Advisory Inc. Mr. Blais has more than 20 years experience in the IT industry, is an accomplished speaker and presenter and is considered to be a leader and visionary in the Information Security space. His services have been provided to both public and private organizations, and international and global enterprises. Mr. Blais has provided presentation material to the US State department, invited to quote on security services to the US Army at the Pentagon, and is cleared to Secret. He can best be reached by email at curtis@savantadvisory.com.

Special Thanks:
The author wishes to thank the following individuals for their contributions toward the RISA Framework white paper:

Brian French, Ratko Spasojevic and Tim Truman

Savant Advisory Inc.

Contents

Introduction 1

Information Security Charter 3

Data Classification 6

Layers & Aspects 9

Bringing it All Together 14

Security Treatment Matrix 19

- Data 20
- Application 22
- Operating System 24
- Hardware / Firmware 26
- Logical 28
- Physical 30
- Personnel 33
- Governance / Compliance 35

Conclusion 36

Savant Advisory Inc.

Document History

Revision Date	Version	Author	Comments
Sept 27, 2010	0.1	Curtis L. Blais	Initial Compilation (Draft)
Oct 14, 2010	1.0	Curtis L. Blais	Version 1 Release

Savant Advisory Inc.

Introduction

This white paper is written to put forward a practical approach for Information Security that is foundationally built on risk. There is a lot of discussion in the Information Security industry about risk; however, almost no risk-based models (practical ones) are directly applicable to the people who implement the security measures for an organization. It is for that reason that the approach described below, if applied systematically, could have a dramatic effect on how Information Security is undertaken in an organization.

It is nearly impossible to identify how much security is "enough", especially when individual security measures (or technologies) are considered in isolation. The technology groups always seem to want more gadgets in the name of better security, but when pushed for the business justification or some measurable means to reveal how much more security would be provided, they are hard pressed to deliver anything more than "because we need it". The business areas typically see security as an impediment to moving the business forward and causing unnecessary expenditures, rather than the guardians of the data for the organization. It is this conflicting type of scenario, technology vs. business, which leads to a nearly random level of Information Security being applied within most organizations. It does not need to be this way.

When most people think of Information Security, they may only think of the latest technology gadget that stops hackers, or prevents viruses. They may think of firewalls, intrusion detection or prevention systems, encryption technologies or just big expensive boxes with blinking red and green lights and a never ending flow of support invoices. And while it is true that the items described above are technological tools used to help enforce Information Security within an organization, it does not provide for the essence for what Information Security's goal really is. The definition of Information Security is much simpler than most people realize; it is to provide the appropriate level of protection to the organization's most important asset, information.

Enter the **R**isk-based **I**nformation **S**ecurity **A**pproach or **RISA** for short. RISA is different from other approaches because it is a more tactical (specific security treatments applied at the appropriate levels) and logical (utilizing the class of data involved) approach versus information security voodoo. When the RISA Framework is applied in a systematic way, an organization can be reasonably assured that the Information Security measures that are applied are appropriate

for their information and information security becomes and enabler to the business[1].

The remainder of this paper explains the components required to realize the implementation of a RISA Framework within an organization and how those components lead to the definition of "appropriate" security for the information at hand. The components required are as follows:

1. An Information Security Charter
2. A Data Classification Standard
3. The Layers and Aspects Model
4. A Security Treatment Matrix

Like any security framework, this approach provides the essential building blocks to achieve an inclusive information security architecture with pre-defined security treatments to protect information; however, RISA was designed with flexibility in mind. Aspects of the framework can (and really should) be adjusted to fit the unique characteristics of the organization within which it is being applied. For example, the Data Classification standard that is discussed here will be shown with five classes of data. Under differing circumstances, a data classification scheme with three, or four, or even nine classes may be appropriate – depending on the environment. These types of changes will not affect the outcome of the RISA Framework in assisting organizations move to a more realistic and practical method of information security.

Finally, given the significant emphasis that is being placed on cloud computing, any organization considering migrating to such a strategy must adjust the focus of their security efforts closer to the heart of where Information security rests – the corporate data. Although this model has not been specifically tested within a cloud computing environment, through a number of discussions and review sessions, it is felt that the RISA Framework holds its integrity within a cloud computing configuration in the same way it does within an enterprise. Additionally, adopting a Cloud strategy necessitates that there are at least two other areas in a larger enterprise environment that would have a significant increase in their importance to ensure that the corporate data is secure; (1) the contracts area and (2) the internal auditors. These two other areas should be considered to ensure that the full extent of the cloud contract and the protection of the data (through the RISA Framework) are being met. These issues and their ramifications deserve an entire paper of their own.

---

[1] Please note that there is no silver-bullet that ensures absolute security of information; however, when security measures are applied in layers and aspects and as described in this framework, it is expected that your chances of successfully protecting your information improves significantly over an ad-hoc model.

Information Security Charter

If you have spent any time in the information security arena at all, what is about to be stated will hardly be a news flash or a revelation by any stretch of the imagination. However, the value of the topic requires that it be re-stated. To be effective within any organization, the Information Security group requires sufficient authority to:

1. Set Information Security Standards for the environment;
2. Design and apply security treatments that assist in the enforcement of the above;
3. Work within all IT related projects (including signoff) to ensure security standards are upheld; and,
4. Validate and report on compliance with the approved Information Security Standards.

To this end, the first component required within the RISA Framework is an Information Security Charter.

The purpose of the Information Security Charter is to put into writing a suitable level of authority for the group responsible for the Information Security for the organization. In many cases, responsibility and authority for Information Security tends to be relegated down through the ranks of the company in such a manner as it becomes ineffective in protecting the enterprise data. They become a reactive body that is only capable of attempting a cleanup of a security incident after it has occurred; and with every occurrence of an Information Security incident, the standing of the security group sinks lower and lower.

To counteract the negative spiral of events as listed above, the Information Security Charter's first order of business should be to describe the establishment of a Chief Information Security Officer (CISO) for the organization whose role is clearly articulated as the individual who is responsible to set the Information Security Standards for the enterprise. The CISO should also have a dual reporting type of arrangement with a "solid-line" reporting to the Chief Information Officer (CIO), or in the absence of a company CIO the Chief Technology Officer (CTO) or the highest ranking individual for IT in the organization. The second stream of reporting for the CISO is a "dotted-line" connection to the Chief Risk Officer (CRO) and/or the Chief Executive Officer (CEO), President, or Board of Directors.

The value in having this dual type of authority connection is to provide the CISO an alternate channel of reporting in the case that Information Security standards are being compromised at a lower level of the executive management of the organization. This organizational alignment would help to ensure the appropriateness of the information Security for the enterprise. The CISO should never be disconnected from the IT organization as they would lose valuable insight into the operations of the environment, which is another reason why a dual reporting type of arrangement is in order for this pivotal role.

Beyond the appointment, authority and reporting of the CISO the Information Security Charter should also contain the following items:

1. The mandate of the Office of the CISO (O-CISO)
2. A statement that indicates the Office of the CISO will conduct itself in accordance with the Code of Conduct and Ethics of the organization
3. Expand on the authority of the Office of the CISO indicating that all parts of the organization are expected to cooperate with CISO efforts.
4. A statement as to the "independence" of the Office of the CISO to ensure that appropriate Information Security measures are put into place.
5. Describe the scope of the activities of the Office of the CISO which include things like:
    a. Testing & validation of compliance with organizational security standards
    b. Reporting to the various bodies on the general state of information security for the organization (which is a good place to define security metrics – another subject worthy of an entire paper of its own)
    c. Participation in all pre-production projects to increase the potential for a successful production launch (from a security perspective)
    d. Monitoring for potential Information Security incidents with an aim to heading off major incidents before they occur (more to come on this through the Layers & Aspects model described later in this document)
    e. Investigation of Information Security incidents or related items and reporting on these items specifically with recommendations
6. A statement that indicates the Office of the CISO will, on some regular interval, assesses the adequacy of the charter and that it provides sufficient authority for it to undertake its mandate.

Once again, the list above is not intended to be exhaustive, and should be somewhat tailored to the specific culture of the organization it is intended to support. However, there is also a caution here in that if the Charter is too watered down and the Office of the CISO is not capable of setting and enforcing the Information Security Standards, then there is little value in creating the Charter at all.

Finally, the Information Security Charter should be signed by the highest level of the organization that is being reported to by the Office of the CISO. If there is a Board of Directors, then the Chair of the board should sign and activate the Charter. If the highest reporting level in the Charter is the President or CEO, then their signature should be garnered to enable the document.

If an example of a Charter of this nature is required, numerous variations can be found by a simple search on the Internet and tailored to meet the needs (with consideration given to the list above) of the organization.

The next component of the RISA framework to be described will become a critical piece of the framework in allowing the O-CISO to define appropriate measures to secure the most important item to all organizations – their data and its classification.

Data Classification

Although there are very few components to the RISA Framework, there is one portion that is fundamental to the structure's function; that is Data Classification.

In the over two decades of this writer's experience in the Information Technology industry, very few enterprises effectively utilize a Data Classification scheme as part of their strategy to protect information. This should be exploited to determine how the data itself it should be treated. As alluded to in the introduction, the overwhelming attraction for most organizations is to drop-ship a variety of the well know security technologies into their environment, hire some savvy technical people and implement the technology without any further consideration as to how much protection the data actually requires. The thought is, "There, security is done now – let's move onto the business." This approach exacerbates the lack of appropriate security measures in an organization.

With an empowered CISO in place and a signed Information Security Charter in hand, it is time to draft, approve and publish a Data Classification Standard for the organization. The data classification standard need only include two items:

1. A definitive list of data classifications organized from least important to most important to the overall strategy of the organization, with unique names;
2. Comprehensive definitions of the various data classifications that are relevant to the organization and the type of data handled.

With an escalating Data Classification Standard in place, it is possible to see where in the spectrum of data class the enterprise's information resides. The heat map in Figure 1 represents this spectrum. Data may fit anywhere along the color spectrum. Data that resides towards the bottom of the scale (or green end of the spectrum) is data that is less critical to the achievement of the strategic objectives of the organization or generally less sensitive in nature should it be exposed. Conversely, data that that resides along the top of the scale (or in the red zone) is data that is critical to the organization achieving its strategic objectives or highly sensitive in nature if publically exposed.

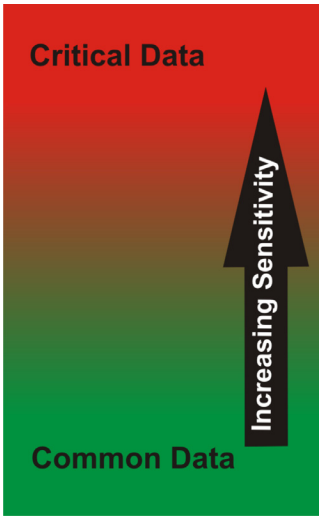


Figure 1

For example, hours of operation of a shoe manufacturing plant might well be considered classed as "common data". If exposed to the public, this would not damage their ability to manufacture shoes. However, the design of a new line of shoes to be manufactured may well be considered "critical data" as if exposed it would let the competition know what new design the shoe manufacturer had chosen. In the healthcare industry, lists of services may be considered more towards common, whereas patient records may be considered more towards critical. In the retail paint industry, available colors may be considered more towards common class, but manufacturers that will be carried in the retail outlets may be considered more towards critical class. Financial institutions will most certainly see customer account numbers and balances as critical, however branch locations would be considered public information. Through these simple examples it can be shown how the definitions of the various classes of data are unique to the various business data that is being protected. The key is to make sure that the data classes that are developed are specific to the organization/industry to which it is being applied.

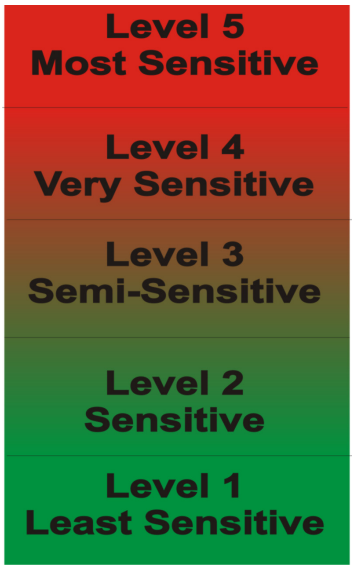


Figure 2

Now to take things one small step further, it is useful to define varying degrees or levels of classification within the full spectrum of classification as shown in Figure 2. For the purposes of illustration, five data classifications are identified in increasing levels of sensitivity. In the example, Level 1 data is considered far less sensitive than Level 5 data. Also, Level 2 data is considered to be more sensitive than level 1 data, but is less sensitive than level 3 data.

It would be difficult or nearly impossible to provide a set of definitions that are pervasive for all the potential business applications of the RISA Framework. What can be stated is that the definitions that are created must be done so with careful thought as to all the different type of data the enterprise utilizes to perform its functions and work towards its strategic objectives and that the definitions are all encompassing. This process will require a number of iterations before the organization has covered the full spectrum of the data utilized within the environment.

As an aside, with a Data Classification Standard in place, it is possible to link to an Enterprise Risk Management (ERM) scale to help quantify risk for the

organization. In larger organizations, there sometimes resides an ERM group that is tasked with assessing and managing organizational risk. In the environment where RISA was developed, this was the circumstance; an ERM group had published their own framework to help the entire organization quantify risk in a consistent manner across all areas of the organization. As it happened in this case, the ERM group utilized a common "Likelihood x Consequence = Risk" model with five levels of likelihood and five levels of consequence.

When the Data Classification scheme was drafted, the number of classifications was deigned to be five in conjunction with the consequence levels from the ERM group effectively tying a data classification directly to a consequence value. What this accomplished for the O-CISO, is that they need only check the classification of the data involved which again, lines up one for one with the ERM consequence levels (like operational, financial, reputational, or personnel) and apply a likelihood value to achieve a Risk quantification. This may not be applicable in all situations, however was extremely valuable where RISA was first developed.

In the next section two more concepts will be described before all of the items are brought together and shown how they may work in concert to provide a comprehensive risk based approach to information security. The two concepts deal with what is termed as Layers and Aspects.

Layers & Aspects

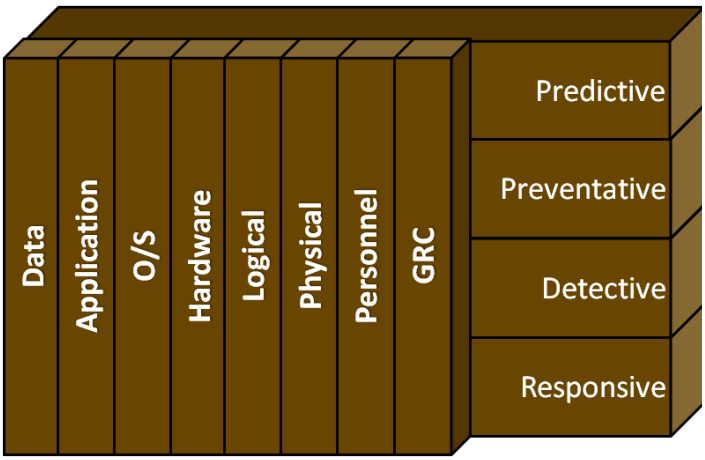
When it comes to the topic of layers and Information Security, there is a common understanding that layers are specific to a more physical approach to securing an IT environment. Starting from the "outside" and moving "in", each concentric "layer" has a very network centric security measure applied.

For example, consider an Internet connection to a large corporate environment. From the outside in one might expect the following items (not an exhaustive list) to be included from a "layered" perspective:

- Packet filtering at the ISP router filtering to the enterprise firewall
- Enterprise firewall filtering into the De-militarized Zone (DMZ)
- An Intrusion Prevention System watching packets coming in from the enterprise firewall.

To be clear – the "network security layer that is described above is NOT the type of layer that is referred to here in the RISA Framework. Layering takes on an entirely new perspective that starts with the enterprise data and moves through a series of steps that evolves from being very tactical in nature driving towards the logical components requiring consideration. Added to the model is a complimentary perspective that is applied to each layer which is called an Aspect. Both Layers and Aspects are described in more detail below.

Layers



Each layer of the model (the eight vertical bars), as shown in Figure 3, has unique threats, vulnerabilities and inherent security weaknesses. Recognizing that these layers exist and that together they cover a broad spectrum of segments that require some form of security treatment in order to protect an organization's information is the first step to understanding how RISA is designed to function.

It is very difficult to design an effective and comprehensive security solution without considering the differing types of risks, sensitivities or vulnerabilities at each individual layer. Gaps (or risks) are lowered by the combined strength of the security treatments applied at each of the successive, yet dissimilar, layers. The storage of the data may be susceptible to compromise in a completely different way than the layer above it – the application; however an application vulnerability may leave the data itself vulnerable. In the same way – the actual hardware may be susceptible to compromise in an unrelated way to the logical access controls of the system; and so on.

For example, if some sensitive data was stored on a system, its application tested for security weaknesses and all known vulnerabilities were mitigated; yet the operating system that the application resides on was left unprotected, it may be possible to leverage an un-mitigated vulnerability on the operating system to get to the sensitive data. This is why security treatments MUST be applied to each and every layer of the model – thereby providing true deep defence of the organization's information.

As shown in Figure 3, there are eight layers where security treatments can be applied and each of the eight is defined as follows:

1. **Data** – is defined as the raw electronic information stored for use by the enterprise to conduct the various business functions that support the overall strategy and operation of the organization. This information is utilized by some form of application within the environment (if it is not you have a totally different problem). Some examples may include: customer account numbers, credit card numbers, inventory, pricing, medical records, user-ids, strategies, plans, project documentation, general ledgers, personnel salaries, etc.
2. **Application** – is defined as computer software designed to help the user perform a particular task, meet a business requirement and/or meet a strategic objective of the organization through interaction with raw data. Some examples may include: Microsoft Office Applications, Microsoft Communicator, Adobe reader, Point of Sale suites, Customer Relationship Management, Accounting Software, Drawing software (engineering, architectural, or artistic), in-house and custom built applications, etc.
3. **Operating System** – is defined as software that provides and environment for the execution of computer programs or applications and may also provide various computer related administrative services. Some

examples include: Microsoft Windows, IBM's AIX, *NIX, OS/2, Novell, z/OS, TSO, VTAM, CP/M, Android, Palm O/S, Symbian, MAC O/S, etc.

4. **Hardware/Firmware** – (Hardware) the physical components of a computer systems and their base operating instructions or mechanical device. Examples include: Desktop/ Laptop Computers, Servers, Routers, Switches, Telephones, Blackberries, iPhones, Printers, Firewalls, IPS/IDS, Thumb drives, Robotic equipment, Photocopiers, etc. (Firmware) the fixed, usually rather small, programs and data structures that internally control various electronic devices and exists between hardware and some form of software – like an operating system. Some examples include: the BIOS in a PC, ROM/PROM chips in a router, Printer instructional code, code on network interface cards, etc.
5. **Logical** – is defined as logical safeguards for an organization's systems, including user Identification and password access, authentication, access rights and authority levels. Some examples would include: User ID's in Active Directory, Authentication, tokens, passwords, etc.
6. **Physical** – is defined as measures necessary (like physical barriers and control processes) to safeguard equipment and data, from access or threats by unauthorized persons or environmental (fire, smoke, temperature, etc) damage. Some examples include: Datacenters, locked doors, filing cabinets, floor to ceiling construction, security guards, CCTV surveillance, physical entry alarms, touchpad entry systems, humidity sensors, air conditioning, generators, etc.
7. **Personnel** – is defined as the practical management and administration of individuals or groups supporting organizational objectives. Some examples include: associates, contractors, partners and vendors.
8. **Governance & Compliance** – (Governance) is defined as consistent management, cohesive policies, processes and decision-rights for a given area of responsibility and it relates to decisions that define expectations, grant power, or verify performance. Some examples include: CobIT 4.1 Framework (as a model), Organizational charts with RACI responsibilities, Charters with terms of reference, etc. (Compliance) is defined as the goal that corporations or public agencies aspire to in their efforts to ensure that personnel are aware of and take steps to comply with relevant policies, standards, laws and regulations. Some examples include: following the password standard, meeting the requirements of PCI/DSS, Performing all of the items detailed in ISO-27001/2, following CMM, programming to OWASP specifications, the RISA Framework, etc.

Considering Information Security from a Layers perspective as described above provides a broad spectrum from which to consider how to secure the organizations information; however, another dimension needs to be considered in order to apply the best possible security treatment. This dimension is known as Aspects.

Aspects

When looking to apply appropriate security treatments at each of the layers as identified above, it is important to recognize that they must be observed from multiple perspectives. These perspectives are collectively referred to as ***Aspects*** (or "controls" for the more audit oriented), and they are listed and defined as follows:

1. **PREDICTIVE** - A mechanism that projects a future status before it occurs based on predefined trends, warning signals or the use of a knowledge base that incorporates past behavior.
2. **PREVENTATIVE** - A proactive measure taken to prevent or mitigate potential problems ***before*** they happen or worsen.
3. **DETECTIVE** - A measure taken to identify a potential problem either ***as it*** happens or after-the-fact; or, the extraction of particular information from a larger stream of information without specific cooperation from or synchronization with the sender.
4. **RESPONSIVE** - A measure or measures taken in reaction to an incident or negative event that has already occurred in order to correct or mitigate the incident or effected item or items.

By themselves, the Layers and Aspects provide exceptional coverage when considering the security of information; however, when applying these four Aspects to each of the Information Security Layers it allows for a full spectrum of security treatments to be considered. In order to give an example of how the Layers and Aspects combination functions, consider the following sample with respect to the second layer (Applications):

APPLICATIONS

Predictive (may include items like):

- Research CVE's (Common Vulnerabilities & Exposures) for the application
- Perform an Application Security Test (web or other)
- Assess risk based on classification of data (as described previously)

Preventative (may include items like):

- Patching cycle for the application
- Whether or not to use an application proxy to protect the application
- How often the application is tested (penetration testing)
- Should a security code review be performed

Detective (may include items like):

- Utilize a File Integrity Monitoring System (e.g., Tripwire)
- Install a Web Application Firewall

Responsive (may include items like):

- If breached – perform the following functions → (list of predefined tasks to perform)

The items as listed above are the security treatments that would be applied from an Application perspective. Each Layer of the Information Security Model would have a list of pre-defined items specific to that Layer geared towards protecting against potential threats and vulnerabilities.

In the next section it is time to pull all these components together to show how they can be leveraged to decide on appropriate security treatments.

Bringing it All Together

To this point the following list of items have been described:

1. **An Information Security Charter** – giving authority to the CISO to set and enforce standards
2. **A Data Classification Scheme** – that allows for the classification of the information within the organization with an increasing sensitivity
3. **The Layers and Aspects Model** – allowing for deep defense with respect to the organizations information

Individually, these items are all powerful tools to help provide a more complete coverage for an organization's information. The real power of the RISA Framework is shown when the Data Classification Standard is added to the Layers and Aspects model. Now, it becomes possible to predefine security measures based on the data classification itself. Since the Data Classification is aligned to increasing sensitivity of the data involved, the security treatment to protect the data can be designed to the appropriate security level. A greater number of security treatments are applied for sensitive data; and, a lesser number of treatments are applied for less sensitive items. The list of treatments essentially drives out the Information Security Architecture for the organization.

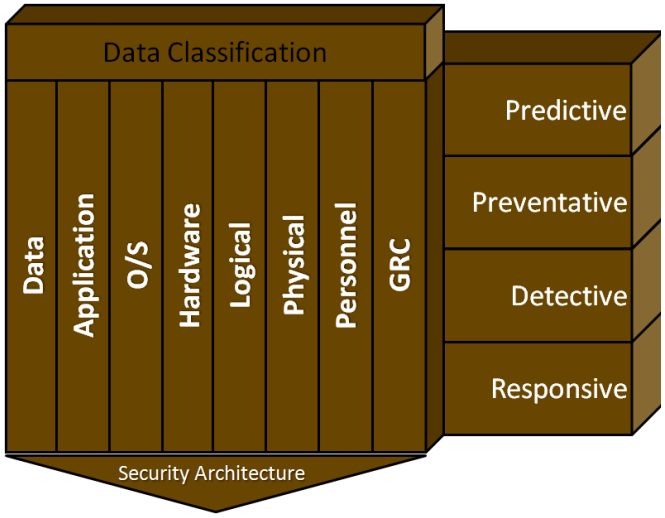


Figure 4

In cases where the Data Classification Standard is aligned to an Enterprise Risk Management framework (as discussed in the Data Classification Standard), it becomes much simpler to show how Information Security is ensuring the risk is within acceptable limits. This is how the RISA Framework utilizes risk to predefine security treatments for the data within an organization. Consider the following matrix that pulls all three of these items together for the Operating System (O/S) layer:

Layer	Aspect	Class. / Risk	Security Treatment
Operating System	Predictive		1. Perform a risk assessment and/or a penetration test of the operating system (or reference a recent previous risk assessment or Pen-Test of the same operating system configuration image) to quantify the level of risk associated with the specific operating system in use. 2. Research Common Vulnerabilities and Exposures (CVE) and security vulnerability trend information. 3. Analyze the information above and compare the previous layers Risk and the Data Classification (layer(s) below) and ensure that they are the same. If not – use the greater risk value of the two for this layer's security measures.
	Preventive	Level 1 Least Sensitive	1. Apply O/S Hardening Standard - Level 1 2. Network FW (port filtering) - No 3. Host Based IPS - No 4. Network Based IPS - Yes 5. O/S Integrity Control - No 6. O/S or Network Layer Test Frequency - Semi-Annually 7. Patching Cycle - Monthly 8. Virus / Malware Protection - Yes
		Level 2 Sensitive	1. Apply O/S Hardening Standard - Level 1 2. Network FW (port filtering) - No 3. Host Based IPS - No 4. Network Based IPS - Yes 5. O/S Integrity Control - No 6. O/S or Network Layer Test Frequency - Quarterly 7. Patching Cycle - Monthly 8. Virus / Malware Protection - Yes
		Level 3 Semi-Sensitive	1. Apply O/S Hardening Standard - Level 2 2. Network FW (port filtering) - Yes 3. Host Based IPS - No 4. Network Based IPS - Yes 5. O/S Integrity Control - Yes 6. O/S or Network Layer Test Frequency - Monthly 7. Patching Cycle - Biweekly 8. Virus / Malware Protection - Yes
		Level 4 Very Sensitive	1. Apply O/S Hardening Standard - Level 3 2. Network FW (port filtering) - Yes 3. Host Based IPS - Yes 4. Network Based IPS - Yes 5. O/S Integrity Control - Yes 6. O/S or Network Layer Test Frequency - Weekly 7. Patching Cycle - Weekly 8. Virus / Malware Protection - Yes

Layer	Aspect	Class. / Risk	Security Treatment
		Level 5 Most Sensitive	1. Apply O/S Hardening Standard - Level 3 2. Network FW (port filtering) - Yes 3. Host Based IPS - Yes 4. Network Based IPS - Yes 5. O/S Integrity Control (lockdown) - Yes 6. O/S or Network Layer Test Frequency - Hourly 7. Patching Cycle - Daily 8. Virus / Malware Protection - Yes
	Detective	Level 1 Least Sensitive	1. SIEM Candidate - No 2. Host Based IDS - No 3. Network Based IDS - Yes 4. O/S Integrity Control (identification) - No 5. Virus / Malware Protection - Yes
		Level 2 Sensitive	1. SIEM Candidate - No 2. Host Based IDS - No 3. Network Based IDS - Yes 4. O/S Integrity Control (identification) - No 5. Virus / Malware Protection - Yes
		Level 3 Semi-Sensitive	1. SIEM Candidate - Yes 2. Host Based IDS - No 3. Network Based IDS - Yes 4. O/S Integrity Control (identification) - No 5. Virus / Malware Protection - Yes
		Level 4 Very Sensitive	1. SIEM Candidate - Yes 2. Host Based IDS - Yes 3. Network Based IDS - Yes 4. O/S Integrity Control (identification) - No 5. Virus / Malware Protection - Yes
		Level 5 Most Sensitive	1. SIEM Candidate - Yes 2. Host Based IDS - Yes 3. Network Based IDS - Yes 4. O/S Integrity Control (identification) - Yes 5. Virus / Malware Protection - Yes
	Responsive	Level 1 Least Sensitive	1. Execute Response Plan: Level 1
		Level 2 Sensitive	1. Execute Response Plan: Level 1
		Level 3 Semi-Sensitive	1. Execute Response Plan: Level 2
		Level 4 Very Sensitive	1. Execute Response Plan: Level 2
		Level 5 Most Sensitive	1. Execute Response Plan: Level 3

The chart above shows the application of the RISA Framework to the Operating System layer. Remember – each layer is considered independently to ensure that the inherent risks or vulnerabilities specific to that layer are considered.

Each layer is viewed through the lens of the four Aspects – the first being Predictive. The Predictive Aspect is applied regardless of the classification of the data being considered and there is a list of three items that are taken into account to cover this specific predictive aspect:

> (1) Test the operating system for known vulnerabilities (before implementation);
>
> (2) Research Common Vulnerabilities and Exposures (CVE's) and other known sources of vulnerability trend information; and,
>
> (3) Compare the risks with the previous layer and compare to the data classification to ensure that the appropriate treatment selections will be made in the subsequent Aspects.

By looking at the Operating System layer through the lens of attempting to predict the potential exposures to the layer at hand – it is possible to understand the kinds of exposures that will need to be mitigated.

The next Aspect is Preventative. The Preventative Aspect is the first Aspect that leans on the Classification of the data in question. Remember – this is still only dealing with the Operating System layer, so the kinds of Preventive treatments listed will be specific to protecting at the Operating System level. The chart below shows the differing levels of treatments for the least and most sensitive data classes within the Preventative Aspect for the O/S layer:

Least Sensitive Data Class	**Most Sensitive Data Class**
1. Apply O/S Hardening Standard - Level 1 2. Network Based IPS - Yes 3. O/S or Network Layer Test Frequency - Semi-Annually 4. Patching Cycle - Monthly 5. Virus / Malware Protection - Yes	1. Apply O/S Hardening Standard - Level 3 2. Network FW (port filtering) - Yes 3. Host Based IPS - Yes 4. Network Based IPS - Yes 5. O/S Integrity Control (lockdown) - Yes 6. O/S or Network Layer Test Frequency - Hourly 7. Patching Cycle – Daily 8. Virus / Malware Protection – Yes

Notice how, based on the level of data classification, varying degrees of security treatments can be applied to appropriately and cost-effectively mitigate risk[2]. Since the classification of the data identifies the importance of that data (or risk to the organization regarding the data), the treatments that are selected are being chosen based on risk. No longer is it a guessing game as to how much security needs to be applied to a new application (and the data that is generated or manipulated as a result).

Please note, for the O/S hardening standard that is listed above, you will see that Level 1 and Level 3 have been indicated. The RISA Framework was not designed to be prescriptive as to what must be applied with respect to O/S hardening. Each organization will need to identify the various measures, based on their individual risk appetites, which they have at their disposal to protect the information in the environment and apply it using the RISA Framework. As a result of reviewing the potential treatments in hand for an organization – it may be discovered that there is not enough measures and more need to be added to a specific layer. Conversely – it may be discovered that far too much security is being applied to places where it is not warranted. Again – this is the strength of utilizing a framework that is built on risk – security treatments can be appropriately justified and help indicate where there is too much and not enough security.

In the next section treatments for all Data Classifications, within all Aspects applied to every Layer of the Security Model are laid out to provide what is termed the Security Treatment Matrix.

[2] Cost effectively in this circumstance is meant by not applying potentially expensive security treatments where they are not warranted.

Security Treatment Matrix

This section of the white paper contains a list of Security Treatments for all Data Classifications within each Aspect for all of the Layers of the Security Model. The matrix that follows will most certainly not be exhaustive with respect to all the possible security treatments available. It has been created to provide a glimpse into the possible types of security treatments available for each of the Layers. Other treatments may well exist (and new ones will most certainly be developed), and if applicable to the organization considering the use of the matrix, they should be added to the list in the appropriate location.

[See next page for the start of the Security Treatment Matrix]

Layer	Aspect	Class. / Risk	Security Treatment
Data	Predictive		1. Identify the Data Classification as identified by the data owner and ensure it matches based on the criteria as identified in the Data Classification Standard: a. Public – Minimal b. Internal – Minor c. Confidential – Moderate d. Critical – Major e. Restricted – Catastrophic 2. (Optional) conduct a risk assessment regarding the data and map result to the appropriate risk category as listed above.
	Preventive	Level 1 Least Sensitive	1. Encryption (at rest) – Choose an item. 2. Encryption (in transit) - Choose an item. 3. Direct Access to Data Store Allowed - Choose an item. 4. Backup - Choose an item. 5. DB Test Frequency - Choose an item.
		Level 2 Sensitive	1. Encryption (at rest) - Choose an item. 2. Encryption (in transit) - Choose an item. 3. Direct Access to Data Store Allowed - Choose an item. 4. Backup - Choose an item. 5. DB Test Frequency - Choose an item.
		Level 3 Semi-Sensitive	1. Encryption (at rest) - Choose an item. 2. Encryption (in transit) - Choose an item. 3. Direct Access to Data Store Allowed - Choose an item. 4. Backup - Choose an item. 5. DB Test Frequency - Choose an item.
		Level 4 Very Sensitive	1. Encryption (at rest) - Choose an item. 2. Encryption (in transit) - Choose an item. 3. Direct Access to Data Store Allowed - Choose an item. 4. Backup - Choose an item. 5. DB Test Frequency - Choose an item.
		Level 5 Most Sensitive	1. Encryption (at rest) - Choose an item. 2. Encryption (in transit) - Choose an item. 3. Direct Access to Data Store Allowed - Choose an item. 4. Backup - Choose an item. 5. DB Test Frequency - Choose an item.
	Detective	Level 1 Least Sensitive	1. File Integrity Monitoring - Choose an item.
		Level 2 Sensitive	1. File Integrity Monitoring - Choose an item.
		Level 3 Semi-Sensitive	1. File Integrity Monitoring - Choose an item.

Layer	Aspect	Class. / Risk	Security Treatment
		Level 4 Very Sensitive	1. File Integrity Monitoring - Choose an item.
		Level 5 Most Sensitive	1. File Integrity Monitoring - Choose an item.
	Responsive	Level 1 Least Sensitive	1. Execute Response Plan: Level 1
		Level 2 Sensitive	1. Execute Response Plan: Level 1
		Level 3 Semi-Sensitive	1. Execute Response Plan: Level 2
		Level 4 Very Sensitive	1. Execute Response Plan: Level 2
		Level 5 Most Sensitive	1. Execute Response Plan: Level 3

Layer	Aspect	Class. / Risk	Security Treatment
Application	Predictive		1. Perform a Risk Assessment on the Application and classify the risk into one of the following risk levels: a. Public – Minimal b. Internal – Minor c. Confidential – Moderate d. Critical – Major e. Restricted – Catastrophic 2. Research CVE's and potential exposures with respect to the specific application. Ensure that treatments for specific exposures are covered by actions below. 3. Perform an Application Security Test (Web or otherwise) and incorporate into predictive findings for classification. 4. Analyze the information above and compare the previous layers Risk and the Data Classification (layer(s) below) and ensure that they are the same. If not – use the greater risk value of the two for this layers security measures.
	Preventive	Level 1 Least Sensitive	1. Patching Cycle - Choose an item. 2. Application Proxy – Choose an item. 3. Application Test Frequency - Choose an item. 4. Security Code Review – Choose an item.
		Level 2 Sensitive	1. Patching Cycle - Choose an item. 2. Application Proxy – Choose an item. 3. Application Test Frequency - Choose an item. 4. Security Code Review – Choose an item.
		Level 3 Semi-Sensitive	1. Patching Cycle - Choose an item. 2. Application Proxy – Choose an item. 3. Application Test Frequency - Choose an item. 4. Security Code Review – Choose an item.
		Level 4 Very Sensitive	1. Patching Cycle - Choose an item. 2. Application Proxy – Choose an item. 3. Application Test Frequency - Choose an item. 4. Security Code Review – Choose an item.
		Level 5 Most Sensitive	1. Patching Cycle - Choose an item. 2. Application Proxy – Choose an item. 3. Application Test Frequency - Choose an item. 4. Security Code Review – Choose an item.
	Detective	Level 1 Least Sensitive	1. File Integrity Monitoring - Choose an item. 2. Web APP FW – Choose an item.
		Level 2 Sensitive	1. File Integrity Monitoring - Choose an item. 2. Web APP FW – Choose an item.
		Level 3 Semi-Sensitive	1. File Integrity Monitoring - Choose an item. 2. Web APP FW – Choose an item.
		Level 4 Very Sensitive	1. File Integrity Monitoring - Choose an item. 2. Web APP FW – Choose an item.

Layer	Aspect	Class. / Risk	Security Treatment
		Level 5 Most Sensitive	1. File Integrity Monitoring - Choose an item. 2. Web APP FW – Choose an item.
	Responsive	Level 1 Least Sensitive	1. Execute Response Plan: Level 1
		Level 2 Sensitive	1. Execute Response Plan: Level 1
		Level 3 Semi-Sensitive	1. Execute Response Plan: Level 2
		Level 4 Very Sensitive	1. Execute Response Plan: Level 2
		Level 5 Most Sensitive	1. Execute Response Plan: Level 3

Layer	Aspect	Class. / Risk	Security Treatment
Operating System	Predictive		1. Perform a risk assessment and/or a penetration test of the operating system (or reference a recent previous risk assessment or Penn-Test of the same operating system configuration image) to quantify the level of risk associated with the specific operating system in use. 2. Research CVE and security vulnerability trend information. 3. Analyze the information above and compare the previous layers Risk and the Data Classification (layer(s) below) and ensure that they are the same. If not – use the greater risk value of the two for this layer's security measures.
	Preventive	Level 1 Least Sensitive	1. Apply O/S Hardening Standard - Choose an item. 2. Network FW (port filtering) - Choose an item. 3. Host Based IPS - Choose an item. 4. Network Based IPS - Choose an item. 5. O/S Integrity Control - Choose an item. 6. O/S or Network Layer Test Frequency - Choose an item. 7. Patching Cycle - Choose an item. 8. Virus / Malware Protection - Choose an item.
		Level 2 Sensitive	1. Apply O/S Hardening Standard - Choose an item. 2. Network FW (port filtering) - Choose an item. 3. Host Based IPS - Choose an item. 4. Network Based IPS - Choose an item. 5. O/S Integrity Control - Choose an item. 6. O/S or Network Layer Test Frequency - Choose an item. 7. Patching Cycle - Choose an item. 8. Virus / Malware Protection - Choose an item.
		Level 3 Semi-Sensitive	1. Apply O/S Hardening Standard - Choose an item. 2. Network FW (port filtering) - Choose an item. 3. Host Based IPS - Choose an item. 4. Network Based IPS - Choose an item. 5. O/S Integrity Control - Choose an item. 6. O/S or Network Layer Test Frequency - Choose an item. 7. Patching Cycle - Choose an item. 8. Virus / Malware Protection - Choose an item.
		Level 4 Very Sensitive	1. Apply O/S Hardening Standard - Choose an item. 2. Network FW (port filtering) - Choose an item. 3. Host Based IPS - Choose an item. 4. Network Based IPS - Choose an item. 5. O/S Integrity Control - Choose an item. 6. O/S or Network Layer Test Frequency - Choose an item. 7. Patching Cycle - Choose an item. 8. Virus / Malware Protection - Choose an item.

Layer	Aspect	Class. / Risk	Security Treatment
		Level 5 Most Sensitive	1. Apply O/S Hardening Standard - Choose an item. 2. Network FW (port filtering) - Choose an item. 3. Host Based IPS - Choose an item. 4. Network Based IPS - Choose an item. 5. O/S Integrity Control (lockdown) - Choose an item. 6. O/S or Network Layer Test Frequency - Choose an item. 7. Patching Cycle - Choose an item. 8. Virus / Malware Protection - Choose an item.
	Detective	Level 1 Least Sensitive	1. SIEM Candidate - Choose an item. 2. Host Based IDS - Choose an item. 3. Network Based IDS - Choose an item. 4. O/S Integrity Control (identification) - Choose an item. 5. Virus / Malware Protection - Choose an item.
		Level 2 Sensitive	1. SIEM Candidate - Choose an item. 2. Host Based IDS - Choose an item. 3. Network Based IDS - Choose an item. 4. O/S Integrity Control (identification) - Choose an item. 5. Virus / Malware Protection - Choose an item.
		Level 3 Semi-Sensitive	1. SIEM Candidate - Choose an item. 2. Host Based IDS - Choose an item. 3. Network Based IDS - Choose an item. 4. O/S Integrity Control (identification) - Choose an item. 5. Virus / Malware Protection - Choose an item.
		Level 4 Very Sensitive	1. SIEM Candidate - Choose an item. 2. Host Based IDS - Choose an item. 3. Network Based IDS - Choose an item. 4. O/S Integrity Control (identification) - Choose an item. 5. Virus / Malware Protection - Choose an item.
		Level 5 Most Sensitive	1. SIEM Candidate - Choose an item. 2. Host Based IDS - Choose an item. 3. Network Based IDS - Choose an item. 4. O/S Integrity Control (identification) - Choose an item. 5. Virus / Malware Protection - Choose an item.
	Responsive	Level 1 Least Sensitive	1. Execute Response Plan: Level 1
		Level 2 Sensitive	1. Execute Response Plan: Level 1
		Level 3 Semi-Sensitive	1. Execute Response Plan: Level 2
		Level 4 Very Sensitive	1. Execute Response Plan: Level 2
		Level 5 Most Sensitive	1. Execute Response Plan: Level 3

Layer	Aspect	Class. / Risk	Security Treatment
Hardware / Firmware	Predictive		1. Perform a risk assessment and/or a security test of the hardware/ firmware (H/F) where possible (or reference a recent previous risk assessment or security test of the same hardware / software version) to quantify the level of risk associated with the specific H/F in use. 2. Research CVE and security vulnerability trend information. 3. Analyze the information above and compare the previous layers Risk and the Data Classification (layer(s) below) and ensure that they are the same. If not – use the greater risk value of the two for this layer's security measures.
	Preventive	Level 1 Least Sensitive	2. Apply H/F Hardening Standard - Choose an item. 3. H/F Revision Level Review Frequency - Choose an item. 4. H/F Configuration Integrity Control - Choose an item. 5. H/F Encryption - Choose an item. 6. Decommission - Choose an item. 7. H/F Test Frequency - Choose an item.
		Level 2 Sensitive	1. Apply H/F Hardening Standard - Choose an item. 2. H/F Revision Level Review Frequency - Choose an item. 3. H/F Configuration Integrity Control - Choose an item. 4. H/F Encryption - Choose an item. 5. Decommission - Choose an item. 6. H/F Test Frequency - Choose an item.
		Level 3 Semi-Sensitive	1. Apply H/F Hardening Standard - Choose an item. 2. H/F Revision Level Review Frequency - Choose an item. 3. H/F Configuration Integrity Control - Choose an item. 4. H/F Encryption - Choose an item. 5. Decommission - Choose an item. 6. H/F Test Frequency - Choose an item.
		Level 4 Very Sensitive	1. Apply H/F Hardening Standard - Choose an item. 2. H/F Revision Level Review Frequency - Choose an item. 3. H/F Configuration Integrity Control - Choose an item. 4. H/F Encryption - Choose an item. 5. Decommission - Choose an item. 6. H/F Test Frequency - Choose an item.

Layer	Aspect	Class. / Risk	Security Treatment
		Level 5 Most Sensitive	1. Apply H/F Hardening Standard - Choose an item. 2. H/F Revision Level Review Frequency - Choose an item. 3. H/F Configuration Integrity Control - Choose an item. 4. H/F Encryption - Choose an item. 5. Decommission - Choose an item. 6. H/F Test Frequency - Choose an item.
	Detective	Level 1 Least Sensitive	1. SIEM Candidate - Choose an item. 2. SNMP Candidate - Choose an item.
		Level 2 Sensitive	1. SIEM Candidate - Choose an item. 2. SNMP Candidate - Choose an item.
		Level 3 Semi-Sensitive	1. SIEM Candidate - Choose an item. 2. SNMP Candidate - Choose an item.
		Level 4 Very Sensitive	1. SIEM Candidate - Choose an item. 2. SNMP Candidate - Choose an item.
		Level 5 Most Sensitive	1. SIEM Candidate - Choose an item. 2. SNMP Candidate - Choose an item.
	Responsive	Level 1 Least Sensitive	1. Execute Response Plan: Level 1
		Level 2 Sensitive	1. Execute Response Plan: Level 1
		Level 3 Semi-Sensitive	1. Execute Response Plan: Level 2
		Level 4 Very Sensitive	1. Execute Response Plan: Level 2
		Level 5 Most Sensitive	1. Execute Response Plan: Level 3

Layer	Aspect	Class. / Risk	Security Treatment
Logical	Predictive		1. Perform a risk assessment and/or a security test of the logical safeguards where possible (or reference a recent previous risk assessment or security test of the same logical structure) to quantify the level of risk associated with the specific logical security mechanism in use. 2. Research CVE and security vulnerability trend information. 3. Analyze the information above and compare the previous layers Risk and the Data Classification (layer(s) below) and ensure that they are the same. If not – use the greater risk value of the two for this layer's security measures.
	Preventive	Level 1 Least Sensitive	1. Apply Electronic Authentication Standard - Choose an item. 2. Logical Cleanup Interval - Choose an item. 3. Require 3rd Factor - Choose an item. 4. Encryption for stored logical info - Choose an item. 5. Logical Test Frequency - Choose an item.
		Level 2 Sensitive	1. Apply Electronic Authentication Standard - Choose an item. 2. Logical Cleanup Interval - Choose an item. 3. Require 3rd Factor - Choose an item. 4. Encryption for stored logical info - Choose an item. 5. Logical Test Frequency - Choose an item.
		Level 3 Semi-Sensitive	1. Apply Electronic Authentication Standard - Choose an item. 2. Logical Cleanup Interval - Choose an item. 3. Require 3rd Factor - Choose an item. 4. Encryption for stored logical info - Choose an item. 5. Logical Test Frequency - Choose an item.
		Level 4 Very Sensitive	1. Apply Electronic Authentication Standard - Choose an item. 2. Logical Cleanup Interval - Choose an item. 3. Require 3rd Factor - Choose an item. 4. Encryption for stored logical info - Choose an item. 5. Logical Test Frequency - Choose an item.
		Level 5 Most Sensitive	1. Apply Electronic Authentication Standard - Choose an item. 2. Logical Cleanup Interval - Choose an item. 3. Require 3rd Factor - Choose an item. 4. Encryption for stored logical info - Choose an item. 5. Logical Test Frequency - Choose an item.
	Detective	Level 1 Least Sensitive	1. SIEM Report (Multiple logins) - Choose an item. 2. SIEM Report (Password Attempts) - Choose an item. 3. Logical Test Frequency - Choose an item.

Layer	Aspect	Class. / Risk	Security Treatment
		Level 2 Sensitive	1. SIEM Report (Multiple logins) - Choose an item. 2. SIEM Report (Password Attempts) - Choose an item. 3. Logical Test Frequency - Choose an item.
		Level 3 Semi-Sensitive	1. SIEM Report (Multiple logins) - Choose an item. 2. SIEM Report (Password Attempts) - Choose an item. 3. Logical Test Frequency - Choose an item.
		Level 4 Very Sensitive	1. SIEM Report (Multiple logins) - Choose an item. 2. SIEM Report (Password Attempts) - Choose an item. 3. Logical Test Frequency - Choose an item.
		Level 5 Most Sensitive	1. SIEM Report (Multiple logins) - Choose an item. 2. SIEM Report (Password Attempts) - Choose an item. 3. Logical Test Frequency - Choose an item.
	Responsive	Level 1 Least Sensitive	1. Exceeded Attempts Lockout - Choose an item. 2. Self re-set allowed? - Choose an item. 3. Execute Response Plan (on compromise): Level 1
		Level 2 Sensitive	1. Exceeded Attempts Lockout - Choose an item. 2. Self re-set allowed? - Choose an item. 3. Execute Response Plan (on compromise): Level 1
		Level 3 Semi-Sensitive	1. Exceeded Attempts Lockout - Choose an item. 2. Self re-set allowed? - Choose an item. 3. Execute Response Plan (on compromise): Level 2
		Level 4 Very Sensitive	1. Exceeded Attempts Lockout - Choose an item. 2. Self re-set allowed? - Choose an item. 3. Execute Response Plan (on compromise): Level 2
		Level 5 Most Sensitive	1. Exceeded Attempts Lockout - Choose an item. 2. Self re-set allowed? - Choose an item. 3. Execute Response Plan (on compromise): Level 3

Layer	Aspect	Class. / Risk	Security Treatment
Physical	Predictive		1. Perform a risk assessment and/or a security test of the physical safeguards where possible (or reference a recent previous risk assessment or security test of the same physical security structure) to quantify the level of risk associated with the specific physical security mechanisms in use. 2. Research current physical security vulnerability trend information. 3. Analyze the information above and compare the previous layers Risk and the Data Classification (layer(s) below) and ensure that they are the same. If not – use the greater risk value of the two for this layer's security measures.
	Preventive	Level 1 Least Sensitive	1. Location - Choose an item. 2. Guards Present - Choose an item. 3. A/C - Choose an item. 4. Power Conditioning - Choose an item. 5. Generator Facilities - Choose an item. 6. Humidity Control - Choose an item. 7. Fire Suppression - Choose an item. 8. Visitors Escorted - Choose an item. 9. Logical Locks (card with logs) - Choose an item.
		Level 2 Sensitive	1. Location - Choose an item. 2. Guards Present - Choose an item. 3. A/C - Choose an item. 4. Power Conditioning - Choose an item. 5. Generator Facilities - Choose an item. 6. Humidity Control - Choose an item. 7. Fire Suppression - Choose an item. 8. Visitors Escorted - Choose an item. 9. Logical Locks (card with logs) - Choose an item.
		Level 3 Semi-Sensitive	1. Location - Choose an item. 2. Guards Present - Choose an item. 3. A/C - Choose an item. 4. Power Conditioning - Choose an item. 5. Generator Facilities - Choose an item. 6. Humidity Control - Choose an item. 7. Fire Suppression - Choose an item. 8. Visitors Escorted - Choose an item. 9. Logical Locks (card with logs) - Choose an item.
		Level 4 Very Sensitive	1. Location - Choose an item. 2. Guards Present - Choose an item. 3. A/C - Choose an item. 4. Power Conditioning - Choose an item. 5. Generator Facilities - Choose an item. 6. Humidity Control - Choose an item. 7. Fire Suppression - Choose an item. 8. Visitors Escorted - Choose an item. 9. Logical Locks (card with logs) - Choose an item.

Layer	Aspect	Class. / Risk	Security Treatment
		Level 5 Most Sensitive	1. Location - Choose an item. 2. Guards Present - Choose an item. 3. A/C - Choose an item. 4. Power Conditioning - Choose an item. 5. Generator Facilities - Choose an item. 6. Humidity Control - Choose an item. 7. Fire Suppression - Choose an item. 8. Visitors Escorted - Choose an item. 9. Logical Locks (card with logs) - Choose an item.
	Detective	Level 1 Least Sensitive	1. CCTV - Choose an item. 2. Door Alarms - Choose an item. 3. Motion Sensors - Choose an item. 4. Flood Sensors - Choose an item. 5. Temperature Sensors - Choose an item. 6. Fire / Smoke Sensors - Choose an item. 7. Logical Locks (card with logs) - Choose an item. 8. Frequency of Physical Security Testing - Choose an item.
		Level 2 Sensitive	1. CCTV - Choose an item. 2. Door Alarms - Choose an item. 3. Motion Sensors - Choose an item. 4. Flood Sensors - Choose an item. 5. Temperature Sensors - Choose an item. 6. Fire / Smoke Sensors - Choose an item. 7. Logical Locks (card with logs) - Choose an item. 8. Frequency of Physical Security Testing - Choose an item.
		Level 3 Semi-Sensitive	1. CCTV - Choose an item. 2. Door Alarms - Choose an item. 3. Motion Sensors - Choose an item. 4. Flood Sensors - Choose an item. 5. Temperature Sensors - Choose an item. 6. Fire / Smoke Sensors - Choose an item. 7. Logical Locks (card with logs) - Choose an item. 8. Frequency of Physical Security Testing - Choose an item.
		Level 4 Very Sensitive	1. CCTV - Choose an item. 2. Door Alarms - Choose an item. 3. Motion Sensors - Choose an item. 4. Flood Sensors - Choose an item. 5. Temperature Sensors - Choose an item. 6. Fire / Smoke Sensors - Choose an item. 7. Logical Locks (card with logs) - Choose an item. 8. Frequency of Physical Security Testing - Choose an item.

Layer	Aspect	Class. / Risk	Security Treatment
		Level 5 Most Sensitive	1. CCTV - Choose an item. 2. Door Alarms - Choose an item. 3. Motion Sensors - Choose an item. 4. Flood Sensors - Choose an item. 5. Temperature Sensors - Choose an item. 6. Fire / Smoke Sensors - Choose an item. 7. Logical Locks (card with logs) - Choose an item. 8. Frequency of Physical Security Testing - Choose an item.
	Responsive	Level 1 Least Sensitive	1. Execute Response Plan: Level 1
		Level 2 Sensitive	1. Execute Response Plan: Level 1
		Level 3 Semi-Sensitive	1. Execute Response Plan: Level 2
		Level 4 Very Sensitive	1. Execute Response Plan: Level 2
		Level 5 Most Sensitive	1. Execute Response Plan: Level 3

Layer	Aspect	Class. / Risk	Security Treatment
Personnel	Predictive		1. Perform a risk assessment and/or a security test specific to the people where possible to quantify the level of risk associated with the identified personnel. 2. Research current personnel security vulnerability trend information. 3. Analyze the information above and compare the previous layers Risk and the Data Classification (layer(s) below) and ensure that they are the same. If not – use the greater risk value of the two for this layer's security measures.
	Preventive	Level 1 Least Sensitive	1. Security Background Check - Choose an item. 2. Segregation of Duties - Choose an item. 3. Security Awareness Training - Choose an item. 4. Security Clearance - Choose an item. 5. Ethics Signoff - Choose an item. 6. Conflict of Interest Disclosure - Choose an item.
		Level 2 Sensitive	1. Security Background Check - Choose an item. 2. Segregation of Duties - Choose an item. 3. Security Awareness Training - Choose an item. 4. Security Clearance - Choose an item. 5. Ethics Signoff - Choose an item. 6. Conflict of Interest Disclosure - Choose an item.
		Level 3 Semi-Sensitive	1. Security Background Check - Choose an item. 2. Segregation of Duties - Choose an item. 3. Security Awareness Training - Choose an item. 4. Security Clearance - Choose an item. 5. Ethics Signoff - Choose an item. 6. Conflict of Interest Disclosure - Choose an item.
		Level 4 Very Sensitive	1. Security Background Check - Choose an item. 2. Segregation of Duties - Choose an item. 3. Security Awareness Training - Choose an item. 4. Security Clearance - Choose an item. 5. Ethics Signoff - Choose an item. 6. Conflict of Interest Disclosure - Choose an item.
		Level 5 Most Sensitive	1. Security Background Check - Choose an item. 2. Segregation of Duties - Choose an item. 3. Security Awareness Training - Choose an item. 4. Security Clearance - Choose an item. 5. Ethics Signoff - Choose an item. 6. Conflict of Interest Disclosure - Choose an item.
	Detective	Level 1 Least Sensitive	1. Accrued Vacation Report – Choose an item. 2. Internet Usage Report – Choose an item. 3. SIEM Access Logs – Choose an item. 4. Physical Access Logs - Choose an item.
		Level 2 Sensitive	1. Accrued Vacation Report – Choose an item. 2. Internet Usage Report – Choose an item. 3. SIEM Access Logs – Choose an item. 4. Physical Access Logs - Choose an item.

		Level 3 Semi-Sensitive	1. Accrued Vacation Report – Choose an item. 2. Internet Usage Report – Choose an item. 3. SIEM Access Logs – Choose an item. 4. Physical Access Logs - Choose an item.
		Level 4 Very Sensitive	1. Accrued Vacation Report – Choose an item. 2. Internet Usage Report – Choose an item. 3. SIEM Access Logs – Choose an item. 4. Physical Access Logs - Choose an item.
		Level 5 Most Sensitive	1. Accrued Vacation Report – Choose an item. 2. Internet Usage Report – Choose an item. 3. SIEM Access Logs – Choose an item. 4. Physical Access Logs - Choose an item.
	Responsive	Level 1 Least Sensitive	1. Execute Response Plan: Level 1
		Level 2 Sensitive	1. Execute Response Plan: Level 1
		Level 3 Semi-Sensitive	1. Execute Response Plan: Level 2
		Level 4 Very Sensitive	1. Execute Response Plan: Level 2
		Level 5 Most Sensitive	1. Execute Response Plan: Level 3

Layer	Aspect	Class. / Risk	Security Treatment
Governance / Compliance	Predictive		1. Perform a risk assessment specific to IT Security Governance where possible to quantify the level of risk associated with IT Security Governance. 2. Perform a risk assessment specific to applicable compliance requirements where possible to quantify the level of risk associated with the various compliance requirements. 3. Research current Governance and Compliance trend information.
	Preventive Detective Responsive	Level 1 Least Sensitive	1. Occasionally monitor compliance/governance item for changes that would increase its risk to the organization in the near future.
		Level 2 Sensitive	1. Regularly monitor compliance/governance item for changes that would increase its risk to the organization in the near future.
		Level 3 Semi-Sensitive	1. Assess the compliance/governance item. 2. Perform a gap analysis and devise a plan to move to a compliance position.
		Level 4 Very Sensitive	1. Target highest risk compliance items with the immediate implementation of temporary compliance controls while assessing the compliance/governance item. 2. Perform a gap analysis and devise a plan to move to a more permanent compliance position.
		Level 5 Most Sensitive	1. Notify CIO and appropriate executive of event. 2. Target highest risk compliance items with the immediate implementation of temporary compliance controls while assessing the compliance/governance item. 3. Perform a gap analysis and devise a plan to move to a more permanent compliance position.

Conclusion

Information Security is a complex component for all organizations that leverage technology to assist in achieving their strategic objectives. Too often, Information Security is relegated to people with IT experience, but little security background. The purpose of this white paper is to put forward a practical approach for Information Security that is foundationally built on risk in order to provide some structure for Information Security groups to determine the appropriate security treatments for the data utilized by their organizations regardless if it is in house, with a trusted partner or moving out to the cloud. To help achieve this, the following components are required:

1. **An Information Security Charter** – giving authority to the CISO to set and enforce standards
2. **A Data Classification Scheme** – that allows for the classification of the information within the organization with an increasing sensitivity
3. **The Layers and Aspects Model** – allowing for deep defense with respect to the organizations information
4. **Security Treatment Matrix** – which outlines the various potential security treatments that can be applied based on the classification of the data involved (or risk to the organization).

As previously noted, this approach provides the essential building blocks to achieve an inclusive information security architecture; however, it should be expected (and it is encouraged) that various aspects within the framework be adjusted to fit the unique characteristics of the organization within which it is being applied. Whether the organization has three data classifications, or six data classifications is not the issue; it is that the organization HAS data classifications that are utilized to identify appropriate security treatments for their data.

By utilizing this model it is possible to more accurately identify the treatments required to protect data based on the importance of the data to the organization. After all, the protection of the organizations data is what information security is tasked to do.