Calibrated Risk Index

Version .10

ASSURA INC
7814 Carousel Lane
Suite 202
Richmond, VA 23294
USA
Phone: 804-672-8714
Fax: 804-672-6442
www.assurainc.com

Version Log

Version	Date	Description
1.0	XXX	First version of document.

Table of Contents

1.0 INTRODUCTION

This document describes Calibrated Risk Index™ (CRI), Assura, Inc's (Assura) proprietary methodology for measuring and reporting Information Technology security (IT Security) risks. CRI is a modified version of the Risk Assessment process published in National Institute of Standards and Technology (NIST) Special Publication 800-30 using proprietary calculations to determine both the quantitative and qualitative effects of a given risk in a single, consolidated rating. CRI also makes use of the security controls catalog published in NIST Special Publication 800-53. As a result of using these two Federal guidelines, CRI is equally applicable to the public and private sectors, and ensures compliance with Federal, State, and Industry IT Security standards.

CRI was developed with the philosophy that not all risks have identical consequences to all organizations. The "calibration" component of CRI is working with an organization to characterize their threat environment and the impacts to their business of those threats coming to fruition in a way that is quantifiable.

The intent of this Risk Management Methodology is to provide a defined, repeatable process for the identification, assessment, and management of risks to information. It also provides a normalized classification and rating system to ensure that all parts of the organization responsible for Governance, Risk, and Compliance (GRC) have consistent information from which to make risk decisions.

2.0 CALIBRATED RISK INDEX

The steps employed to measure risks using CRI are based on the process defined in NIST Special Publication 800-30. While the sequence of the steps does not align one-for-one to Special Publication 800-30, the data points necessary for risk calculation are identical.

Figure 1: Evaluation and Reporting Process

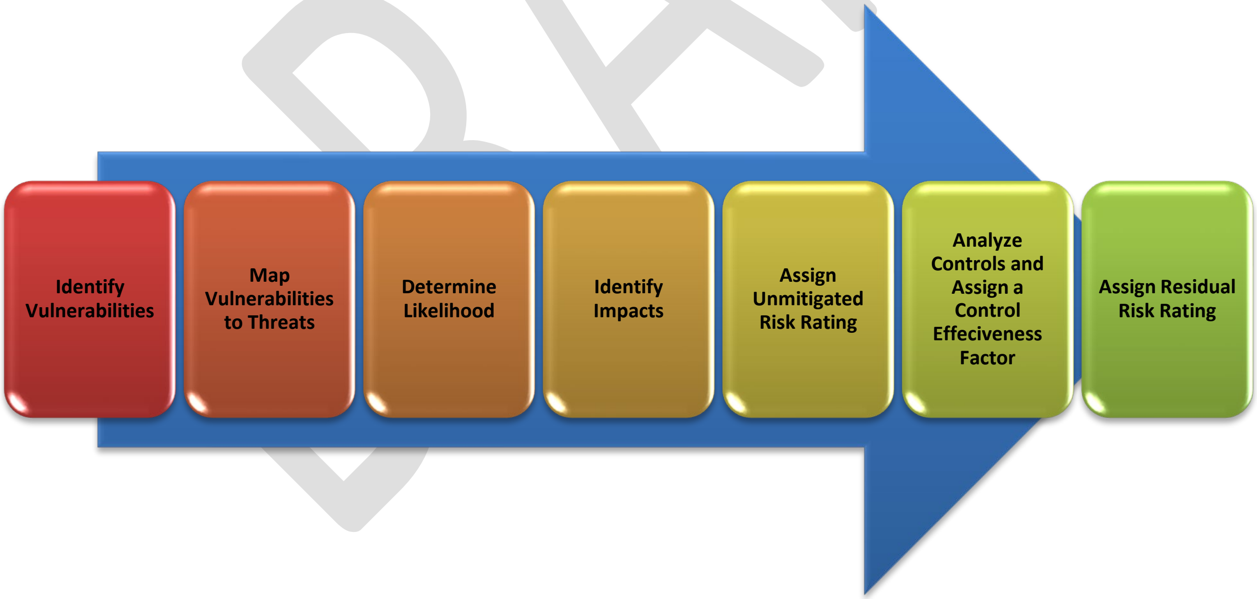
Identify Vulnerabilities
Map Vulnerabilities to Threats
Determine Likelihood
Identify Impacts
Assign Unmitigated Risk Rating
Analyze Controls and Assign a Control Effeciveness Factor
Assign Residual Risk Rating

Figure 1 shows the sequence of the inputs used to derive a risk rating using CRI.

CRI uses a series of computations of the geometric mean of threats, vulnerabilities, and impacts as well as multipliers to determine both the likelihood of a given risk coming to fruition and the effectiveness of in place controls to mitigate that risk. The reason for such heavy reliance on geometric mean (i.e., geometric average) rather than arithmetic mean (i.e., simple average) is twofold:

1. Changes to threats, vulnerabilities, and impacts have a geometric (i.e., non-linear) effect on risk. An arithmetic mean does not adequately capture the scale or consequence of changes in each variable.
2. It recognizes the phenomenon of regression to the mean so that risks are not understated or overstated. This helps to prevent organizations from artificially minimizing risks that would otherwise require urgent management attention or, conversely, focusing on “black swan” events (i.e., highly improbable events with enormous impact). Either could result in flawed risk management decisions, which in turn could have far reaching financial and legal consequences.

Step 1: Identify Threats is where *credible* threats to systems and data are identified. A hostile threat consists of adversaries[1] who have both the capability and the intent to initiate an attack on a system. Consideration of the “threat” can also include natural threats such as severe weather events. The emphasis placed on these two aspects of the threat depends on the specific operating environment and the nature of the operation. In some situations, natural threats play a key role in determining the overall threat, whereas in others, a hostile man-made threat represents the major concern. The severity scores that follow pertain to both hostile and natural threats. Note: hostile adversaries can be internal as well as external and may be non-state-sponsored as well as foreign governmental entities.

Threat identification can be performed by:

- Analyzing historical records;
- Examining public sources of information;
- Conducting interviews with key personnel about current and past threats;
- Applying industry standard threat matrices.

For each threat identified, a severity score is assigned. The severity scores are:

1 – LOW: There are no known dedicated adversaries with both the capability and motivation to carry out a specific threat against the organization's resources or mission; and the introduction of such adversaries is not highly likely within the timeframe of interest.

2 – MEDIUM: Some adversaries exist who possess the capability and motivation to target the assessed organization. No specific targeting information has surfaced.

3 – HIGH: The existence of adversaries having both capability and motivation is extremely likely, as well as the intent to specifically target the assessed organization.

4 – CRITICAL: Dedicated adversaries with demonstrated capability and motivation exist, and there is evidence that they intend to specifically target the assessed organization.

These tables are populated based on discussions with the organization and must within the context of the agency’s threat environment.

Tables 1 and 2 are samples matrices in descending order of severity of environmental and man-made threats along with example scores. Note that these will vary from organization to organization.

Table 1: Sample Environmental Threat Matrix

Environmental	Rating
Tornado	3
Wind	3
Air Conditioning Failure	2
Blizzard/Snowfall	2
Chemical Spills	2
Communication Failure	2
Electromagnetic Interference	2
Flooding/Water Damage	2
Hurricane	2

[1] Use of the word “adversaries” in this instance denotes both natural and man-made.

Environmental	Rating
Lightning	2
Pandemic	2
Power Loss	2
Fire	2
Power fluctuations	2
Biological Contamination	1
Earthquake	1
Hardware Failure	1
Nuclear Accidents	1
Structural failure due to construction defect/weakness	1

Table 2: Sample Manmade Threat Matrix

Man-made	Rating
Botnets	3
Data Theft	3
Fraud (billing)	3
Human Error	3
Identity Theft	3
Industrial Espionage/competitive intelligence	3
Loss of Key Personnel	3
Malicious Code/Malware (including spyware and adware)	3
Malicious Use	3
Software defects	3
Unauthorized Access or Use	3
Computer Crime	2
Equipment Theft	2
Labor Strife	2
Sabotage	2
Workplace Violence	2
Aircraft Accident	1
Blackmail	1
Bomb Threats and incidents	1
Cyber-Terrorism	1
Embezzlement	1
Terrorism	1
Vandalism and/or Rioting	1

When a risk involves multiple threats, the geometric mean of the threats is used in the risk calculation, i.e.:

$$Threat = \sqrt[y]{Threat_1 \times Threat_2 \times Threat_n}$$

The variable y in this equation represents the number of threats calculated to derive the threat score.

Step 2: Determine Likelihood is the step where we identify the probability that a given threat will exploit a corresponding vulnerability based on a combination of historical data, current intelligence information, and, in the case of man-made threats, the means (i.e., resources, money, etc.) and motivation. Likelihood is a weighting factor assigned to each threat within the context of the agency's business. The weighting factor definitions for likelihood are:

> **.25 – LOW:** Events that are likely to occur every twenty-five (25) or more calendar months. No known attacks exist.

.5 – MEDIUM: Events that are likely to occur every thirteen (13) to twenty-four (24) calendar months. An attack exists but is not known to have been employed by a threat at the time of the assessment.

.75 – HIGH: Events that are likely to occur every two (2) to twelve (12) calendar months. Attacks known to be available and used but no known events have occurred to the organization.

1 – CRITICAL: Likely to occur at least once per month. Attacks known to be available and used and events have occurred to the organization.

Step 3: Identify Vulnerabilities. Vulnerabilities are security weaknesses that represent avenues by which an adversary can implement a threat. In order to be of significance, vulnerabilities must be observable or identifiable by an adversary and must be exploitable by an adversary. Vulnerabilities are mitigated by the application of controls (also known as “countermeasures”) which may be in the form of policies, procedures, tactics, hardware, software, etc.

Vulnerabilities may be identified through:

1. Interviews with key personnel and experts.
2. Utilization of tools to identify technical weaknesses such as:
    a. Fortify
    b. Nessus
    c. Trust Keeper
    d. Metasploit
3. Conducting both technical and social engineering penetration tests of systems using the methodologies employed by Certified Ethical Hackers, Licensed Penetration Testers, and PCI Security Standards Council Approved Scanning Vendors.
4. Manual auditing, analysis, inspection, and observation of processes and systems/system configurations.

All vulnerabilities fall into one or more classes: Management, Operational, or Technical. The class of each vulnerability must be identified in the Risk Assessment report.

Vulnerability scores are:

1 – LOW: A small number of weaknesses may exist, but they are not easily identifiable or exploited without a significant degree of effort and the use of tactics which could easily be detected or thwarted by existing security measures.

2 – MEDIUM: Some weaknesses exist which may or may not be observable, but which can be exploited by a credible adversary with some degree of dedicated effort.

3 – HIGH: Highly significant and obvious weaknesses exist that could be exploited by a credible adversary without significant degree of effort.

4 – CRITICAL: Severe and/or numerous weaknesses exist which can easily be identified and exploited.

In general, technical vulnerabilities that are the result of software flaws from widely known vendors such as Microsoft[2], Cisco, Oracle, and others are registered in the National Vulnerabilities Database (NVD) located at http://web.nvd.nist.gov. Each of these vulnerabilities is assigned a severity score using the Common Vulnerability Scoring System (CVSS). CVSS scores vulnerabilities on a scale of zero (0) to ten (10). The CVSS score maps directly to one of the vulnerability scores listed above as illustrated in Table 3 below.

[2] Although Microsoft has its own well-known Severity Rating System that can be found at http://technet.microsoft.com/en-us/security/bulletin/rating, each vulnerability published by Microsoft is also analyzed and assigned a CVSS score in the NVD.

Table 3: Mapping of CVSS Scores to Calibrated Risk Index Vulnerability Scores

Low (1)	Moderate (2)	High (3)	Critical (4)
0-3.99	4-6.99	7-8.99	9-10

Analysis of system vulnerabilities against databases of well-known weaknesses is also mandatory. The Common Weaknesses Enumeration Specification (CWE) – found at http://cwe.mitre.org - provides information about common vulnerabilities due to misconfiguration or coding method that introduces a vulnerability to a system or application. CWE incorporates weaknesses from other frameworks such as the Open Web Application Security Project (OWASP), which can be found at http://www.owasp.org.

Step 4: Identify Impacts is the step where we derive a projection of what the effect of a threat exploiting a vulnerability to an organization *might be,* given current best knowledge. This is also the second calibration conducted with the organization for which the Risk Assessment is being conducted. For instance, a financial impact of $250,000 may be critical to a small organization, while it may constitute a simple annoyance to a large, multinational corporation or government entity.

Impact scores are computed by calculating the impact scores for each of the three fundamental tenants of information security: confidentiality, integrity, and availability (i.e., the CIA Triad). Those scores are then computed together to form a single overall impact score.

Impacts are assessed using the six dimensions of consequences of a data compromise to *confidentiality* and *integrity* assigned in the agency's Data Classification analysis: Legal, Financial, Service Delivery, Brand/Public Trust, Labor, and Safety. Impact scores for *availability* are derived from the system's Recovery Time Objective (RTO) as determined in the agency's BIA.

The following are baseline impact category definitions and scores for **confidentiality** and **integrity**. These should be discussed with the organization prior to conducting the Risk Assessment.

Legal – Identifies the legal, regulatory or contractual impacts and the penalties based upon the following parameters:

0 – None: No impact.

1 – LOW: Infraction or minor legal actions include a writ of mandamus or injunction.

2 – MODERATE: Misdemeanor irrespective of degree or class.

3 – HIGH: Data breach that affects 1,000 or fewer individuals. Felony of second degree or higher. Breach of contract, Memorandum of Understanding, Memorandum of Agreement, or Grant subject to legal sanctions.

4 – CRITICAL: Data breach that affects 1,000 or more individuals. First-degree felony. Breach of contract, Memorandum of Understanding, Memorandum of Agreement, or Grant that subjects the organization to government oversight such as a Consent Decree, Consent Agreement, or receivership.

Financial – Identifies financial losses (e.g., lost revenue, lost property, property damage, insurance deductibles, etc.) based upon the following parameters:

0 – None: No impact.

1 – LOW: $5,000 or less.

2 – MODERATE: $5,001 – $100,000.

3 – HIGH: $100,001 – $250,000.

4 – CRITICAL: Greater than $250,000.

Service Delivery – Identifies the impacts to services based upon the following parameters:

0 – None: No impact.

1 – LOW: Little to no effect on stakeholders.

2 – MODERATE: Delay of services to stakeholders with no downstream effect to those stakeholders.

3 – HIGH: Late delivery of services to stakeholders that causes downstream effects to those stakeholders.

4 – CRITICAL: Failure to deliver services to stakeholders.

Brand and Public Trust – Identifies any impact to the brand/market perception/image based upon the following parameters:

0 – None: No impact.

1 – LOW: Negative media reports or other publicity (e.g., Internet) with no further action required.

2 – MODERATE: Negative media reports or other publicity (e.g., Internet) that prompt a press release or other official statement.

3 – HIGH: Negative media reports or other publicity (e.g., Internet) that prompt angry letters from 1,000 or fewer individuals or notification from a government agency.

4 – CRITICAL: Negative media reports or other publicity (e.g., Internet) that prompt angry letters from 1,000 or more people, public outcry and/or legislative scrutiny.

Labor – Identifies labor impacts based upon the following parameters:

0 – None: No impact.

1 – LOW: Could cause some individual hardship, attrition, and/or productivity loss (0 – 10%).

2 – MODERATE: Moderate for over ten percent (10%) to twenty percent (20%) absenteeism, productivity loss, and/or attrition.

3 – HIGH: High for over twenty percent (20%) to fifty percent (50%) absenteeism, productivity loss, and/or attrition.

4 – CRITICAL: Over fifty percent (50%) absenteeism, productivity loss, and/or attrition; or an illegal strike action.

Safety – Identifies whether a risk could result in personal injury or death. These impacts are given a rating based upon the following parameters:

0 – None: No impact.

1 – LOW: The possibility of personal injury treatable with rudimentary first aid. Examples include minor cuts and abrasions, bruising, etc.

2 – MODERATE: The possibility of personal injury requiring medical treatment but no permanent effects. Examples include severe cuts, broken bones, contusions, mild concussions, internal soft tissue damage, sprains, etc.

3 – HIGH: The possibility of personal injury resulting in long-term disability. Examples include amputation, brain injury, internal organ damage, post-traumatic stress disorder, etc.

4 – CRITICAL: The possibility of the death of a person.

The impact scores for **availability** are as follows:

1 – LOW: RTO of >7 Days

2 – MODERATE: RTO of >3 Days to 7 Days

3 – HIGH: RTO of >1 Day – 3 Days

4 – CRITICAL: RTO of <= 1 Day

To compute the impact score, solve the following equations:

1. Compute Confidentiality Impact (inputs from Data Classification):

$$Confidentiality\ Impact\ = \sqrt[6]{Legal \times Financial \times Service\ Delivery \times Brand \times Labor \times Safety}$$

   If any impact category is rated zero (0) – no impact, then .01 is substituted as the input for in the calculation.

2. Compute Integrity Impact (inputs from Data Classification):

$$Integrity\ Impact\ = \sqrt[6]{Legal \times Financial \times Service\ Delivery \times Brand \times Labor \times Safety}$$

   If any impact category is rated zero (0), then .01 is substituted as the input for in the calculation.

3. Compute Availability Impact (input from Business Impact Analysis):

$$Availability\ Impact\ = [Low, Moderate, High, Critical]$$

4. Compute the overall impact score:

$$Overall\ Impact = \sqrt[3]{Confidentiality\ Impact \times Integrity\ Impact \times Availability\ Impact}$$

Step 5: Assign Unmitigated Risk Rating, which is the calculation of:

$$Unmitigated\ Risk = \sqrt[3]{(Threat \times Likelihood) \times Vulnerability \times Impact}$$

This calculation derives the geometric mean of the unmitigated risk (i.e., risk without factoring compensating controls/countermeasures).

Step 6: Assign a Control Effectiveness Factor is a calculation that describes the effect that in-place controls (also known as "countermeasures" or "compensating controls") have on an unmitigated risk. This calculation is made by identifying controls from a Control Catalog and assigning a Control Effectiveness Rating (CER) assigned to that control. Each control in the catalog is assigned a CER, which ranges from one (1) to four (4) as follows:

1 – CRITICAL: Highly effective and known to prevent, detect, or correct threats from exploiting vulnerabilities.

2 – HIGH: Mostly effective and known to prevent, detect, or correct most (but not all) threats from exploiting vulnerabilities.

3 – MODERATE: Somewhat effective and known to prevent, detect, or correct some threats from exploiting vulnerabilities.

4 – LOW: Usually ineffective and in general does not prevent, detect, or correct a threat from exploiting vulnerabilities.

The Control Catalog is derived from the Security Control Catalog (Appendix F) of National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 3 (August 2009). All controls have a unique *identifier* and are grouped into a *family* and *class*. Each control is grouped into one of seventeen *families*. These are described in NIST Special Publication 800-53 thusly:

> *"Each security control family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each security control family. In addition, there are three general classes of security controls: management, operational, and technical."*

Table 4 summarizes the classes and families in the security control catalog and the associated security control family identifiers.

Table 4: Security Control Classes, Families, and Identifiers

Identifier	Family	Class
AC	Access Control	Technical

AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

Each CER is run through a computation to derive an overall **Control Effectiveness Factor (CEF)**. The CEF is a multiplier applied in Step 8 that determines how much a given risk is mitigated. CEF is computed by calculating the geometric mean of the CERs in aggregate. This is expressed by the equation:

$$CEF = \sqrt[y]{CER_1 \times CER_2 \times CER_N}$$

The variable y in this equation represents the number of in-place controls analyzed from the Control Catalog.

Many controls have enhancements that are required depending on the classification of the system. The conglomeration of those enhancements for a system classification forms a **control baseline**. System classifications will vary from organization to organization. However, CRI uses the classification ratings derived from the data and system classification analysis usually conducted prior to a CRI-based Risk Assessment. That classification system calls for three tiers of classification called for in Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* published by NIST. These three tiers are: Low Impact, Moderate Impact, and High Impact.

Some organizations use a binary classification system (e.g., Non-Sensitive and Sensitive). In those cases, the Low Impact control baseline is applied for Non-Sensitive systems and the High Impact control baseline is used for Sensitive systems.

Table 5 provides a listing of all of the controls in the NIST Special Publication 800-53 control Catalog, along with the CER and the control baseline for each classification of system. A number in parenthesis identifies control enhancements after the Control Number. Note that a control only receives the CER specified if <u>all</u> of the control enhancements (if specified) are in place in accordance with the control baseline. The CEF is calculated by an aggregation algorithm that factors all recommended controls that **should** be in place to address the risk, along with the controls that are **actually** in place. If not all aspects of a control (or their required enhancements) are in place, then the control is not in place and the control receives a CER of 4.

Table 5: Control Baselines and Control Effectiveness Ratings

CNTL NO.	CONTROL NAME	CER	CONTROL BASELINES		
			Low Impact	Moderate impact	High Impact
Access Control (AC)					
AC-1	Access Control Policy and Procedures	3	AC-1	AC-1	AC-1
AC-2	Account Management	2	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	2	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	1	Not Selected	AC-4	AC-4

CNTL NO.	CONTROL NAME	CER	CONTROL BASELINES		
			Low Impact	Moderate impact	High Impact
AC-5	Separation of Duties	2	Not Selected	AC-5	AC-5
AC-6	Least Privilege	2	Not Selected	AC-6 (1) (2)	AC-6 (1) (2)
AC-7	Unsuccessful Login Attempts	3	AC-7	AC-7	AC-7
AC-8	System Use Notification	4	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	3	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	4	Not Selected	Not Selected	AC-10
AC-11	Session Lock	2	Not Selected	AC-11	AC-11
AC-12	Session Termination (Withdrawn)	N/A	---	---	---
AC-13	Supervision and Review—Access Control (Withdrawn)	N/A	---	---	---
AC-14	Permitted Actions without Identification or Authentication	4	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking (Withdrawn)	N/A	---	---	---
AC-16	Security Attributes	1	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	2	AC-17	AC-17 (1) (2) (3) (4) (5) (7) (8)	AC-17 (1) (2) (3) (4) (5) (7) (8)
AC-18	Wireless Access	2	AC-18	AC-18 (1)	AC-18 (1) (2) (4) (5)
AC-19	Access Control for Mobile Devices	1	AC-19	AC-19 (1) (2) (3)	AC-19 (1) (2) (3)
AC-20	Use of External Information Systems	3	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	User-Based Collaboration and Information Sharing	3	Not Selected	Not Selected	Not Selected
AC-22	Publicly Accessible Content	2	AC-22	AC-22	AC-22
Awareness and Training (AT)					
AT-1	Security Awareness and Training Policy and Procedures	4	AT-1	AT-1	AT-1
AT-2	Security Awareness	2	AT-2	AT-2	AT-2
AT-3	Security Training	2	AT-3	AT-3	AT-3
AT-4	Security Training Records	4	AT-4	AT-4	AT-4
AT-5	Contacts with Security Groups and Associations	4	Not Selected	Not Selected	Not Selected
Audit and Accountability (AU)					
AU-1	Audit and Accountability Policy and Procedures	4	AU-1	AU-1	AU-1
AU-2	Auditable Events	4	AU-2	AU-2 (3) (4)	AU-2 (3) (4)
AU-3	Content of Audit Records	3	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	3	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	3	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	2	AU-6	AU-6	AU-6 (1)
AU-7	Audit Reduction and Report Generation	2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	3	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	2	AU-9	AU-9	AU-9
AU-10	Non-repudiation	1	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	2	AU-11	AU-11	AU-11
AU-12	Audit Generation	1	AU-12	AU-12	AU-12 (1)
AU-13	Monitoring for Information Disclosure	3	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	1	Not Selected	Not Selected	Not Selected
Security Assessment and Authorization (CA)					
CA-1	Security Assessment and Authorization Policies and Procedures	3	CA-1	CA-1	CA-1
CA-2	Security Assessments	2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	Information System Connections	2	CA-3	CA-3	CA-3
CA-4	Security Certification (Withdrawn)	N/A	---	---	---

CNTL NO.	CONTROL NAME	CER	CONTROL BASELINES		
			Low Impact	Moderate impact	High Impact
CA-5	Plan of Action and Milestones	3	CA-5	CA-5	CA-5
CA-6	Security Authorization	3	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	2	CA-7	CA-7	CA-7
Configuration Management (CM)					
CM-1	Configuration Management Policy and Procedures	3	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	2	CM-2	CM-2 (1) (3) (4)	CM-2 (1) (2) (3) (5) (6)
CM-3	Configuration Change Control	1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	2	Not Selected	CM-5	CM-5 (1) (2) (3)
CM-6	Configuration Settings	2	CM-6	CM-6 (3)	CM-6 (1) (2) (3)
CM-7	Least Functionality	2	CM-7	CM-7 (1)	CM-7 (1) (2)
CM-8	Information System Component Inventory	2	CM-8	CM-8 (1) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	2	Not Selected	CM-9	CM-9
Contingency Planning (CP)					
CP-1	Contingency Planning Policy and Procedures	4	CP-1	CP-1	CP-1
CP-2	Contingency Plan	2	CP-2	CP-2 (1)	CP-2 (1) (2) (3)
CP-3	Contingency Training	2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercises	1	CP-4	CP-4 (1)	CP-4 (1) (2) (4)
CP-5	Contingency Plan Update (Withdrawn)	N/A	---	---	---
CP-6	Alternate Storage Site	3	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	3	Not Selected	CP-7 (1) (2) (3) (5)	CP-7 (1) (2) (3) (4) (5)
CP-8	Telecommunications Services	3	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	1	CP-9	CP-9 (1)	CP-9 (1) (2) (3)
CP-10	Information System Recovery and Reconstitution	1	CP-10	CP-10 (2) (3)	CP-10 (2) (3) (4)
Identification and Authentication (IA)					
IA-1	Identification and Authentication Policy and Procedures	4	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	1	IA-2 (1)	IA-2 (1) (2) (3) (8)	IA-2 (1) (2) (3) (4) (8) (9)
IA-3	Device Identification and Authentication	2	Not Selected	IA-3	IA-3
IA-4	Identifier Management	1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	1	IA-5 (1)	IA-5 (1) (2) (3)	IA-5 (1) (2) (3)
IA-6	Authenticator Feedback	3	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	1	IA-8	IA-8	IA-8
Incident Response (IR)					
IR-1	Incident Response Policy and Procedures	4	IR-1	IR-1	IR-1
IR-2	Incident Response Training	2	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing and Exercises	4	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	1	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	4	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	2	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	3	IR-7	IR-7 (1)	IR-7 (1)

CNTL NO.	CONTROL NAME	CER	CONTROL BASELINES		
			Low Impact	Moderate impact	High Impact
IR-8	Incident Response Plan	2	IR-8	IR-8	IR-8
Maintenance (MA)					
MA-1	System Maintenance Policy and Procedures	4	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	2	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	2	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Non-Local Maintenance	2	MA-4	MA-4 (1) (2)	MA-4 (1) (2) (3)
MA-5	Maintenance Personnel	2	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	2	Not Selected	MA-6	MA-6
Media Protection (MP)					
MP-1	Media Protection Policy and Procedures	4	MP-1	MP-1	MP-1
MP-2	Media Access	2	MP-2	MP-2 (1)	MP-2 (1)
MP-3	Media Marking	3	Not Selected	MP-3	MP-3
MP-4	Media Storage	1	Not Selected	MP-4	MP-4
MP-5	Media Transport	1	Not Selected	MP-5 (2) (4)	MP-5 (2) (3) (4)
MP-6	Media Sanitization	1	MP-6	MP-6	MP-6 (1) (2) (3)
Physical and Environmental Protection (PE)					
PE-1	Physical and Environmental Protection Policy and Procedures	4	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	2	PE-2	PE-2	PE-2
PE-3	Physical Access Control	1	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	3	Not Selected	PE-4	PE-4
PE-5	Access Control for Output Devices	4	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	3	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	Visitor Control	2	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Records	3	PE-8	PE-8	PE-8 (1) (2)
PE-9	Power Equipment and Power Cabling	3	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	4	Not Selected	PE-10	PE-10
PE-11	Emergency Power	1	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	4	PE-12	PE-12	PE-12
PE-13	Fire Protection	2	PE-13	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	3	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	2	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	2	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	2	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	3	Not Selected	PE-18	PE-18 (1)
PE-19	Information Leakage	2	Not Selected	Not Selected	Not Selected
Planning (PL)					
PL-1	Security Planning Policy and Procedures	4	PL-1	PL-1	PL-1
PL-2	System Security Plan	3	PL-2	PL-2	PL-2
PL-3	System Security Plan Update (Withdrawn)	N/A	---	---	---
PL-4	Rules of Behavior	3	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	4	PL-5	PL-5	PL-5
PL-6	Security-Related Activity Planning	4	Not Selected	PL-6	PL-6
Personnel Security (PS)					
PS-1	Personnel Security Policy and Procedures	4	PS-1	PS-1	PS-1

CNTL NO.	CONTROL NAME	CER	CONTROL BASELINES		
			Low Impact	Moderate impact	High Impact
PS-2	Position Categorization	4	PS-2	PS-2	PS-2
PS-3	Personnel Screening	3	PS-3	PS-3	PS-3
PS-4	Personnel Termination	1	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	2	PS-5	PS-5	PS-5
PS-6	Access Agreements	3	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	2	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	1	PS-8	PS-8	PS-8
Risk Assessment (RA)					
RA-1	Risk Assessment Policy and Procedures	4	RA-1	RA-1	RA-1
RA-2	Security Categorization	4	RA-2	RA-2	RA-2
RA-3	Risk Assessment	4	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update (Withdrawn)	N/A	---	---	---
RA-5	Vulnerability Scanning	1	RA-5	RA-5 (1)	RA-5 (1) (2) (3) (4) (5) (7)
System and Services Acquisition (SA)					
SA-1	System and Services Acquisition Policy and Procedures	4	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	4	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	2	SA-3	SA-3	SA-3
SA-4	Acquisitions	3	SA-4	SA-4 (1) (4)	SA-4 (1) (2) (4)
SA-5	Information System Documentation	2	SA-5	SA-5 (1) (3)	SA-5 (1) (2) (3)
SA-6	Software Usage Restrictions	3	SA-6	SA-6	SA-6
SA-7	User-Installed Software	2	SA-7	SA-7	SA-7
SA-8	Security Engineering Principles	2	Not Selected	SA-8	SA-8
SA-9	External Information System Services	2	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	2	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing	2	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	2	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	3	Not Selected	Not Selected	SA-13
SA-14	Critical Information System Components	2	Not Selected	Not Selected	Not Selected
System and Communications Protection (SC)					
SC-1	System and Communications Protection Policy and Procedures	4	SC-1	SC-1	SC-1
SC-2	Application Partitioning	2	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	2	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	1	SC-5	SC-5	SC-5
SC-6	Resource Priority	1	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	1	SC-7	SC-7 (1) (2) (3) (4) (5) (7)	SC-7 (1) (2) (3) (4) (5) (6) (7) (8)
SC-8	Transmission Integrity	1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	Transmission Confidentiality	1	Not Selected	SC-9 (1)	SC-9 (1)
SC-10	Network Disconnect	3	Not Selected	SC-10	SC-10
SC-11	Trusted Path	1	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	2	SC-12	SC-12	SC-12 (1)
SC-13	Use of Cryptography	1	SC-13	SC-13	SC-13
SC-14	Public Access Protections	1	SC-14	SC-14	SC-14
SC-15	Collaborative Computing Devices	2	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	2	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	1	Not Selected	SC-17	SC-17

CNTL NO.	CONTROL NAME	CER	CONTROL BASELINES		
			Low Impact	Moderate impact	High Impact
SC-18	Mobile Code	1	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	3	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	1	SC-20 (1)	SC-20 (1)	SC-20 (1)
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	1	Not Selected	Not Selected	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	2	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	2	Not Selected	Not Selected	SC-24
SC-25	Thin Nodes	2	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	3	Not Selected	Not Selected	Not Selected
SC-27	Operating System-Independent Applications	4	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	1	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	2	Not Selected	Not Selected	Not Selected
SC-30	Virtualization Techniques	3	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	3	Not Selected	Not Selected	Not Selected
SC-32	Information System Partitioning	1	Not Selected	SC-32	SC-32
SC-33	Transmission Preparation Integrity	3	Not Selected	Not Selected	Not Selected
SC-34	Non-Modifiable Executable Programs	2	Not Selected	Not Selected	Not Selected
System and Information Integrity (SI)					
SI-1	System and Information Integrity Policy and Procedures	4	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	2	SI-3	SI-3 (1) (2) (3)	SI-3 (1) (2) (3)
SI-4	Information System Monitoring	1	Not Selected	SI-4 (2) (4) (5) (6)	SI-4 (2) (4) (5) (6)
SI-5	Security Alerts, Advisories, and Directives	2	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	2	Not Selected	Not Selected	SI-6
SI-7	Software Information Integrity	1	Not Selected	SI-7(1)	SI-7(1)(2)
SI-8	Spam Protection	1	Not Selected	SI-8	SI-8(1)
SI-9	Information Input Restrictions	2	Not Selected	SI-9	SI-9
SI-10	Information Input Validation	1	Not Selected	SI-10	SI-10
SI-11	Error Handling	2	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	3	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	2	Not Selected	Not Selected	Not Selected
Program Management (PM)					
PM-1	Information Security Program Plan	4	**Deployed organization-wide Supporting all baselines**		
PM-2	Senior Information Security Officer	4			
PM-3	Information Security Resources	4			
PM-4	Plan of Action and Milestones Process	4			
PM-5	Information System Inventory	4			
PM-6	Information Security Measures of Performance	4			
PM-7	Enterprise Architecture	4			
PM-8	Critical Infrastructure Plan	4			
PM-9	Risk Management Strategy	4			
PM-10	Security Authorization Process	4			

CNTL NO.	CONTROL NAME	CER	CONTROL BASELINES		
			Low Impact	Moderate impact	High Impact
PM-11	Mission/Business Process Definition	4			
Other					
OT	Other Control Not in the Control Catalog	*N*[3]		Not Selected	Not Selected

Step 7: Assign Residual Risk Rating is the step where a risk rating is calculated as the product of the unmitigated risk score and the CEF calculated in Step 7. Therefore:

$$Residual\ Risk = Unmitigated\ Risk \times CEF$$

Each risk is then assigned an overall rating of low, medium, high, or critical as illustrated in Table 3.

Table 6: Residual Risk Ratings

Low	Moderate	High	Critical
0-4.99	5-8.99	9-12.99	13-16

3.0 CONCLUSION

Calibrated Risk Index provides a defined, repeatable process for the identification, assessment, and measurement of risks to information systems. Because of its direct tie-in to an organizations BIA and System Sensitivity Analysis, it is able to measure both the quantitative and qualitative effects of risk to the organization. In order to ensure maximum applicability to industry, government, and international standards, CRI leverages U.S. Federal standards and implementation guidance for Information Systems Security. As a result, CRI not only ensures compliance, it provides organizational leadership with the information it needs to make informed Governance, Risk and Compliance decisions.

[3] Assigned by the analyst.