Cadre
information security

Guide to Understanding Your Cadre INFORMAL RISK ASSESSMENT

UNDERSTANDING RISK ASSESSMENTS

A required and critical component of creating polices, choosing standards, formulating plans, mitigating issues and managing all aspects of information security is having a good risk assessment. Informal Risk assessments are included with all Trusted Advisor and vCISO Tiers; however, the type and scope of the Risk Assessment scales with those Tiers. The included Risk Assessment will be a custom instrument reflecting the organization's current state and future objectives. Additional Risk Assessment features and scopes can also be added as optional services at the vCISO discounted rates.

Ideally all aspects of information security relate directly to a risk item in a risk analysis. There is literally no rationale for any control, policy or program to be in place if it does not address an identified risk for an organization.

Cadre Trusted Advisor programs can use your organization's provided Formal Risk Assessment for our work, if you have one. However, we will require time to analyze and process this assessment and then relate it to your SOW. More commonly we will use an Informal Risk Assessment as the first step in beginning work as this allows a quicker more efficient start to the program.

RISK ASSESSMENTS VS. VULNERABILITY ASSESSMENTS

With a variety of assessments available from security consultants, the differences can be confusing. To help you set the proper expectations from your organization, we have outlined the differences between Risk Assessments and Vulnerability Assessments below.

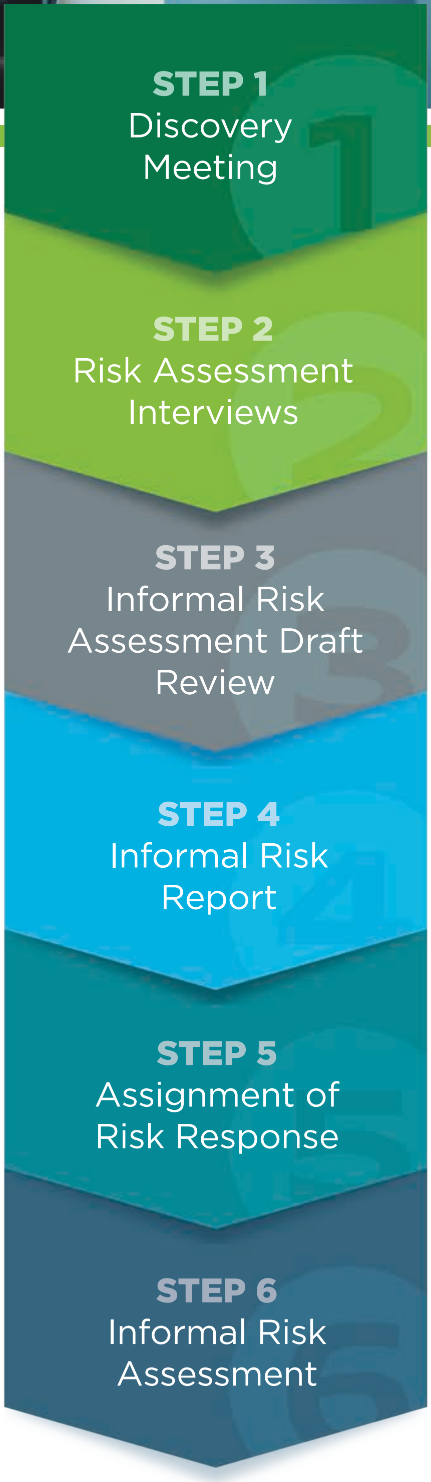
RISK ASSESSMENTS VS. VULNERABILITY ASSESSMENTS

RISK ASSESSMENT

A strategic tool meant to be used by senior level employees including the Board of Directors, C-Level Employees and Directors or other Department or Program heads. It helps guide Policy, Budgets and Objectives, and provides evidence of Due Diligence and Due Care.

VULNERABILITY ASSESSMENT

A tactical tool typically documenting the results of a network or device scan that is used by IS/IT managers. It helps spot configuration issues and can be used to confirm a degree of compliance to frameworks. An executive summary of Vulnerability Assessments is typically given to directors of IT or IS.



STEP 1
Discovery Meeting

STEP 2
Risk Assessment Interviews

STEP 3
Informal Risk Assessment Draft Review

STEP 4
Informal Risk Report

STEP 5
Assignment of Risk Response

STEP 6
Informal Risk Assessment

WHAT TO EXPECT FROM YOUR RISK ASSESSMENT

DISCOVERY MEETING

This is a meeting between your Trusted Advisor Liaison and a few of your origination's employees to determine who would be best suited to interview for the risk analysis.

RISK ASSESSMENT INTERVIEWS

These interviews allow the Trusted Advisor team to learn about your organization's business processes and what risks your organization might have.

INFORMAL RISK ASSESSMENT DRAFT REVIEW

Your Trusted Advisor team will compile the interview information and create a draft of the Risk Assessment. This draft will need to be reviewed to make sure the information from the interviews is accurate. Typically, this review is done with the employees that were in the Discovery Meeting.

INFORMAL RISK REPORT

This is the completed list of risks discovered for your organization.

ASSIGNMENT OF RISK RESPONSE

Using the Informal Risk Report your Trusted Advisor will work with organizational stakeholders of your choosing to determine how the organization will want to respond to the risks. The Trusted Advisor Liaison will lead your team through this process.

INFORMAL RISK ASSESSMENT

Your assessment is now complete. You now have the critical information needed for a wide range of important decisions, policies and programs!

REQUIRED INPUT

To create the Informal Risk Assessment, we will use the following tools:

QUESTIONNAIRE

Cadre may use a brief questionnaire under the direction of your Trusted Advisor Liaison to learn about your organization's stakeholder's key metrics on security goals, risk responsibility, policies, data use, controls, access, business continuity plan components, incident response, and general business model practices.

INTERVIEWS

Cadre will conduct interviews to build the draft Informal Risk Assessment. These interviews may be conducted in person or remotely with the stakeholders of your choosing. Should you need assistance selecting stakeholders, your Trusted Advisor will provide the necessary guidance. Generally, your Trusted Advisor will recommend a sampling of organization stakeholders who can articulate the organization's principal business models, security goals, organizational responsibilities and policies. Additionally, Trusted Advisors typically interview representatives from security, HR and IT.

DOCUMENTATION

Cadre will incorporate any relevant information provided in any past Risk Assessments (formal or informal) or other related assessments, as well as documentation related to the people, processes and technology of security.

DRAFT

The Draft Informal Risk Assessment is reviewed and updated to clarify discovery items for the final document. The review does not require evaluation by all the interviewees so long as the organization feels the document represents a reasonably accurate and complete report.

POSSIBLE OUTPUT

Based on the needs of the organization and scope of the Risk Assessment, there are potential outputs that you can expect:

EVIDENCE OF DUE DILIGENCE

Boards of Directors, senior executives and oversight frameworks often need evidence of Due Diligence and or Due Care to meet policy or regulatory requirements, avoid possible litigation issues, or meet responsibilities codified in organization bylaws.

MATURITY MODELING

Risk Assessments provide most, or even all of the information required to construct a variety of Security Maturity Models. When using an Informal Risk Assessment, it is common to create an Informal Maturity Model, which provides at a minimum:

- Current organizational maturity state
- Cybersecurity objectives (Maturity Model targets)
- Assistance with aligning of security policies, controls and training with business goals and processes
- A dashboard that facilitates production of overview of goals and progress
- An educational tool for understanding the state of the organization in relation to industry standards and practices

GAP ANALYSES

Comparing risks against controls and other mitigations gives you the map needed to find gaps in not only physical controls, but also policies and training.

FIT FOR USE AND FIT FOR PURPOSE CONTROL EVALUATION

Every information security control used by the organization from firewalls to antimalware software should have its existence, scope and cost justified by risk. Fit for Use and Fit for Purpose Control Evaluation ensures you can tie controls back to the risks they mitigate–eliminating any guessing about adequacy, rationale or appropriate costs and responsibilities for those controls.

TEMPLATE FOR EXECUTIVE BRIEFINGS

Executives need to know the risks and mitigations that they are responsible for. A risk-to-mitigation briefing is one of the most efficient ways to document and communicate this information.

OVERALL RATIONALE

In additional to formal outputs, Risk Assessments provide overall rationale for the following:

- Information Security Policy
- Information Security Controls
- Security Awareness Program Design

REVIEW AND REVISIONS

Like most assessments, the relevance and accuracy of findings tends to diminish over time. How frequently Risk Assessments need to be reviewed and revised will depend on many factors both internal and external to the organization. As a general rule of thumb, Risk Assessments need review and revision annually.

Disclaimer:

Please note that Cadre Information Security only provides INFORMAL Risk Assessments unless a specific and separate SOW has been approved and implemented.

Cadre Information Security advises that our customers acquire a FORMAL Risk Assessment that matches the needs of your organization. Typically, this is a program that at minimum meets the NIST 800-30 Guidelines for Conducting Risk Assessments.

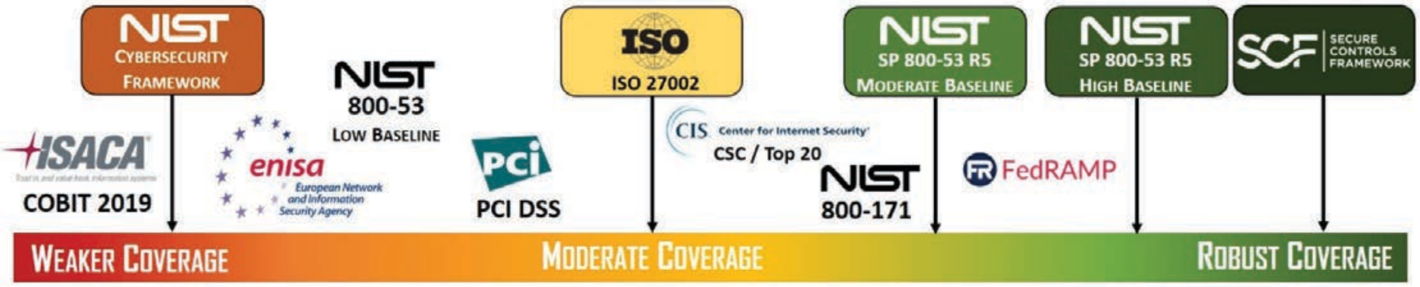

NIST Cybersecurity Framework
NIST 800-53 Low Baseline
ISO ISO 27002
NIST SP 800-53 R5 Moderate Baseline
NIST SP 800-53 R5 High Baseline
SCF Secure Controls Framework
ISACA Trust in, and value from, information systems
COBIT 2019
enisa European Network and Information Security Agency
PCI PCI DSS
CIS Center for Internet Security
CSC / Top 20
NIST 800-171
FR FedRAMP
Weaker Coverage
Moderate Coverage
Robust Coverage

FIGURE 1: SOME EXAMPLES OF POPULAR FORMAL RISK ASSESSMENT FRAMEWORKS