Duty of Care Risk Analysis Standard

Version 1.1

June 2021

Approved for final publication by the DoCRA Council Board of Directors

---

Analyzing Risk
for Reasonable and Appropriate Safeguards

A Publication by The DoCRA Council

www.docra.org/DoCRAv1.1.pdf

Duty of Care Risk Analysis Standard

Version 1.1

Approved for final publication by The DoCRA Council Board of Directors



Analyzing Risk for
Reasonable and Appropriate Safeguards

Commentary by The DoCRA Council

Charter Members
HALOCK Security Labs
Center for Internet Security

www.docra.org
1834 Walden Office Square
Suite 200
Schaumburg, IL 60173

The DoCRA Council

The DoCRA Council is a not-for-profit (501(C)(3)) organization that authors, maintains, and distributes standards and methods for analyzing and managing risk. The DoCRA Council is comprised of member organizations that require standards of practice in risk analysis and risk management, and who therefore have an interest in the methods used for analysing risks and safeguards that reduce risk.

The DoCRA Council operates under a charter (available upon request) that describes its methods of authorship, review, and stewardship of risk analysis standards and methods.

Inquiries about the The DoCRA Council's methods and practices, and inquiries into membership and participation in The DoCRA Council's activities may be made using the following contact information:

Email

info@docra.org

Postal

The DoCRA Council

Inquiries

1834 Walden Office Sq.

Suite 200

Schaumburg, IL 60173

Other Information May Be Found At:

www.docra.org

Comments on this publication may be submitted to:

The DoCRA Council

Suite 200

1834 Walden Office Sq.

Schaumburg, IL 60173

Duty of Care Risk Analysis Standard - Abstract

The Duty of Care Risk Analysis Standard ("DoCRA" or "the Standard") presents principles and practices for analyzing risks so that risk assessors equitably evaluate the interests of all parties potentially affected by risks. DoCRA is designed so it is either the basis of a risk analysis, or an enhancement of other risk analysis methods so they retain their benefits while also addressing duty of care.

Duty of Care Risk Analysis Standard - Introduction

As organizations engage in public life they offer benefits to themselves and others, but they also pose potential harm. Legal authorities and the public hold those organizations accountable for balancing benefit and harm using concepts such as "reasonableness," "duty of care," and "due care." Duty of Care Risk Analysis helps organizations determine whether they apply safeguards that appropriately protect others from harm while presenting a reasonable burden to themselves.

Organizational leaders will find that DoCRA's principles and practices will help them consciously and explicitly minimize the risk of harm to others by using reasonable safeguards. In this way, organizations that use DoCRA explicitly plan positive outcomes for themselves and all interested parties, or all parties who may be harmed by risks. Moreover, organizations that follow DoCRA's principles and practices will be able to articulate risks that involve highly specialized subjects – such cybersecurity, biological sciences, and information science – using non-technical jargon and in terms that address business outcomes.

This Standard describes processes for evaluating risks and their safeguards so that the resulting analysis is supportive of organizations' missions, objectives and obligations, but so that it is also easily communicated to and accepted by authorities - such as regulators and judges - and to other parties who may be harmed by those risks. Regulators expect that the burden of safeguards should be balanced against an organization's mission. Attorneys and judges similarly use balancing tests to determine whether foreseeable harm could have been prevented by safeguards that would pose a reasonable burden. Conventional risk analysis has neglected to include these significant perspectives. DoCRA describes how these perspectives may be included in conventional risk analysis methods.

The DoCRA Standard is designed to process various expressions of risk (e.g. financial amounts, populations, percentages of a whole, matrices populated by plain language, or ordinal values). Because of this, a risk assessor can compare multiple risks that are expressed in various forms that are meaningful to various interested parties. While an organization may evaluate some costs risks in financial terms, the public may be concerned about degrees to which they may be harmed individually or as a population, or degrees of lost benefit that may result from a realized risk. While any such factor may be expressed financially, as is custom in many risk assessments, those factors often lose their meaning after being translated to financial terms. DoCRA allows risks to be expressed in terms that are directly meaningful to each interested party by using "resilience thresholds."

Resilience thresholds are degrees of risk that, when encountered or crossed, become distinctly more or less tolerable to an interested party. For example, a for-profit company that evaluates its financial risk may draw a resilience threshold at a point where they would not be profitable and describe all risks below that point, "acceptable." They may draw another resilience threshold where they would need to change their operations or strategy to recover profitability and describe all risks below that point "unacceptable." They may consider all risks greater than that resilience threshold "catastrophic." If a risk lands between "zero" and the first resilience threshold, then they could

accept such a risk. Moreover, the public may be concerned about risks that are most directly expressed in terms of population, such as the number of individuals who are provided a needed service. That risk may be expressed as a percentage of the total population which is not directly comparable to financial risks. The company could assign resilience thresholds of the same names (“acceptable,” “unacceptable,” and “catastrophic”) to percentages of the population that they believe describe the population’s tolerance for failure to deliver the needed services. In this way, the company can determine whether its risks create an intolerable harm to the public or to themselves. As well, the company could determine whether safeguards that would reduce risks to the public create risk burdens to the company that are greater than the risk itself (that the company would face unacceptable risks using a safeguard that provides an acceptable risk to the public).

Because the Standard is meant to be flexible for a wide variety of cases and risk analysis methods, the Standard provides a set of principles and practices to guide risk assessors, rather than instructions for using DoCRA in its various potential permutations.

Referencing the Duty of Care Risk Analysis Standard

The Duty of Care Risk Analysis Standard may be referenced by other information security standards, methods, instructions, and similar materials, according to the Creative Commons License. Standards and methods that state their conformance to the standard must quote the principles in their entirety and must describe practices that sufficiently support those principles.

Duty of Care Risk Analysis Standard Version 0.6 Draft

1.0 The standard document.

The Standard is designed with the following objectives:

1.1 To provide to the public a risk analysis method that aligns with judicial and regulatory expectations for demonstrating "due care," the "reasonable person," and "reasonable," and "appropriate" safeguards.

1.1.1 As a method for supporting the "cost-benefit" analysis in the United States as required in Executive Order 12866, and as commonly stated in the Code of Federal Regulations as "risk analysis," "reasonable safeguards," "appropriate safeguards," and "reasonable risk."

1.1.2 As a method for supporting judicial analysis such as "multi-factor" balancing tests for determining whether the "reasonable person" standard has been met.

1.1.3 As a method for supporting international standards and regulations for demonstrating "reasonable" risk.

1.2 To supplement and not replace established risk assessment standards and methods. For example, quantitative probabilistic analysis, qualitative use of ordinals, and standards such as ISO/IEC 31000 can all be supplemented and accommodated by DoCRA.

1.3 To describe risk analysis to the extent that risk analysts who are experienced with established risk assessment standards may design, develop, and conduct assessments that achieve DoCRA's principles.

1.4 To describe risk analysis to the extent that other standards bodies may create or enhance their own risk analysis processes so that they achieve the benefits of the Standard.

1.5 To be neutral to specific industries, professional fields, legal forums, and regulatory regimes that require risk analysis. This neutrality is to provide the Standard with portability and usefulness to a wide variety of cases and needs.

2.0 Terms and definitions.

The Standard uses terms that are defined as:

2.1 **Appropriate risk**: Risk that, as evaluated and stated, would appear to an organization, its interested parties, and authorities as acceptably low given the interests of parties who may be harmed by the risk.

2.2 **Assessing organizations**: Organizations that analyze risks that they may pose to others.

2.3 **Adjudicators**: Usually regulators or judges who may evaluate reasonableness of safeguards as compared to harm to others and may impose penalties as a result of their evaluation.

2.4 **Due care**: A degree of protection that a reasonable person applies to protect others from harm.

2.5 **Duty of care**: The responsibility of one party to prevent harm to others.

2.x **Factor**: A likelihood of an impact where multiple factors may be included in one risk analysis. For example the likelihood of harm to consumers is one factor while the likelihood of decreased efficiency is another factor; both of which may be part of one risk analysis.

2.6 **Impact**: The magnitude of harm that may be suffered by any party as a result of a threat. Can be stated qualitatively and quantitatively.

2.7 **Interested parties**: Individuals or organizations that may benefit by engaging in risk or that may be harmed if risk is realized.

2.8 **Likelihood**: The frequency, probability, or foreseeability of a threat creating an impact. Can be stated qualitatively and quantitatively.

2.9 **Reasonable safeguards**: Protections against the foreseeability or magnitude of risks that do not pose a burden that is greater than the risk it protects against.

2.x Resilience Thresholds: Likelihoods of impact that parties may tolerate or survive when a risk is realized.

2.10 **Risk Acceptance Criteria**: The likelihood of an impact that the organization equates with appropriate risk.

2.x **Risk Analysis**: A single evaluation of a risk – using one or more factors – to derive the likelihood of impacts.

2.x **Risk Analysis Mode**: A technique used to analyze the likelihood and magnitude of harm (e.g. qualitative analysis using ordinal values, or quantitative analysis using monetary values, population counts, percentages of reduced benefit, etc.).

2.x **Risk Assessment**: A process of evaluating many risks, often to understand the breadth and depth of risks in an environment.

2.11 **Threat**: An act or an omission that may create harm.

2.12 **Vulnerability**: A weakness or lack of a safeguard that may permit a threat to create harm.

3.0 Principles

The Standard applies three principles to risk analysis to ensure that the result of the analysis is fair to interested parties, is appropriate to all parties, and is reasonable to the assessing organization. Principles align with expectations that are commonly stated by regulatory bodies and judges.

3.1 Risk analysis must consider the interests of all parties that may be harmed by the risk.

3.1.1 Risk evaluations must include the foreseeability and magnitude of harm that may be experienced by any party.

3.1.2 Risk evaluations must characterize degrees of risk using resilience thresholds. These thresholds must be applied to all factors in a risk analysis so that degrees of risk to different parties may be compared equitably.

3.1.2 Assessing organizations may indicate the nature of their relationship to the other parties to declare whether they believe they have a duty of care to those parties. [1]

3.2 Risks must be reduced to a level that would not require a remedy to any party.

3.2.1 Assessing organizations must declare their intention to present risks to themselves and others that a reasonable person would accept as a consequence of engaging in the risk that would not require a remedy.

3.2.2. Estimations of risks that would be acceptable to other parties may be attained through rigorous estimation, assumption on the part of the assessor, explicit or tacit agreement with other parties, or other means.

3.3 Safeguards must not be more burdensome than the risks they protect against.

3.3.1 Assessing organizations must declare their intention to reduce risks using safeguards that are not more burdensome than the risks that the safeguards protect against.

[1] An assessor may evaluate risks to third parties for extra-legal reasons.

3.3.2. The assessing organization may compare the total burden to the total risk, or may evaluate alternative controls by comparing incremental burdens to incremental reductions in risk that the alternative control would incur.

4.0 Practices

The Standard declares ten practices that assessing organizations should apply to achieve the three principles. Practices are not commonly stated by authorities, such as regulators or standard bodies. Assessing organizations may develop variations on these practices that effectively support the principles.

4.1 Risk analysis considers the likelihood that threats could create magnitudes of impact.

4.1.1 Risk evaluations may be calculated using many means, such as by modeling probabilities using statistical analysis or by using simple ordinal values that are used in equations such as, “Risk = Impact x Likelihood.”

4.2 Tolerance thresholds are stated in plain language and are applied to each factor in a risk analysis.

4.2.1 Example tolerance thresholds are “Negligible,” “Acceptable,” “Unacceptable,” “Recoverable,” and “Catastrophic.”

4.2.2 Tolerance thresholds, once defined for the risk analysis, are applied to all factors in the analysis, regardless of the mode of risk analysis that is being used.

4.2.3 Because reasonableness of safeguards is evaluated by comparing them to the risks they would protect against, safeguards and risks must be comparable and therefore should be evaluated using the same tolerance thresholds.

4.3 Impact and likelihood scores have a qualitative component that concisely states the concerns of interested parties, authorities, and the assessing organization.

4.3.1 Whether using qualitative or quantitative risk evaluation modes, risks should be stated using language that easily communicates the potential of harm and the reasonableness of safeguards.

4.4 Impact and likelihood scores are derived by a quantitative calculation that permits comparability among all evaluated risks, safeguards, and against risk acceptance criteria.

4.4.1 Comparability among risks enables prioritization of risks.

4.4.2 Comparability against risk acceptance criteria enables a consistent standard for determining appropriateness.

4.4.3 Comparability between risks and safeguards permits a consistent process for determining reasonableness.

4.5 Impact definitions ensure that the magnitude of harm to one party is equated with the magnitude of harm to others.

4.5.1 Numeric impact scores should be assigned to magnitudes of impact .

4.5.2 Each numeric impact score should be associated with a definition of harm for each party that is considered in the risk analysis.

4.5.3 Numeric impact scores and their associated definitions of harm should be aligned such that a description of harm for one party is comparable to the description degree of harm suffered by any other party.

4.6 Impact definitions should have an explicit boundary between those magnitudes that would be acceptable to all parties and those that would not be.

4.6.1 An impact score that aligns with acceptable impacts to one party should consistently align with acceptable impacts to all other parties.

4.7 Impact definitions address; the organization's mission or utility to explain why the organization and others engage risk, the organization's self-interested objectives, and the organization's obligations to protect others from harm.

4.7.1 "Mission" or "utility" describes the benefit that interested parties may gain from the risk that is posed by the assessing organization.

4.7.2 "Objectives" describe the internal goals that assessing organizations set for themselves, or need to accomplish in order to successfully operate.

4.7.3 "Obligations" describe the harm that may come to others that assessing organizations intend to reduce or prevent.

4.8 Risk analysis relies on a standard of care to analyze current controls and recommended safeguards.

4.8.1 Standards of care include descriptions of good practice that guide behavior, expectations, or rules of behavior for industries, specialized fields, or professions.

4.9 Risk is analyzed by subject matter experts who use evidence to evaluate risks and safeguards.

4.9.1 Subject matter experts who can identify vulnerabilities that may lead to realized risks, who are capable of modeling threats that may realize risks, and who can determine whether safeguards are effective against risks, should conduct risk analysis.

4.9.2 Risk analysis should use available evidence, data, and information to assist in the modeling of threats, evaluation of vulnerabilities and safeguards, and in estimating the likelihood and impact of risks.

4.9.3 Risk analysis should include insights from the assessing organization's personnel to help identify risks and to estimate the likelihood and impact of risks.

4.10 Risk assessments cannot evaluate all foreseeable risks. Risk assessments re-occur to identify and address more risks over time.

4.10.1 Risk assessment projects should continuously evaluate risks in the environment. Opportunities for continuous risk analysis include:

4.10.1.1 When new threats become foreseeable.

4.10.1.2 When the environment changes.

4.10.1.3 When new interested parties are exposed to risks.

4.10.1.4 To determine the acceptability of exceptions to policies, rules, or controls.

4.10.1.5 When new vulnerabilities are identified.

4.10.1.6 After risks are realized to add new evidence to risk analysis.

5.0 Adoption and customization by assessing organizations

Assessing organizations that adopt the Standard may create a customized approach to analyzing risks.

5.1 Organizations conform to the Standard when they effectively demonstrate the three principles described in 3.1, 3.2, and 3.3.

5.2 Assessing organizations may conform to the Standard by using practices that vary from those described in 4.0, but will conform to the Standard only if their practices consistently lead to results that conform to the principles described in 3.1, 3.2, and 3.3.

6.0 Adoption and customization by standards bodies and professional associations

Standards bodies and professional associations may adopt the DoCRA Standard to create risk assessment methods for use by their constituents.

6.1 Risk assessment methods must quote from and conform to the three principles described in 3.1, 3.2, and 3.3.

6.2 Risk assessment methods may recommend practices other than those that are described in 4.0, but the methods must satisfy the objectives of those practices to conform to the Standard and must consistently lead to results produce the principles described in 3.1, 3.2, and 3.3.