DoCRA CHECKLIST

DoCRA

HALOCK®

halock.com | 847-221-0200 | Incident Response Hotline: 800-925-0559

An Information Security Industry Problem

Managing information security is hard enough without the hackers. Long before a security breach, information security leaders struggle to meet the needs of their executive management, regulators, and demanding clients. Limited budgets, competing priorities, and contentious auditors all create pressures that distract us from our mission.

Getting information security right isn't just about stopping the attacks. It's about balancing security against the needs of management, interested parties, and authorities.

That's why regulations, courts, and information security standards focus on risk. When done right, risk assessments set priorities by evaluating the likelihood of harm, they design safeguards that do not harm the mission, and can determine when certain risks are acceptable.

Interested Party	Their Concerns	Your Challenges
CIOs / Executives / Board	How does our **investment** in the security controls tie to what is important to the business?	Justifying **security investments** requires a defendable risk calculation, risks translated into initiatives, and executive-level dashboards.
Attorneys / Judges	Did you implement **reasonable** controls that could have prevented a breach?	Demonstrating to a judge that the security controls you implemented are **reasonable**.
Regulators	Is your use of the security controls **reasonable and appropriate** to achieve their version of **compliance?**	Showing regulators that your implemented security controls achieves their version of **compliance**.
Customers	Are you **appropriately protecting information** from harm?	Assuring customers that their information is **appropriately protected**.
IT and Security Professionals	How can we **get this done**?	**Prioritizing the implementation of security controls** and accepting risks at a reasonable level.

Is Your Risk Analysis DoCRA Compatible? A Checklist

DoCRA applies three (3) principles to risk analysis to ensure that the result of the analysis is fair, reasonable, and appropriate to all parties. The principles align with expectations that are commonly stated by regulatory bodies and judges.

THE DoCRA PRINCIPLE CHECKLIST

Principle	Question	(Y/N)
Principle 1 Risk analysis must consider the interests of **all parties** that may be harmed by the risk.	Does your risk evaluation include the foreseeability and magnitude of harm that may be experienced by all parties engaged in the risk?	☐
Principle 2 Risks must be **reduced to a level** that authorities and potentially affected parties would find appropriate.	Does your activity pose risks to yourself and others that a reasonable person would accept?	☐
Principle 3 Safeguards must **not be more burdensome** than the risks they protect against.	Do you reduce risks using safeguards that are not more burdensome than the risks that they protect against?	☐

Additionally, DoCRA declares **ten (10) practices** that assessing organizations should apply to achieve the three principles.

THE DoCRA PRACTICE CHECKLIST

Practice Question	Example	(Y/N)
Practice 1 Does your risk analysis **consider the likelihood** that certain threats could create measurable impact?	Risk evaluations may be calculated using many means, such as modeling probabilities using statistical analysis or by using simple ordinal values that are used in equations such as, "Risk = Impact x Likelihood."	☐
Practice 2 Are your **risks and safeguards are evaluated using the same criteria** so they can be compared?	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 criteria.	☐
Practice 3 Do your impact and likelihood scores have a qualitative component that concisely states the concerns of i**nterested parties, authorities, and the assessing organization**?	Whether using qualitative or quantitative risk evaluation methods, risks should be stated using language that easily communicates the potential of harm and the reasonableness of safeguards.	☐

The Solution - How DoCRA Solves this Industry Problem

The Duty of Care Risk Analysis ("DoCRA") Standard creates a common language, method, and understanding so that information security, legal, regulators, customers, and business management can address security and compliance together rather than competing for resources and strategic mindshare.

Interested Party	DoCRA Solution
CIOs / Executives / Board	Risks are concisely calculated and prioritized against the needs of customers, business objectives, and external entities. This helps justify investment, create defendable risk calculations, and translate risks into prioritized initiatives.
Attorneys / Judges	DoCRA allows you to achieve a **reasonable** implementation of security controls by evaluating your risks in a a manner than aligns with judicial reasoning.
Regulators	DoCRA helps to balance risks with burdens to match regulators' expectation for reasonable and appropriate **compliance.**
Customers	**The Acceptable Risk Definition** is stated in plain language allowing you to explain to customers how their information is **appropriately protected.**
IT and Security Professionals	DoCRA allows you to prioritize what matters to interested parties and to accept risks at a level the organization agreed to.

THE DoCRA PRACTICE CHECKLIST

Practice Question	Example	(Y/N)
Practice 4 Are your impact and likelihood scores derived by a **quantitative calculation that permits comparability** among all evaluated risks, safeguards, and against risk acceptance criteria?	**Comparability** among risks enables prioritization of risks. **Comparability** against risk acceptance criteria enables a consistent standard for determining appropriateness. **Comparability** between risks and safeguards permits a consisten process for determining reasonableness.	☐
Practice 5 Do your impact definitions ensure that the **magnitude of harm to one party is equated with the magnitude of harm to others**?	Numeric impact scores should be assigned to magnitudes of impact. Each numeric impact score should be associated with a definition of harm for each party that is considered in the risk analysis. 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.	☐
Practice 6 Do your impact definitions have an **explicit boundary between those magnitudes that would be acceptable to all parties** and those that would not be?	An impact score that aligns with acceptable impacts to one party should consistently align with **acceptable impacts to all other parties**.	☐
Practice 7 **Do your 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?	**"Mission"** or "utility" describes the benefit that interested parties may gain from the risk that is posed by the assessing organization. **"Objectives"** describe the internal goals that assessing organizations set for themselves or need to accomplish in order to successfully operate. **"Obligations"** describe the harm that may come to others that assessing organizations intend to reduce or prevent.	☐

THE DoCRA PRINCIPLE CHECKLIST

Practice Question	Example	(Y/N)
Practice 8 Does your risk analysis rely on a **standard of care** to analyze current controls and recommended safeguards?	Standards of care include descriptions of good practice that guide behavior, expectations, or rules of behavior for industries, specialized fields, or professions.	☐
Practice 9 Is your risk **analyzed by subject matter experts** who use evidence to evaluate risks and safeguards?	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. 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. Risk analysis should include insights from the assessing organization's personnel to help identify risks and to estimate the likelihood and impact of risks.	☐
Practice 10 Risk assessments cannot evaluate all foreseeable risks. Do your **risk assessments re-occur on a regular basis** to identify and address more risks over time?	Risk assessment projects should continuously evaluate risks in the environment. Opportunities for continuous risk analysis include: When new threats become foreseeable. When the environment changes. When new interested parties are exposed to risks. To determine the acceptability of exceptions to policies, rules, or controls. When new vulnerabilities are identified. After risks are realized to add new evidence to risk analysis.	☐

Getting Started with DoCRA

If you have answered "No" to any of the three Principles or struggle with the 10 Practices above, you may benefit from DoCRA expert to help you achieve DoCRA compatibility. HALOCK Security Labs has many ways to help you get started:

1

DoCRA Gap Assessment – This short engagement analyzes your risk method, identifies gaps to DoCRA, and makes high-level recommendations to get you DoCRA compatible.

2

DoCRA Risk Upgrade – Already have a risk method, but it's not DoCRA compatible? HALOCK can assist you in retrofitting your risk analysis to meet DoCRA requirements.

3

Full DoCRA Risk Assessment – HALOCK will conduct a complete DoCRA compatible risk assessment leveraging one or many control sets such as CIS Critical Controls, ISO 27001, NIST SP800-53, the HIPAA Security Rule, or PCI DSS.

HALOCK®

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
844-570-4666

halock.com

About HALOCK

HALOCK is a U.S.-based information security consultancy that is privately owned and operated out of its headquarters in Schaumburg, IL. From mid-sized to the Fortune 100, our clients span a variety of industries including financial services, healthcare, legal, education, energy, SaaS/cloud, enterprise retail, and many others. HALOCK strives to be your security partner, providing both strategic and technical security offerings. We combine strong thought leadership, diagnostic capabilities, and deep technical expertise with a proven ability to get things done. HALOCK helps clients prioritize and optimize their security investments by applying just the right amount of security to protect critical business assets while satisfying compliance requirements and corporate goals.