

The Problem: Risk Affects More than Cybersecurity Management

Information security professionals do more than just stop the hackers... they also must demonstrate to executives, regulators, and sometimes judges, whether security safeguards are **reasonable**. The challenge is that these interested parties have varying concerns. Security assessments and plans must evaluate controls based on the foreseeability of threats and the impacts to the organization and the public. When the burden of safeguards is in balance with the **appropriate** risk, then judges, regulators, and executives can agree that **due care** is applied.

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 defensible 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.

The Solution

The **Duty of Care Risk Analysis** (“DoCRA¹”) standard presents principles and practices for analyzing risks and communicating risks to technologists, executives, regulators, and judges. Regulators expect that the **burden of safeguards** should be balanced against an **organization’s mission** and objectives. Attorneys and judges conduct **balancing tests** to determine whether safeguards are **reasonable**. Conventional risk analysis has neglected to include these significant concepts. DoCRA combines regulatory and legal reasoning with information security standards of practice, allowing your organization to serve and easily communicate with all interested parties.

As organizations are different in their ability to assess and respond to risk, HALOCK adjusts our approach for each environment – easing in organizations that are just starting to analyzing risk, or a full-on approach with **Attack Path Threat Modeling**² for the seasoned experts.

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 defensible 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 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.

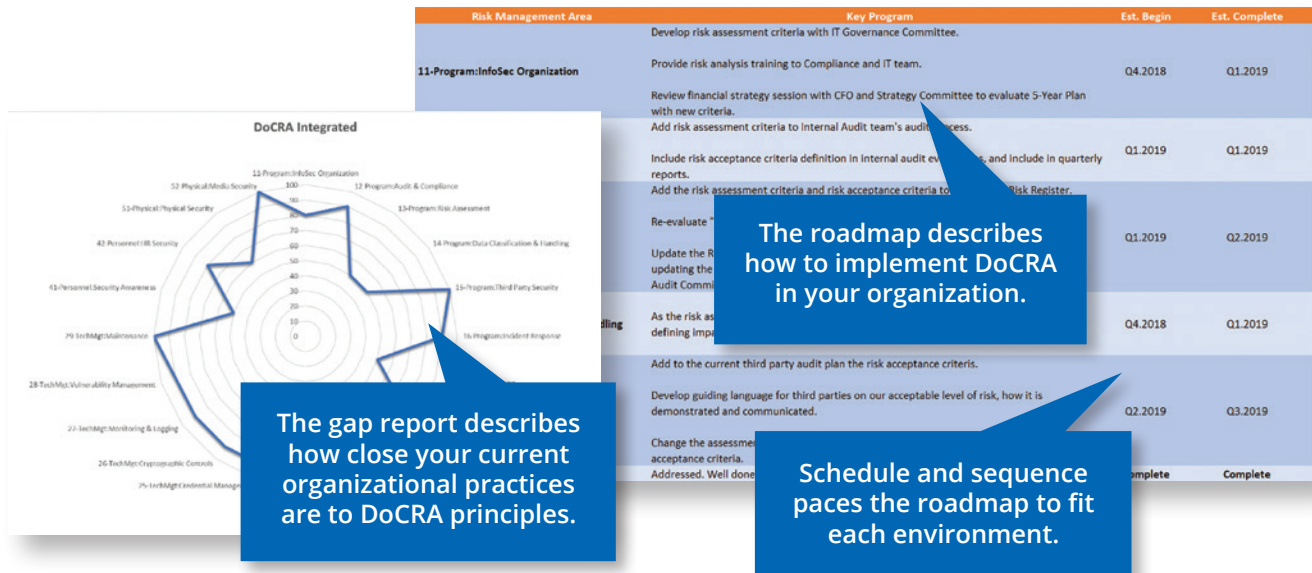
¹Please see DoCRA.org for more information.

²CIS Community Attack Model

HALOCK® DoCRA GAP ASSESSMENT

DoCRA Gap Assessment and Roadmap

For organizations that wish to learn about DoCRA and assess what it would take to implement DoCRA in their organization, HALOCK can perform a **DoCRA Gap Assessment and Roadmap** project. During the project a senior HALOCK resource will spend a business day on-site at your company to understand your environment, mission, priorities, and role of information security. The DoCRA Gap Assessment will familiarize your organization with DoCRA principles, practices and method for analyzing risk. Deliverables from the project include: DoCRA Gap Assessment Report and Roadmap for Implementing DoCRA at your organization.



HALOCK's Risk Management Services

If you wish to comply with DoCRA, you may need a DoCRA expert to assist in the transition. HALOCK Security Labs has a variety of DoCRA offerings to assist you.

HALOCK's Risk Management Services help organizations find the balance between information security and the competing needs of management, customers, regulators, and legal authorities. HALOCK's risk management offerings include:

- **DoCRA Gap Assessment and Roadmap** to help organizations assess and plan their move toward the DoCRA Standard.
- **DoCRA Upgrade** to help organizations transition their risk assessment process to the DoCRA Standard.
- **DoCRA Risk Assessments** to implement a DoCRA process from the ground up and to design the risk treatment safeguards.
- **Risk Management** to help organizations integrate DoCRA practices in their security program, such as vulnerability management, vendor management, executive reporting, etc.

About HALOCK

HALOCK is a U.S.-based information security consultancy that is privately owned and operated out of its headquarters in Schaumburg, IL since 1996. From mid-sized to the Fortune 100, HALOCK's 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. HALOCK combines 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.