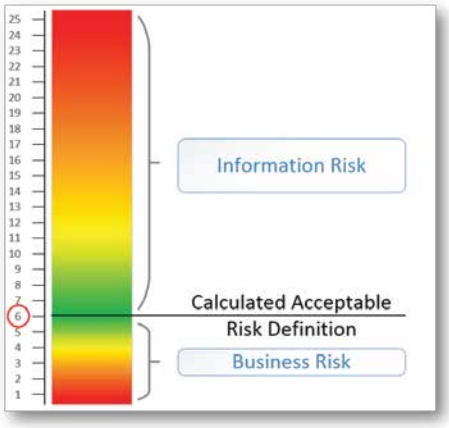
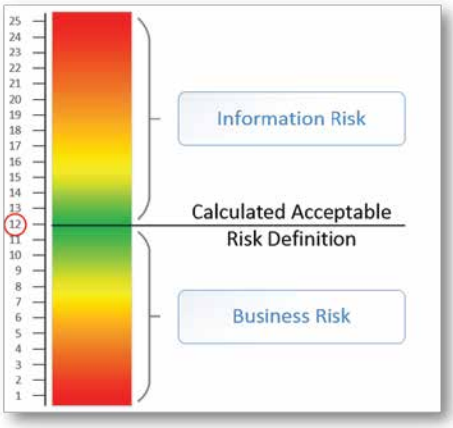
Calculated Acceptable Risk Definition

HALOCK's Calculated Acceptable Risk Definition (C.A.R.D.) allows organizations to start making security and compliance decisions based on risk even without starting their risk assessment! By engaging HALOCK to develop this critical management metric your organization will have a business-based test for determining whether controls and security investments meet regulatory requirements and business objectives. Your C.A.R.D. provides a "litmus test" for security budget requests and client security demands, and establishes your security controls as reasonable compliance when a breach occurs!

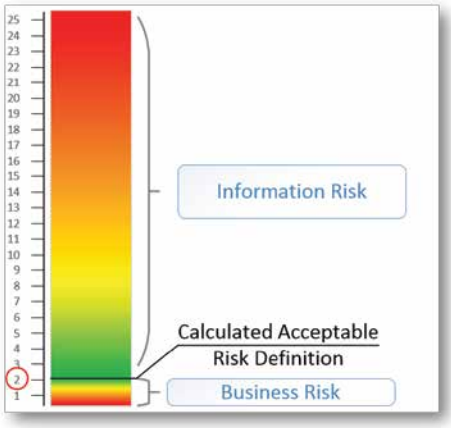
C.A.R.D. for a Retailer



C.A.R.D. for a Health Clinic



C.A.R.D. for a SaaS Provider



C.A.R.D. Scenario 1: Penetration Testing

- Know which of your systems should be tested with greater scrutiny than others based on whether their risk is above or below your C.A.R.D. number.
- Plan your pen testing schedule, assessing higher risk systems more often than lower risk systems.
- Demonstrate why a security fix is a reasonable repair for a discovered vulnerability based on its risk being below your C.A.R.D. number.
- Document why you have accepted some vulnerabilities based on their risk being below your C.A.R.D. number.

C.A.R.D. Scenario 2: Vulnerability Management Program

- Design a secure configuration baseline for systems that is defined by a risk-validated application of best-practices (SCAP) documentation.
- Justify variances from security best practices by demonstrating that those business-needed variances create risks that fall below your C.A.R.D. number.
- Address and correct variances that evaluate above your C.A.R.D. number, and demonstrate that your corrections were reasonable.
- Prioritize which systems to harden and test based on their risk evaluation.

C.A.R.D. Scenario 3: Hiring and Developing Security Personnel

- Determine which skillset you must acquire or develop first, based on risk calculations. Talented security professionals who are most experienced at managing the highest risk controls should be prioritized.
- Justify your "build vs. buy" strategy based on availability of security skills versus your need to continuously operate inherently risky systems and processes.
- Justify your "out-source vs. in-source" strategy by balancing the cost for specialized skills against the impact of risks that professionals protect against

C.A.R.D. Scenario 4: Evaluating New Security Technologies

- Prioritize the acquisition of security technologies that address your highest risks.
- Configure and architect new security technologies to prioritize risks that are above your C.A.R.D. number.
- Simplify potentially complex deployments by ignoring risks that are below your C.A.R.D. number.
- Demonstrate "due diligence" by responding to security events based on how their risk compares to your C.A.R.D. number.

HALOCK® Purpose Driven Security

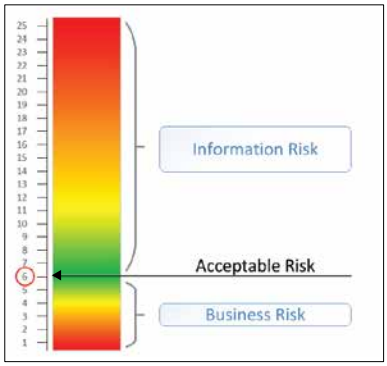
847.221.0200 | 800.925.0559 | info@halock.com | www.halock.com
NON EMERGENCY EMERGENCY RESPONSE HOTLINE

BBB ACCREDITED BUSINESS

EXAMPLE C.A.R.D.

Impact Score	Patient Care	Profitability	Patient Confidentiality
1. Negligible	No impact to patient care	$0.00	No impact to patient confidentiality
2. Low	Patient may feel inconvenienced	Up to $100,000	No impact to patient confidentiality
3. Medium	Near-miss	Up to $250,000	Patient confidentiality, short of ePHI exposure, occurs
4. High	Sentinel Event or need for transfer to hospital	Up to $1,000,000	ePHI is exposed for few patients
5. Catastrophic	Death of a patient	Over $1,000,000	ePHI is exposed for many patients

Likelihood Score	Likelihood Definition
1	Not foreseeable within 3 years
2	One occurrence within 2-3 years
3	Once per year
4	Once per six months
5	Monthly



"We will invest against incidents that foreseeably could, within the next three years:

- Create a near-miss, or worse, during a surgery,
- Would reduce profits by more than $100,000,
- Would expose patient information of any kind."

"So we can accept any risk that is lower than that."
-and-
"We can accept risks lower than '6' out of '25'"