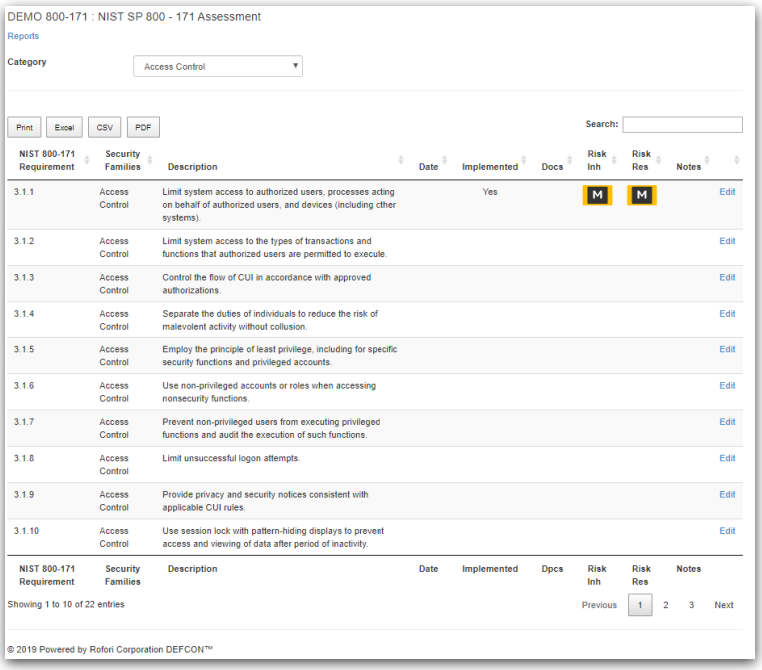
Cybersecurity Risk Assessment (NIST SP 800-171 / DFARS 7012)

The protection of unclassified federal information in non-federal information systems, such as government contractors (DFARS 7012), is dependent upon NIST SP 800-171 as a disciplined and structured process for identifying the different types of controlled unclassified information (CUI) that are routinely used by federal agencies.

800-171 Assessment Action Status	Inherent Risk Avg	Inherent Risk Max	Residual Risk Avg	Residual Risk Max
Access Control - 31%	M	VH	M	VH
Awareness and Training - 0%	H	H	H	H
Audit and Accountability - 11%	H	H	M	H
Configuration Management - 0%	H	H	H	H
Identification and Authentication - 0%	H	H	H	H
Incident Response - 0%	H	H	H	H
Maintenance - 0%	H	H	H	H
Media Protection - 0%	H	H	H	H
Personnel Security - 0%	H	H	H	H
Physical Protection - 16%	H	H	M	H
Risk Assessment - 0%	H	H	H	H
Security Assessment - 0%	H	H	H	H
System and Communications Protection - 0%	H	H	M	H
System and Information Integrity - 28%	H	H	M	H

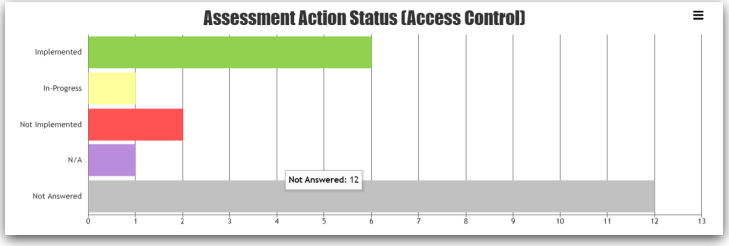
The Rofori Cybersecurity Risk Assessment—NIST SP 800-171 is a cloud-based solution that helps to reduce risk through continuous assessment and scoring, based on your alignment to NIST SP 800-171. This Cybersecurity Risk Assessment is a fundamental component of an organizational risk management process. Risk assessments are used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the country, resulting from the operation and use of information systems. In accordance with the NIST SP 800-171, the Rofori Risk Assessment lays out the entire Special Publication in an easy-to-use environment that a user can manage an organizations security program.

The Risk Assessment enables users to maintain and update the security posture over the course of time in a collaborative environment. Multiple individuals can access this system to continuously update their respective function in an



organization and all can quickly see where the organization's compliance IAW NIST SP 800-171 at any moment in time. The Rofori Cybersecurity Risk Assessment 's inherent and residual risk feature, nested with NIST SP 800-30, enables an organization to assess risk prior to and after mitigation measures are implemented. This feature serves as a core capability that enables an organization's ability to manage risk priorities and risk tolerance. The dashboard enables individuals at all levels of the organization to quickly see the organizational risk in accordance with their preferred cybersecurity standard. The current inherent and residual risk calculation is promptly displayed helping you understand your most critical risks within your organization and serves as a means to focus on implementing proper remediation to protect what is most important.

The Rofori Cybersecurity Risk Assessment was designed for easy implementation and delivery of risk status at-a-glance, in the form of a drill-down dashboard status display providing detailed visibility to your cybersecurity assessment status, as determined by your implementation response. Experience how the Rofori Cybersecurity Risk Assessment can make you more aware of the cyber risk in your business operations and help prioritize remediations while maintaining compliance with NIST SP 800-171!



Contact Us: sales@roforicorp.com Website: www.rofori.com