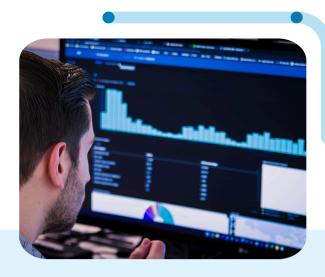# Is your organization compliance-ready?

Identify potential risks to the confidentiality, integrity, or availability of your environment.

## What is an IT Risk Assessment

A risk assessment is a systematic process aimed at evaluating potential threats and vulnerabilities in an organization's information tech infrastructure. It plays a fundamental role in a strong cybersecurity posture and ensures alignment with compliance frameworks like FTC/SEC, CMMC, HIPAA, GDPR, SOC, SEC/FINRA, and others.

It aids in identifying priorities and determining where organizations should focus implementation efforts.

## Key Components of an IT Risk Assessment

**Step 1**
Identification of Assets

**Step 2**
Threat Identification

**Step 3**
Vulnerability Assessment

**Step 4**
Risk Analysis

**Step 5**
Risk ID and Control

**Step 6**
Documentation and Reporting

## Why Complete an IT Risk Assessment?

- Contribute to Proactive Cybersecurity Measures
- Improve Incident Response Preparedness
- Enhance Business Continuity Planning

- Meet Regulatory Compliance Requirements
- Enhance Decision-Making
- Identify Opportunities to Proactively Mitigate Risk

**Learn More at www.gadellnet.com**

Navigating IT Security with a Risk Assessment

**St. Louis**: (314) 736-5304 | **Indianapolis:** (317) 912-3091 | **Denver:** (720) 464-5920

## GADELLNET