Information security risk management is a dynamic and fluid process – and a careful balancing act. Despite this fact, the process of identifying and managing security risks is a foundational component of any security program.

NCA’s Information Security Risk Management offering is designed to help organizations measure and manage their security risks by:

- Establishing clearly-defined risk tolerance thresholds
- Monitoring and evaluating the changing threat landscape
- Identifying security vulnerabilities and potential exposures
- Assessing the potential business impact of a security breach
- Offering risk treatment options that are driven by requirements

Many security practitioners have embraced commonly accepted risk management practices without fully understanding them or recognizing their inherent limitations. True risk management is a matter of thresholds, probabilities, and loss magnitudes that are measured against real-world business needs. NCA’s security consultants are carefully trained to separate fact from fiction and have adopted a variation of the Factor Analysis of Information Risk (FAIR) methodology for conducting risk assessments. Our consultants can also customize a solution that is unique to your business needs by leveraging:

- Risk Management Guide for Information Technology Systems (NIST SP800-30)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
- Information Security Management Systems (ISO 27001)
- Fundamental Information Risk Management (FIRM)
- Information Risk Analysis Methodologies (IRAM)
- Simplified Process for Risk Identification (SPRINT)
- RISK IT Framework (Risk IT)

Once engaged, the knowledge, skills, and experience that NCA’s seasoned security consultants bring to the table can greatly enhance the validity and value of your overall risk management program.