The Opportunity. When the International Organization for Standardization (ISO) released an updated set of requirements called ISO 27001:2013 Information Security Management System (ISMS), our client sought to integrate these new requirements into its enterprise Information Security Management framework. Incorporating a consortium of industry-accepted information security standards would further strengthen the credit union’s framework and streamline compliance efforts.

The Client
A global credit union that provides a wide range of financial services to over four million members.

The Obstacles
To integrate the two sets of control requirements, the credit union needed to perform a gap analysis between its existing security framework (based on the SANS critical security controls) and the newly released ISO requirements. However, a deeper understanding of the frameworks and industry best-practices would be needed to demonstrate compliance with an integrated and rationalized security controls baseline before the next regulatory audit.

The Acceleration
The credit union engaged Celerity’s IT Risk Management experts to perform a gap analysis and incorporate additional security best practices and standards into the framework. Our seasoned consultants quickly leveraged our experience in designing risk and compliance programs to help our client establish a foundation that supports the objectives of an Integrated Risk and Compliance Program.

Over the course of two months, Celerity worked with the client to create a hybrid framework that successfully integrates ISO and SANS controls. We:

- Reviewed and validated the existing information security framework against the new ISO 27001:2013 requirements
- Developed measurements of effectiveness for the ISO 27001:2013 control requirements based on identified coverage gaps
- Established measurement data to gauge the effectiveness of the ISO 27001 controls for the identified coverage gaps, with linkage to key risks
- Recommended and published updates to the current Information Security Framework to reflect the updated ISO requirements
Celerity’s deep understanding of these information security controls frameworks enabled a speedy integration into the organization’s operating model.

**Our Project Deliverables included:**
- Rationalized information security requirements baseline
- Information security metrics plan, including formula, trending and implementation evidence
- Enterprise Information Security Framework

**Lasting Results**
In just two months, Celerity’s team helped to bolster an enterprise information security framework based on the latest ISO 27001 requirements, while improving operational compliance and efficiency by reducing the number of duplicate control activities.

**Lasting positive effects of this project include:**
- Streamlined compliance efforts by creating an integrated rationalized security controls baseline that satisfies requirements from multiple standards or frameworks
- Created an analysis dashboard to highlight coverage analysis (e.g., percentage of ISO controls that have no coverage, partial coverage, or full coverage) that helps to reduce inconsistencies or overlaps between requirement sets
- Established measures of effectiveness for 14 ISO security domains to standardize metrics collection, analysis and reporting
- Recommended trending analysis on security controls to improve compliance visibility and continued adherence to the ISO framework
- Made recommendations to and updated the organization’s Information Security Management Framework to ensure current alignment with ever-changing information security best practices

**Methodologies & Standards**
- SANS 20 Critical Controls
- ISO 27001: 2013
- ISO 27002: 2013
- NIST Special Publications
- COBIT 5.0

**About Celerity**
Celerity accelerates business results in the emerging digital economy through a unique blend of technical, business, and experiential design competencies. Our service areas include Business Transformation, Enterprise Technology, Web & Mobile, and Talent.

**CONTACT**
Ellen Ozderman
Director, Information Security & IT Risk Management
bts@celerity.com

**Corporate Headquarters**
P. 703.848.1900  F. 703.848.2139