NCDOR NORTH CAROLINA DEPARTMENT OF REVENUE

North Carolina Department of Revenue Certification and Accreditation Project

Category: Cybersecurity

State: North Carolina

Contact: Jerome.Smith@ncdor.gov
December 2015-April 2016

Executive Summary

The North Carolina Department of Revenue needed a process for the accreditation and certification of technologies and Capabilities. Technology Capabilities allow our agency to successfully carry out key mission and business functions. Capabilities include, as constituent components, a range of diverse computing platforms from mainframe to smart phones. Capabilities can also include very specialized resources such as IVR, predictive dialer, next generation firewalls, and other IT services. For this reason, it is equally important for agencies to ensure they are adequately protected.

Data and Capabilities are subject to serious threats that can have adverse impacts on Department operations (including mission, functions, image, and reputation), Department Resources, staff, and work with other organizations. Threats can compromise the confidentiality, integrity, or availability of Data that is processed, stored, or transmitted within those Capabilities. Threats include environmental disruptions, human or machine errors, and purposeful attacks. Attacks on resources today are often aggressive, disciplined, well-organized, well-funded, and in a growing number of documented cases, very sophisticated. Therefore, successful attacks on Department Capabilities can result in serious or grave damage to the economic security interests of the State.

Given the significant and growing danger of these threats, it is imperative that leaders at all levels of the Department understand their responsibilities. We need a method to achieve adequate information security and manage Capability-related security risks. The accreditation and certification process helps to ensure that new and existing Capabilities obtain an appropriate security process necessary to protect these resources.

Project Narrative:

Concept

This project, based on NIST Special Publication 800-37 rev 1, implements the North Carolina Department of Revenue Certification & Accreditation (C&A) process. It provides essential information to the CIO regarding the acceptance of risk arising from the operation and use of described Capabilities. It utilizes monthly metrics, dashboards, and serves as the agency's governance model for the protection of taxpayers' assets.

The C&A process has the following characteristics and elements:
Promotes the concept of Information Security Management being fully integrated into the System Development Lifecycle (ITIL).
Promotes the concept of Information Security Management being fully integrated into the System Development Lifecycle (ITIL).
Provides emphasis on the selection, implementation and assessment of security controls.
Links risk management processes at the Capability level to risk management processes at the Department level through a risk executive function, the Department CIO.
Establishes responsibility and accountability for security controls deployed within Department Capabilities.
Allocates Resources to include both funding to carry out the risk management tasks and assigning qualified personnel needed to accomplish the tasks.
Assesses processes by review of the C&A documentation

The C&A process is applied to Department Capabilities through a publication which includes these phases:

1. Security categorization
2. Security control selection and implementation
3. Security control assessment
4. Capability authorization

This publication is communicated to the stakeholders during the design phase. It ensures that stakeholders understand that the C&A process has to be finalized to receive an ATO (Authority to Operate) from the CIO.

Significance

The process ensures that:

- The managing Capability related security risks are consistent with the Department's mission & business objectives, and supports an overall risk strategy established by the senior leadership, through the CIO.

- Information security requirements, including necessary security controls, are integrated into the Department's enterprise architecture, as defined by the Architect, and the Department's system development life cycle processes, ITIL. This applies to all Resources and Data that is stored, processed, or transmitted by the Department and includes all environments (e.g. Development, Test, Production, Training, etc.)

It is a consistent and yet customizable way to address organizational risk. It has the added benefit of being understood and actionable by all levels of the organization. It addresses the individual areas of concern that each department or area of the agency may have. The guidelines in the publication are applicable to all Department Capabilities.

Impact

C&A establishes a centralized process and management for Capability-related security risks. The process leads to substantial and measurable change by making the agency more governance oriented.

Benefits include:

- Incorporating risk management principles and best practices into Department-wide strategic planning considerations, mission and core business processes, and supporting Department Capabilities.

- Integrating information security requirements into the ITIL lifecycle process for all environments (i.e. Development, Test, Production, Training, and Disaster Recovery)

- Establishing practical and meaningful boundaries for Department Capabilities.

- Allocating security controls to Department Capabilities.

- Responding to regulatory audits with ease.

- Applying a consistent and effective approach to all risk management processes and procedures.

Allocating Resources

The CIO identifies the resources necessary to complete the risk management tasks described in this publication and ensures that those resources are made available to the CISO. Resource allocation includes both funding to carry out the risk management tasks and assigning qualified personnel needed to accomplish the tasks.

Certification & Accreditation Checklist

Data Classification

1-1	Data Classification	Has the Architect determined the Data classification as will be stored, processed or transmitted by the Capability?
1-2	Architecture	Are the Business, Information (Data) & Solution (Build), and Technical (network) architectures documented?
1-3	Asset	Has the Department registered the Resource or Capability?

Security Plan

2-1	Risk Assessment	Is there a Risk Assessment Report as required by DOR Security Policy CA-2?
2-2	Select Security Controls	Have the controls for the Capability been selected based on the Data classification as determined by the Architect?
2-3	Security Plan	Is the application of the controls for the Capability in the Security Plan?
2-4	Continuous	Has the Department developed a continuous monitoring strategy for the Capability?

Implement Security Controls

3-1	Implement controls	Has the Department documented how external services have been implemented?
3-2	Document the application of controls	Has the Department documented how controls have been implemented in the Security Plan?

Security Assessment

4-1	Security Assessment plan	Is the Security Plan complete? Including how external services have been implemented? Is the Security Assessment Plan reviewed and approved by the CIO?
4-2	Security Assessment	Is the Security Assessment complete? Including those provided by external service providers?
4-3	Security Assessment report	Is the Security Assessment Report complete?
4-4	Initial Remediation	Has the CISO mitigated initial control weaknesses?

Authority to Operate

5-1	POA&M	Has the POA&M been completed and addresses all defined control Weaknesses?
5-2	Request for ATO	Capability Owner submits the authorization package including the Risk Assessment, Security Plan, Security Assessment, and CISO Recommendation.
5-3	Risk Determination	CIO determines if the risk to Department operations, Resources, Staff, and other organizations associated with the operation of the Capability is acceptable.
5-4	Authority to Operate	Is the authorization package (request for ATO) complete? Was the authorization decision conveyed to appropriate organizational personnel including Resource owners and external service providers?