Office of the Chief Information Officer Directive: IT 7.05	Published: 04/2021
Chapter: Monitoring and Evaluation	Last Review: 01/2024
Subject: **Cyber Security Risk Assessments**	

1 DIRECTIVE

1.01 A Cyber Security Risk Assessment will be completed for all new Critical GNB Information Systems or Services. A Cyber Security Risk Assessment will be completed every three years thereafter, or whenever the Critical Information System or Service is significantly changed.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that existing security threats are being appropriately handled and that new and evolving threats will be considered and appropriately addressed.

This ensures proper documentation of information risk and non-compliance associated with the assets being assessed and ensures Business Owners are informed about identified risk so that necessary action can be taken.

3 SCOPE

3.01 This directive applies to all Departments using the GNB Networks and any devices and personnel involved in that use.

This directive supersedes the GISSP Standards & Directives Document published in November 2006.

4 RESPONSIBILITY

4.01 OCIO is responsible to initiate a Cyber Security Risk Assessment on critical systems and present the findings and proposed action plans for approval by the Business Owner.

4.02 OCIO is responsible:

(a) To manage each Cyber Security Risk Assessment. The actual work involved may be done by the DISO (or designate) or a Third Party.

(b) To initiate a Cyber Security Risk Assessment if a new security threat is identified well in advance of the next regular security review.

5 DEFINITIONS

5.01 “Business owner” is a senior member within the organization who is accountable for overall management of defined data set for a line of business. The business owner has decision-making authority for who accesses and uses the data and is usually supported by data stewards. They approve processes and policies to uphold data quality and standardize data management processes.

5.02 “Cyber Security Risk Assessment” is a snapshot of the cyber security risks and existing cyber security controls of a technology system or application.

5.03 "Critical Information System or Service" is an information system or service essential to the delivery of Critical GNB Services.

5.04 "Critical GNB Service" is a service essential to GNB or the public to prevent losses related to health and safety, finance, confidence in the government, environment, or social hardship.

6 RELATED DIRECTIVES

OCIO IT Chapter 8 – Physical and Systems Security
OCIO IT Chapter 9 – Data Security
OCIO IT Chapter 11 - Backup and Disaster Planning