THE CENTRAL BANK OF BELIZE

MISSION

To promote the stability of monetary and financial systems for the wellbeing of Belize.

AML STRATEGY

It is the policy of the Central Bank of Belize (Central Bank) to contribute to the national AML strategy to prevent money laundering, terrorism financing, and financing the proliferation of weapons of mass destruction.

This strategy is a collaborative effort between the Central Bank, other domestic and foreign supervisory authorities, and supervised institutions to actively identify, understand, and assess ML/TF/PF risks in Belize's financial system. Together, risk-based mitigating measures are implemented to align with international standards and best practices. In addition, on-going outreach is undertaken to sensitize stakeholders on AML matters.

CENTRAL BANK of BELIZE

Gabourel Lane
Belize City
BELIZE
Tel: (501) 223 – 6194
Web: www.centralbank.org.bz
Email: compliance@centralbank.org.bz

CENTRAL BANK of BELIZE

ANTI-MONEY LAUNDERING HIGHLIGHTS

Notice No. 2 | June 2024

CYBERSECURITY

WHAT IS CYBERSECURITY?

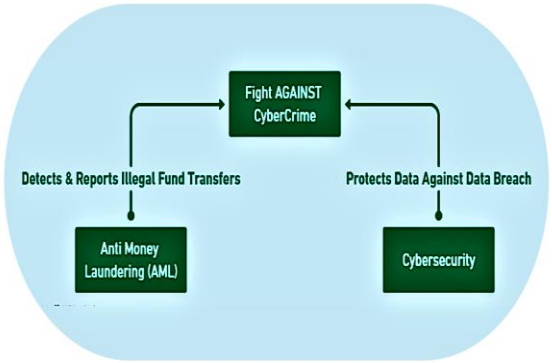
Cybersecurity is defined by the International Organization for Standardization (ISO) as the safeguarding of people, society, organizations and nations from cyber risks. Safeguarding means to keep cyber risk at a tolerable level.

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information (Cybersecurity & Infrastructure Security Agency, 2021).

RELATIONSHIP BETWEEN CYBERSECURITY AND AML SYSTEMS

Cybersecurity and anti-money laundering (AML) compliance are closely intertwined. Here's how they connect:

- **Data Protection**: AML systems collect and store sensitive customer information, such as identity verification, transaction details, and adverse media reports (Cybergate, 2020).
- **Fraud Detection**: Cybersecurity tools help detect and prevent fraudulent activities, which are often linked to money laundering (Cybergate, 2022).
- **Incident Reporting**: Cyber incidents, such as data breaches, can be indicators of money laundering or other financial crimes (Cybergate, 2022).



Source: Google Photos

- **Collaboration**: Effective AML compliance requires collaboration between cybersecurity and compliance teams (Cybergate, 2022).

In 2016, the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury that gathers and scrutinizes financial transactions to prevent money laundering and terrorism financing, issued a guide outlining the below five key components of an effective cybersecurity program. Financial institutions are to:

- Conduct a thorough risk assessment to identify potential cybersecurity threats and vulnerabilities.
- Implement appropriate controls and safeguards to manage cybersecurity risks.
- Participate in information-sharing programs to enhance their understanding of cybersecurity threats and to stay up-to-date on the latest threats and vulnerabilities.
- have an incident response plan in place to respond quickly and effectively to cyber attacks.
- Review and update their cybersecurity program continuously to address new and emerging threats.

CyberCrimes 2013 to 2018				% per annum
	Crimes targeting technology, etc.*	Crimes committed through technology**		Growth
Year	Incidents	Incidents	Total # Incidents	
2013	521	80	601	
2014	663	116	779	29.62%
2015	713	166	879	12.84%
2016	818	145	963	9.56%
2017	773	118	891	-7.48%
2018	768	136	904	1.46%

* For example cellphones, computers, note books, theft, damage, virus etc.
** For example, social engineering, phishing, texts, emails, etc.

Source: National Cybersecurity Strategy Towards a Secure Cyberspace 2020-2023

- ***For more information read the Cybergate article and the FinCEN guide at the links below:***
- https://cybergateinternational.com/blog/exploring-how-cyber-security-and-anti-money-laundering-go-hand-in-hand/
- https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf

KEY TAKEAWAYS:

Financial institutions should:

- Integrate cybersecurity with AML compliance so your financial institution can better protect its systems and data, detect and prevent financial crimes, and ensure it meets regulatory requirements.
- Ensure robust cybersecurity measures are in place to help mitigate risks and protect your institution.
- Implement cybersecurity measures, to significantly enhance your institution's cybersecurity posture.