



The Official Gazette

PUBLISHED
BY
AUTHORITY

VOL. CLX No. 9

Part B

BRIDGETOWN, BARBADOS, 30TH JANUARY, 2025

Contents

Executories re Estates of Randal Miller, Clyde Denny a.k.a. Clyde Austin Denny, Lionel Othniel Evelyn and Anthony Alieston King a.k.a. Anthony Aeilston King a.k.a. Anthony King	2, 3
Notice of Application for Declaration of Ownership and Certificate of Title for Frank Desmond Skeete et al	5
Notice re Guardian Life Limited	4
Notices of Revival of Registration re: Verus Investments Holdings Inc. and Verus International Group Limited	1
Probate Advertisements	11-17
Republic Bank (Barbados) Limited Summary Non-Consolidated Statements of Financial Position as at 30 September 2024	6-10

Financial Services Commission re Fitness & Propriety Guideline
Technology and Cyber Risk Management Guideline
Domestic Non-Bank Systemically Important Financial
Institutions Guideline

NOTICE NO. 1

THE COMPANIES ACT, CAP. 308
(Section 339)

NOTICE OF REVIVAL OF REGISTRATION

VERUS INVESTMENTS HOLDINGS INC.
Company No. 40517

In accordance with Section 339(3) of the Companies Act, Cap. 308 Notice is hereby given that the registration of the above-mentioned external company has been revived by the Registrar of Companies with effect from November 27th, 2024.

Dated 17th day of December 2024.

STEVEN K. PARKER
Director.

NOTICE NO. 2

THE COMPANIES ACT, CAP. 308
(Section 339)

NOTICE OF REVIVAL OF REGISTRATION

VERUS INTERNATIONAL GROUP LIMITED
Company No. 40518

In accordance with Section 339(3) of the Companies Act, Cap. 308 Notice is hereby given that the registration of the above-mentioned external company has been revived by the Registrar of Companies with effect from November 27th, 2024.

Dated 17th day of December 2024.

STEVEN K. PARKER
Director.

NOTICE NO. 3

NO.: 466 of 2024

IN THE HIGH COURT OF JUSTICE*Civil Division
(Probate)**In the Matter of the Estate of***RANDAL MILLER***Deceased*

NOTICE IS HEREBY GIVEN in accordance with Section 31 of the Trustee Act, Cap. 250 to all persons having any debts, claims or demands upon or affecting the Estate of RANDAL MILLER deceased late of No. 33 Callender's Crescent in the parish of Christ Church in this Island of Barbados, who died at Callender's Main Road in the parish of Christ Church in this Island on the 17th day November, 2022, to send particulars of their claims duly attested to Vincent D. Watson, Attorney-at-Law of Legis Chambers, Upper Collymore Rock in the parish of Saint Michael in this Island for JACQUELINE PAULETTE BRANDFORD the Administratrix of the Estate of the said RANDAL MILLER, on or before the 30th day of March, 2025, after which the Administratrix and Personal Representative, shall proceed to distribute the assets of the Estate among the persons entitled thereto having regard only to the debts and claims of which the Administratrix and Personal Representative shall then have had notice at the time of distribution and all persons indebted to the said Estate are required to settle their account without delay.

Dated the 28th day of January, 2025.

VINCENT D. WATSON, Attorney-at-Law
for JACQUELINE PAULETTE BRANDFORD
the Administratrix and Personal Representative
of the above-named Estate.

NOTICE NO. 4

*In the Estate of***CLYDE DENNY also known as
CLYDE AUSTIN DENNY***Deceased*

NOTICE IS HEREBY GIVEN pursuant to Section 31 of the Trustee Act, Cap. 250 of the Laws of Barbados, to any person having any claim against or interest in the Estate of CLYDE DENNY also known as CLYDE AUSTIN DENNY, deceased, late of Passage View, Passage Road in the parish of Saint Michael in Barbados who died at the Queen Elizabeth Hospital in the parish of Saint Michael in Barbados on the 18th day of August 2023 to send particulars in writing of his or her claim or interest to TRENA A. KELLMAN of Morris & Kellman Attorneys-at-Law, Suite 1 Building 2, Manor Lodge Complex in the parish of Saint Michael in Barbados on or before the 28th day of March 2025 after which date the Executrix will convey and distribute the assets of the Estate among the persons entitled having regard only to the valid claims of which she shall then have had notice. And all persons indebted to the said Estate are required to settle their indebtedness without delay.

Dated this 28th day of January 2025.

TRENA A. KELLMAN
Attorney-at-Law for the Executrix
of the Estate of CLYDE DENNY also known as
CLYDE AUSTIN DENNY, deceased.

NOTICE NO. 5

**UNDER SECTION 31 OF THE TRUSTEE ACT,
Cap. 250***In the Estate of***LIONEL OTHNIEL EVELYN***Deceased*

NOTICE is hereby given pursuant to Section 31 of the Trustee Act, Cap. 250 of the Laws of Barbados to all persons having any debts, claims or demands upon or affecting the Estate of LIONEL OTHNIEL EVELYN, deceased, late of 14510 NW 12th Avenue, Miami, Florida 33168 in the United States of America who died in the United States of America on the 4th day of May 2012, to send particulars of their claims duly attested to JESSICA EVELYN the appointed Administratrix of the Estate of the deceased in care of INTERCARIBBEAN LEGAL, Attorneys-at-Law, Cnr. Pine and Belmont Roads, Belleville, St. Michael on or before the 1st day of April 2025 after which the said JESSICA EVELYN will distribute the Estate among the persons entitled thereto having regard only to the claims and interest of which she shall have notice and will not in respect of the property so distributed be liable to any person of whose claim she shall not then have had notice.

And all persons indebted to the said Estate are requested to settle their accounts without delay.

Dated this 30th day of January 2025.

INTERCARIBBEAN LEGAL
Attorneys-at-Law of the Administratrix.

NOTICE NO. 6

BARBADOS

*In the Matter of the Estate of***ANTHONY ALIESTON KING also known as
ANTHONY AEILSTON KING also known
ANTHONY KING***Deceased*

PURSUANT to the Trustee Act, Cap. 250 of the Laws of Barbados Notice is given that all Creditors and other persons having claims or demands against the Estate of ANTHONY ALIESTON KING also known as ANTHONY AEILSTON KING also known ANTHONY KING, deceased late of Jericho, Near Market Hill in the parish of Saint George in this Island who died on the 17th day of April, 2019 are hereby required to send such particulars in writing of their claims and demands to the Administratrix JACQUELINE PETRINA BRATHWAITE (acting herein by LURLEEN LYNETTE SOBERS her duly appointed Attorney on record in this Island C/O Alphonza McD. Carew, Attorney-at-Law, AMC Law Chambers, Lower Bank Hall Cross Road, St. Michael no later than the 4th day of April, 2025 after which date the Administratrix will distribute the property among the persons entitled thereto having regards only to the claims and demands of which they shall not be liable for the property of the said deceased or any person or persons of whose claims and demands they shall not have had notice.

AND all persons indebted to the said Estate are required to settle their indebtedness without delay.

Dated the 30th day of January 2025.

ALPHONZA McD. CAREW
Attorney-at-Law for the abovenamed Estate.

NOTICE NO. 4 (third publication)

GUARDIAN LIFE LIMITED PUBLIC NOTICE

NOTICE is hereby given that Guardian Life Limited has never under-written any business in the Island of Barbados but has run-off a portfolio which it acquired in 1999.

Guardian Life Limited therefore intends to apply for the release of its deposit presently held by the Financial Services Commission under Section 5(2) of the First Schedule of the Insurance Act CAP.310, on or about April 1, 2025, which is three (3) months from the date of this Notice being placed in a newspaper and the Official Gazette in accordance with the terms of the Insurance Act CAP.310.

Any policyholder who has an outstanding claim against Guardian Life Limited is invited to write to the Chief Executive Officer, Financial Services Commission, Bay Corporate Building, Bay Street, St. Michael, Bridgetown, Barbados, or via e-mail at insurance@fsc.gov.bb and to Suzette Radlein, Guardian Life Limited, 12 Trafalgar Road, Kingston 5, Jamaica, or via e-mail at suzette.radlein@myguardiangroup.com.

Guardian Life Limited
Suzette Radlein
Assistant Vice President-Legal, Compliance and Risk



live secure | live easy



NOTICE NO. 3 (third publication)

Land (Title Proceedings) Act, 2011
(Act 2011-7)

Form 3

**NOTICE OF APPLICATION FOR DECLARATION OF OWNERSHIP AND
CERTIFICATE OF TITLE IN RESPECT OF ALL THAT LAND
SITUATE AT ERMY BOURNE HIGHWAY, FORMERLY
EAST COAST ROAD, SAINT ANDREW IN THIS ISLAND**

**SUPREME COURT OF BARBADOS
IN THE HIGH COURT OF JUSTICE**

CLAIM NO. CIV 1309 of 2024

**IN THE MATTER OF THE LAND (TITLE PROCEEDINGS) ACT, 2011
(section 3);**

AND IN THE MATTER OF ALL THAT land containing by admeasurement 3,665.0 square metres or thereabouts situate at Ermy Bourne Highway formerly East Coast Road in the parish of Saint Andrew in this Island and bearing the land tax reference number 21.12.01.012 **ABUTTING AND BOUNDING** on lands now or late of Fitz Collymore, on lands now or late of the Estate of Erma Rock and on the Ermy Bourne Highway or however else the same may abut and bound.

TAKE NOTICE that **FRANK DESMOND SKEETE** (as the duly appointed Executor and personal representative of the Estate of **EDWARD ANDREW BRUCE SKEETE**) of Edgumbe Plantation, Edgumbe in the parish of Saint George in this Island, **RICHARD ALAN COX** (as the duly appointed Executor and personal representative of the Estate of **MARY PATRICIA COX née SKEETE**) of #5 Montview Terrace, Jordans in the parish of Saint George in this Island and **ANDREW PAUL BARKER** (as one of the duly appointed attorneys of **HILDA ELIZABETH BARKER née SKEETE**) of Pine Tops, 14 Hillcrest Close, Wyesham, Monmouth NP25 3LN in the United Kingdom have applied to the High Court for a declaration of ownership and a certificate of title in respect of the properties described above.

Any person having any adverse claim, lien or charge or right or interest against the said property should submit the claim duly authenticated on oath to the Registrar of the Supreme Court, Bridgetown on or before the **17th day of February 2025**.

Any other person who has any information relating to the ownership of the said property is invited to give such information in writing to the Registrar of the Supreme Court, Bridgetown on or before the **17th day of February 2025**.

Dated the 2nd day of January 2025.

TESO LAW
Attorneys-at-Law for the Applicants,
whose place of business and address for service is “Dormers”,
Prior Park, St. James.



Republic Bank (Barbados) Limited

(A Subsidiary of Republic Financial Holdings Limited)

SUMMARY NON-CONSOLIDATED STATEMENT OF FINANCIAL POSITION AS AT 30 SEPTEMBER 2024

(Expressed in thousands of Barbados dollars)

	2024	2023
ASSETS		
Cash and cash equivalents	75,255	33,408
Deposits with Central Bank	291,943	432,034
Due from banks and related banks	58,543	74,214
Advances	1,773,051	1,665,713
Other assets	647,670	662,210
TOTAL ASSETS	2,846,462	2,867,579
LIABILITIES AND EQUITY		
LIABILITIES		
Customers' current, savings and deposit accounts	2,407,597	2,424,545
Other liabilities	154,878	81,035
TOTAL LIABILITIES	2,562,475	2,505,580
EQUITY		
Stated capital	48,000	48,000
Statutory reserves	48,000	48,000
Revaluation reserve	4,844	5,004
Other reserves	(34,623)	(37,201)
Retained earnings	217,766	298,196
TOTAL EQUITY	283,987	361,999
TOTAL LIABILITIES AND EQUITY	2,846,462	2,867,579

These summary financial statements were approved by the Board of Directors on 5 December, 2024 and signed on its behalf by:

Carlene Seudat

Director

Geoffrey Roach

Director

Debbie Fraser

Director



Republic Bank (Barbados) Limited

(A Subsidiary of Republic Financial Holdings Limited)

SUMMARY NON-CONSOLIDATED STATEMENT OF INCOME FOR THE YEAR ENDED 30 SEPTEMBER 2024

(Expressed in thousands of Barbados dollars)

	2024	2023
Net interest income and other income	142,122	140,064
Operating expenses	(111,731)	(91,902)
Operating profit	30,391	48,162
Credit loss recovery on financial assets	6,934	105,034
Net profit before taxation	37,325	153,196
Taxation credit (expense)	485	(5,401)
Net profit after taxation	37,810	147,795

SUMMARY NON-CONSOLIDATED STATEMENT OF COMPREHENSIVE INCOME FOR THE YEAR ENDED 30 SEPTEMBER 2024

(Expressed in thousands of Barbados dollars)

	2024	2023
Net profit after taxation	37,810	147,795
Other comprehensive loss:		
<i>Other comprehensive loss that will not be reclassified to the income statement:</i>		
Re-measurement losses on defined benefit plans, net of tax	(6,222)	(11,403)
Loss on revaluation of premises	(160)	-
Items that will not be reclassified to statement of loss in subsequent periods:	(6,382)	(11,403)
Total other comprehensive loss for the year	(6,382)	(11,403)
Total comprehensive income for the year	31,428	136,392



Republic Bank (Barbados) Limited

(A Subsidiary of Republic Financial Holdings Limited)

SUMMARY NON-CONSOLIDATED STATEMENT OF CHANGES IN EQUITY FOR THE YEAR ENDED 30 SEPTEMBER 2024

(Expressed in thousands of Barbados dollars)

	Stated Capital	Statutory Reserves	Revaluation Reserve	Other Reserves	Retained Earnings	Total
Balance at						
30 September 2022	48,000	48,000	5,004	(25,798)	196,481	271,687
Total comprehensive income for the year	-	-	-	(11,403)	147,795	136,392
Dividends	-	-	-	-	(46,080)	(46,080)
Balance at						
30 September 2023	48,000	48,000	5,004	(37,201)	298,196	361,999
Total comprehensive income for the year	-	-	(160)	(6,222)	37,810	31,428
Transfer to general contingency reserves	-	-	-	8,800	(8,800)	-
Dividends	-	-	-	-	(109,440)	(109,440)
Balance at						
30 September 2024	48,000	48,000	4,844	(34,623)	217,766	283,987

SUMMARY NON-CONSOLIDATED STATEMENT OF CASH FLOWS FOR THE YEAR ENDED 30 SEPTEMBER 2024

(Expressed in thousands of Barbados dollars)

	2024	2023
Net cash used in operating activities	(95,154)	(269,764)
Net cash provided by/(used in) investing activities	25,860	(6,594)
Net cash used in financing activities	(42,431)	(20,942)
Net decrease in cash and cash equivalents	(111,725)	(297,300)
Cash and cash equivalents at beginning of year	417,031	714,331
Cash and cash equivalents at end of year	305,306	417,031
Cash and cash equivalents at end of year are represented by:		
Cash on hand	75,255	33,408
Balance with Central Bank other than mandatory reserve deposits	171,508	309,409
Due from banks and related banks	58,543	74,214
	305,306	417,031



Republic Bank (Barbados) Limited

(A Subsidiary of Republic Financial Holdings Limited)

Note to the Summary Non-Consolidated Financial Statements

Note 1

The summary non-consolidated financial statements are prepared in accordance with criteria developed by management. Under management's established criteria, management discloses the summary non-consolidated statement of financial position, summary non-consolidated statement of income, summary non-consolidated statement of comprehensive income, summary non-consolidated statement of changes in equity and summary non-consolidated statement of cash flows. These summary non-consolidated financial statements are derived from the audited non-consolidated financial statements of Republic Bank (Barbados) Limited for the year ended 30 September 2024, which are prepared in accordance with IFRS Accounting Standards.

Republic Bank (Barbados) Limited Board of Directors:

Karen Yip Chuck – Chairperson, Carlene Seudat – MD & CEO, Donna Every, Debbie Fraser, Geoffrey Roach, Jerry Franklin, L.I. Simone Brathwaite, Riah Dass-Mungal, Robert A. Carter and Andrew McConney



Ernst & Young Ltd
P.O. Box 261
Bridgetown, BB11000
Barbados, W.I.

Tel: 246 430 3900
Fax: 246 426 9551
246 430 3879
www.ey.com

Street Address
One Welches
Welches
St. Thomas, BB22025
Barbados, W.I.

REPORT OF THE INDEPENDENT AUDITOR ON THE SUMMARY NON-CONSOLIDATED FINANCIAL STATEMENTS

TO THE SHAREHOLDER OF REPUBLIC BANK (BARBADOS) LIMITED

Opinion

The summary non-consolidated financial statements, which comprise the summary non-consolidated statement of financial position as at 30 September 2024, the summary non-consolidated statement of income, summary non-consolidated statement of comprehensive income, summary non-consolidated statement of changes in equity and summary non-consolidated statement of cash flows for the year then ended, and related notes, are derived from the complete audited non-consolidated financial statements of Republic Bank (Barbados) Limited for the year ended 30 September 2024.

In our opinion, the accompanying summary non-consolidated financial statements are consistent, in all material respects, with the audited non-consolidated financial statements, on the basis described in Note 1.

Summary Non-Consolidated Financial Statements

The summary non-consolidated financial statements do not contain all the disclosures required by IFRS Accounting Standards applied in the preparation of the audited financial statements of Republic Bank (Barbados) Limited. Reading the summary non-consolidated financial statements and the auditor's report thereon, therefore, is not a substitute for reading the audited non-consolidated financial statements and the auditor's report thereon.

The Audited Non-Consolidated Financial Statements and Our Report Thereon

We expressed an unmodified audit opinion on the audited non-consolidated financial statements in our report dated 6 December 2024.

Management's Responsibility for the Summary Non-Consolidated Financial Statements

Management is responsible for the preparation of the summary non-consolidated financial statements in accordance with Note 1.

Auditor's Responsibility for the Summary Non-Consolidated Financial Statements

Our responsibility is to express an opinion on whether the summary non-consolidated financial statements are consistent, in all material respects, with the audited non-consolidated financial statements based on our procedures, which were conducted in accordance with International Standard on Auditing (ISA) 810 (Revised), Engagements to Report on Summary Financial Statements.

BARBADOS
6 December 2024

Probate Advertisements

NOTICE NO. 7

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

*High Court
Probate Division*

In the Estate of

**MARISA ALIX PETERKIN
also known as ALEX MARISA PETERKIN
also known as MARISA PETERKIN**

Deceased

late of Rendezvous Retreat, Rendezvous
in the parish of Christ Church in this Island

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Probate namely:-

PROBATE of the Will dated the 21st day of October 2003 to the Estate of MARISA ALIX PETERKIN also known as ALEX MARISA PETERKIN also known as MARISA PETERKIN, deceased, late of Rendezvous Retreat, Rendezvous in the parish of Christ Church in this Island, formerly of "Maryville" #6 Club Morgan in the parish of Christ Church in this Island, who died at Rendezvous Retreat, Rendezvous in the parish of Christ Church in this Island on the 20th day of December 2016 by JEAN MARIE MARK the sole Executrix named in the Will of the said Deceased.

An application shall be submitted to the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second notice of advertisement.

Dated this 30th day of January 2025.

TESO LAW
Attorneys-at-Law
"Dormers"
Prior Park, St. James.

NOTICE NO. 8

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court

In the Matter of the Estate of

**GEORGE WHITFIELD LORDE
also known as GEORGE LORDE**

Deceased

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Probate namely:-

PROBATE of the Will dated the 26th day of February, 2024 of GEORGE WHITFIELD LORDE also known as GEORGE LORDE late of Small Land, Bridge Gap, Black Rock in the parish of Saint Michael in this Island, who died at the Queen Elizabeth Hospital, Martindales Road in the parish of Saint Michael in this Island on the 22nd day of July 2024 by SHERRY LORDE the Executrix named in the Will of the deceased.

An Application shall be submitted to the Registrar of the Supreme Court fourteen (14) days from the date of this advertisement to proceed with the above-named application for Probate.

Dated the 30th day of January, 2025.

VINCENT D. WATSON
Attorney-at-Law.

NOTICE NO. 9

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court

In the Estate of

**RITA AILEEN KING also known as
PEGGY KING**

Deceased

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Probate namely:-

PROBATE of the last Will and Testament of the deceased dated the 4th day of June 2014 late of Sandford in the parish of Saint Philip in Barbados who died at Sandford in the parish of Saint Philip on the 12th day of November 2024 by EDMUND RADCLIFFE KING the Executor named in the Will of the said deceased.

An application shall be submitted to the Supreme Court 14 days from the date of Notice in the *Official Gazette* and from the date of the second notice of advertisement.

EDMUND R. KING, SC
Attorney-at-Law.

NOTICE NO. 10

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court

In the Estate of

**ANN LESLEY HADCHITY
also known as ANN HADCHITY**

Deceased

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Probate namely:-

PROBATE of the Will dated the 16th day of December, 2019 of ANN LESLEY HADCHITY also known as ANN HADCHITY deceased late of "Kent

Cottage", Kent in the parish of Christ Church in this Island who died in this Island on the 25th day of December, 2023 by JOHN MICHAEL DAVID HADCHITY the person named as Executor and Trustee in the Will of the said deceased.

An application shall be submitted to the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second Notice of advertisement.

Dated 30th day of January, 2025.

FITZWILLIAM STONE & ALCAZAR
Attorneys-at-Law.

NOTICE NO. 11

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court

In the Estate of

**ELSIE ELAINE HUNTE-PHILLIPS
also known as
ELSIE ELAINE HUNTE**

Deceased

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Probate namely:-

PROBATE of the Will dated the 2nd October, 2020 of ELSIE ELAINE HUNTE-PHILLIPS also known as ELSIE ELAINE HUNTE, late of Dash Valley in the parish of Saint George, who died in this Island on the 7th November, 2023 by MICHAEL LEROY PAYNE and RACHID H.K. PHILLIPS the Executors named in the Will of the said deceased.

An application shall be submitted to the Registrar of the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the second notice of advertisement to proceed with the above-named application for Grant of Probate.

Dated this 30th day of January, 2025.

RECO S.K. BLACKMAN
Attorney-at-Law.

NOTICE NO. 12

BARBADOS

IN THE SUPREME COURT OF JUDICATURE*High Court**In the Matter of the Estate of***PATSY RUTH CARRINGTON also known as
PATSY CARRINGTON***Deceased*

PUBLIC NOTICE is hereby given that application has been made for the following Grant of Probate namely:-

PROBATE of the Will dated the 11th day of August, 2023 of PATSY RUTH CARRINGTON also known as PATSY CARRINGTON, late of No. 2, Rectory Hill in the parish of Saint George in this Island who died at Rectory Hill in the parish of Saint George in this Island on the 6th day of December, 2024, by JOHN STANLEY CARRINGTON, MICHAEL BERTRAM CARRINGTON and BRIAN MARK CARRINGTON the Executors named in the said Last Will and Testament of the deceased.

An Application shall be submitted to the Registrar of the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second notice of advertisement.

BRENT J.A. CHANDLER
Attorney-at-Law.

NOTICE NO. 13

BARBADOS

IN THE SUPREME COURT OF JUDICATURE*High Court**(Probate Division)**In the Estate of***TREVOR ALPHONSO MCKAY**

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Probate namely:-

PROBATE of the Will dated 11th day of December, 2002 of TREVOR ALPHONSO MCKAY late of Crosbys in the parish of Saint George's in the Island of Antigua who died in the parish of St. John in

the Island of Antigua on the 5th July 2011 by HAZEL MYRA HARPER MCKAY the Executrix named in the Will of the deceased.

An application shall be submitted to the Registrar of the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second Notice of this Advertisement.

Dated this 30th day of January, 2025.

IAN C. A. BISHOP
Attorney-at-Law.

NOTICE NO. 14

BARBADOS

IN THE SUPREME COURT OF JUDICATURE*High Court**(Probate Division)**In the Estate of***BRENDA DAISY JOYCE WHITE**

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Probate namely:-

PROBATE of the Will dated 4th day of June, 2009 of BRENDA DAISY JOYCE WHITE late of Roseville Home for the Elderly, Durants Green, Durants in the parish of Christ Church in this Island who died at Roseville Home for the Elderly, Durants Green, Durants in the parish of Christ Church on the 20th January 2018 by HAZEL MYRA HARPER MCKAY the Executrix named in the Will of the deceased.

An application shall be submitted to the Registrar of the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second Notice of this Advertisement.

Dated this 30th day of January, 2025.

IAN C. A. BISHOP
Attorney-at-Law.

NOTICE NO. 15

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court

In the Estate of

ELMA KATHLEEN INNISS

PUBLIC NOTICE is hereby given that an Application is being made for the following Grant of Probate namely:-

PROBATE of the Will dated 6th day of January, 2006 of ELMA KATHLEEN INNISS late of No. 23 Mount Standfast Plantation in the parish of St. James in this Island who died on the 24th April, 2021 at Golden Years Retreat Nursing Home, Golf View Terrace, Golf Club Road in the parish of Christ Church by MARCIA DIANE STABLER the Executrix named in the Will of the deceased.

An application shall be submitted to the Registrar of the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second Notice of this Advertisement.

Dated this 30th day of January, 2025.

IAN C. A. BISHOP
Attorney-at-Law.

NOTICE NO. 16

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court

In the Estate of

ARTHUR STREETLY

PUBLIC NOTICE is hereby given that an Application is being made for the following Grant of Probate namely:-

PROBATE of the Will dated 10th day of February, 2015 of ARTHUR STREETLY late of #34 Bannatyne in the parish of Christ Church in this Island who died on the 16th November, 2017 at the Queen Elizabeth Hospital, by ELIZABETH STREETLY, LAETITIA CHARLOTTE STREETLY

and WILLIAM PAUL STREETLY, the Executors named in the Will of the deceased.

An application shall be submitted to the Registrar of the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second Notice of this Advertisement.

Dated this 30th day of January, 2025.

IAN C. A. BISHOP
Attorney-at-Law.

NOTICE NO. 17

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court

In the Matter of the Estate of

**URCILLE IONE SOBERS also known as
URCILE SOBERS**

Deceased

PUBLIC NOTICE is hereby given that application is being made for the following Grant of Probate namely:-

PROBATE of the Will dated 15th day of February 2022 of URCILLE IONE SOBERS also known as URCILE SOBERS late of Babbs in the parish of St. Lucy who died at Queen Elizabeth Hospital in the parish of St. Michael in this Island on the 1st day of October 2024 by CARL CECIL GREAVES and LINDA IONE HENRY, the Executors named in the Will of the deceased.

An application shall be submitted to the Registrar of the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second notice of advertisement.

Dated this 30th day of January 2025.

EMERSON GRAHAM, K.C.
Attorney-at-Law
65-67 Roebuck Street
Bridgetown.

NOTICE NO. 18

BARBADOS

IN THE SUPREME COURT OF JUDICATURE*High Court**In the Estate of***STANLEY DEVERE WHARTON**

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Administration namely:-

LETTERS OF ADMINISTRATION to the Estate of STANLEY DEVERE WHARTON late of 76 Welches Terrace in the parish of Saint Thomas in this Island, who died in this Island on the 24th day of September 2023 by ROSALIND KATHLEEN THOMPSON, the spouse of the said deceased.

An application shall be submitted to the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second notice of advertisement.

Dated the 30th January 2025.

ANTHONY D. FRANCIS-WORRELL

Attorney-at-Law
Versus Legal
River Road
St. Michael.

NOTICE NO. 19

BARBADOS

IN THE SUPREME COURT OF JUDICATURE*High Court**In the Estate of***MAUREEN DIANA BOWEN also known as
MAUREEN BOWEN***Deceased*

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Administration namely:-

LETTERS OF ADMINISTRATION to the Estate of MAUREEN DIANA BOWEN also known as

MAUREEN BOWEN late of Salmonds in the parish of St. Lucy in this Island who died at Queen Elizabeth Hospital in the parish of St. Michael on the 29th March 2024 by BENTLY TYRON YEARWOOD who is the spouse of the deceased.

An application shall be submitted to the Registrar of the Supreme Court fourteen (14) days from the date of the Notice in the *Official Gazette* and from the date of the second notice of this advertisement.

Dated this 30th day of January 2025.

EMERSON GRAHAM, K.C.

Attorney-at-Law.

NOTICE NO. 20

BARBADOS

IN THE SUPREME COURT OF JUDICATURE*High Court**In the Estate of***LINUS WILLIAM ROOSEVELT ALKINS****also known as****LINUS ALKINS also known****LINUS WILLIAM R ALKINS also known as****LINUS W ALKINS also known as****LINUS WILLIAM ALKINS***Deceased*

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Administration namely:-

LETTERS OF ADMINISTRATION of the Estate of LINUS WILLIAM ROOSEVELT ALKINS also known as LINUS ALKINS also known as LINUS WILLIAM R ALKINS also known as LINUS W ALKINS also known as LINUS WILLIAM ALKINS Deceased late of Hannay's Valley Christ Church, Barbados, who died at the Queen Elizabeth Hospital, St. Michael, Barbados on the 26th day of October 2023 by LORAIN ALEXIS ALKINS the wife of the deceased.

An application shall be submitted to the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second notice of advertisement.

Dated the 30th day of January 2025.

JEPTER LORDE

Attorney-at-Law.

NOTICE NO. 21

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court

In the Estate of

HAROLD WILFRED TROTMAN
also known as HAROLD TROTMAN

Deceased

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Administration namely:-

LETTERS OF ADMINISTRATION to the Estate of HAROLD WILFRED TROTMAN also known as HAROLD TROTMAN deceased, late of 4th Avenue Ventura, Club Morgan in the parish of Christ Church in Barbados who died at 4th Avenue Ventura, Club Morgan in the parish of Christ Church in Barbados on the 23rd day of October 2021 by DORIS TROTMAN, who is the spouse of the deceased.

An application shall be submitted to the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the Second Notice of advertisement.

Dated the 30th day of January 2025.

DANIELLE A. M. HUMPHRIES
Attorney-at-Law.

NOTICE NO. 22

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court
Civil Division
(Probate)

In the Estate of

MARILYN SEBRO-SEALY

Deceased

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Letters of Administration namely:-

LETTERS OF ADMINISTRATION to the Estate of MARILYN SEBRO-SEALY, Deceased late of Lower Thorpes Cottage in the parish of Saint George

in Barbados who died on the 17th day of August, 2014 at Queen Elizabeth Hospital, Martindales Road in the parish of Saint Michael by ANDRE PATRICK ARCHIBALD the nephew of the deceased and JOSETTE BARBARA-ANN ARCHIBALD the niece of the deceased.

An application shall be submitted to the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second notice of advertisement.

Dated this 30th day of January, 2025.

CHANCERY CHAMBERS
Attorneys-at-Law.

NOTICE NO. 23

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court

In the Estate of

DOUGLAS WINFIELD BOYCE
also known as DOUGLAS BOYCE

Deceased

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Letters of Administration namely:-

LETTERS OF ADMINISTRATION to the Estate of DOUGLAS WINFIELD BOYCE also known as DOUGLAS BOYCE late of 2nd Avenue St. Matthias in the parish of Christ Church in this Island, who died at St. Matthias in the parish of Christ Church in this Island on the 23rd day of September 2020 by YVONNE EUDELL WEEKES, who is the daughter of the deceased.

An application shall be submitted to the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second notice of advertisement.

Dated the 30th day of January 2025.

M TARIQ KHAN
Attorney-at-Law.

NOTICE NO. 24

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court

In the Estate of

CARL RICARDO NURSE
also known as CARL NURSE

Deceased

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Letters of Administration namely:-

LETTERS OF ADMINISTRATION to the Estate of CARL RICARDO NURSE also known as CARL NURSE, deceased late of No. 17 Jessamine Avenue, Bayville in the parish of Saint Michael in this Island, who died in the parish of Saint Joseph in this Island on the 11th day of May 2004 by LAMIKA CAROL-ANN JONES, the daughter of the deceased.

An application shall be submitted to the Registrar of the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of the second notice of advertisement.

Dated this 30th day of January 2025.

DEVON O. EDWARDS
Attorney-at-Law.

NOTICE NO. 25

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court

In the Estate of

WASHINGTON ST. ELMO WILLIAMS

Deceased

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Administration namely:-

LETTERS OF ADMINISTRATION to the Estate of WASHINGTON ST. ELMO WILLIAMS of French Village in the parish of St. Peter in this Island who died at Sandy Crest Medical Centre,

Sunset Crest in the parish of St. James on the 3rd October 2017 by CHRISTINE MARJORIE WILLIAMS who is the wife of the deceased.

An application shall be submitted to the Registrar of the Supreme Court fourteen (14) days from the date of the Notice in the *Official Gazette* and from the date of the second notice of this advertisement.

Dated this 30th day of January 2025.

EMERSON GRAHAM, K.C.
Attorney-at-Law.

NOTICE NO. 26

BARBADOS

IN THE SUPREME COURT OF JUDICATURE

High Court

In the Estate of

RUTHIE ELENE PRESCOD
also known as
RUTHIE PRESCOD

Deceased

PUBLIC NOTICE is hereby given that an application is being made for the following Grant of Administration namely:-

LETTERS OF ADMINISTRATION CUM TESTAMENTO ANNEXO to the Estate of RUTHIE ELENE PRESCOD also known as RUTHIE PRESCOD late of Fairview in the parish of Christ Church in this Island who died at Fairview in the parish of Christ Church in this Island on the 12th day of May 2021 by MAURICE ROBERT PRESCOD who is one of the beneficiaries named in the Will dated the 23rd day of April 2012 of the deceased.

An application shall be submitted to the Supreme Court fourteen (14) days from the date of Notice in the *Official Gazette* and from the date of this second notice of advertisement.

Dated this 30th day of January 2025.

TRINITY LAW CHAMBERS
Attorneys-at-Law for the Applicant.

30th January, 2025

FINANCIAL SERVICES COMMISSION

FITNESS & PROPRIETY GUIDELINE



**FINANCIAL SERVICES
COMMISSION**

FITNESS & PROPRIETY GUIDELINE

**This Guideline was issued on December 1st, 2024
pursuant to Section 53 of the Financial Services Commission Act,
2010-10**

CONTENTS

1. Purpose and Scope.....	1
2. Definitions.....	2
3. Who must be Fit and Proper?	3
Groups of Companies.....	5
4. Fit and Proper Test.....	5
Honesty, Integrity and Reputation	7
Competence and Capability	9
Financial Soundness	11
Additional Factors to be Considered	12
5. Obligations of the Financial Institution Regarding Fitness & Propriety	13
6. Assessment of Fitness & Propriety by the Commission.....	14
Assessment of Individuals.....	15
Fit & Proper Documentation for Individuals	16
Assessment of Corporate Bodies.....	16
Fit & Proper Documentation for Corporate Bodies	17
Fitness & Propriety Assessment where there is a Material Change in Circumstances	18
Submission of Documentation	18
Fitness & Propriety Interview	18
Whistleblowing	19
Confidentiality, Disclosure and Maintenance of Information.....	19

1. PURPOSE AND SCOPE

- 1.1 This Guideline aims to establish the expectations of the Financial Services Commission (“the Commission”) as it relates to the fitness and propriety of all relevant persons carrying out any activity regulated by the Commission under the Financial Services Commission Act and its specified enactments.
- 1.2 This Guideline applies to all relevant persons, whether individuals or corporate bodies, registered or licensed by the Commission (“financial institutions”).
- 1.3 This Guideline seeks to ensure that financial institutions understand the importance of fitness and propriety requirements imposed by the Commission, the specific criteria that must be satisfied, and the Commission’s approach to conducting fit and proper assessments.
- 1.4 As part of the overall governance of financial institutions, the Commission requires that financial institutions develop and implement clear policies, procedures and systems to guide the recruitment and appointment of directors, senior officers and other key personnel statutorily required to be fit and proper. More detailed requirements for the recruitment and appointment of such persons can be found under the Corporate Governance Guideline issued by the Commission.
- 1.5 The onus is on each financial institution to establish that the fit and proper criteria are met for each relevant person, and not for the Commission to show otherwise. Where a financial institution is required under this Guideline or the relevant legislation to ensure that a relevant person is fit and proper, the onus is on the financial institution to establish to the satisfaction of the Commission that the fit and proper criteria are met in each instance.
- 1.6 The Commission will assess compliance with this Guideline in a manner and to the extent suitable to the circumstances, considering the financial institution's size, complexity, structure, economic significance, business model, and risk profile, as well as the nature of the relevant person's responsibilities.
- 1.7 This Guideline is designed to provide general guidance and replaces the Commission’s Circular on Fitness & Propriety. However, this Guideline does not replace or override any legislative provisions and should be read in conjunction with other guidance and information issued by the Commission, including:
 - a) FAQs on Fitness & Propriety.
 - b) Guideline No. 2 – Corporate Governance.
 - c) Provisions of the relevant legislation.
 - d) Subsidiary legislation made under the relevant legislation; and
 - e) Written directions, notices, codes, and other Guidelines that the Commission may issue from time to time.

- 1.8 The Commission will review this Guideline periodically or upon the occurrence of an event it considers to be significant in order to ensure continued relevance and adherence to international standards and best practices.
- 1.9 Financial institutions are required to reflect the elements of this Guideline in their internal policies, procedures, and controls and apply this guidance in assessing individuals who manage, control, direct, or perform key functions.

2. DEFINITIONS

2.1 Board of Directors

A body of elected or appointed individuals ultimately responsible for the governance and oversight of a financial institution.

2.2 Board Member or Director

(Interchangeable) A member of the Board of Directors of a financial institution.

2.3 Commission

The Financial Services Commission of Barbados.

2.4 Competent Authority

A person or organisation that possesses a legally delegated authority, capacity or power to perform a designated function in relation to the activities of the relevant person.

2.5 Controlling Shareholder

An individual or corporate body who exercises or controls on their own or together with any person with whom they are acting in concert, 30% or more of the votes able to be cast on all or substantially all matters at general meetings of the company.

2.6 Financial Institution

An institution or a business governed by any of the specified enactments set out in the Second Schedule of the Financial Services Commission Act, 2010, or a credit union.

2.7 Financial Services

Services governed by the relevant legislation along with related subsidiary legislation made under those enactments.

2.8 Insurance Intermediary

Any broker, salesman, agent, sub-agent, adjuster, loss assessor or insurance surveyor.

2.9 Relevant Person

A natural or legal person whose business activity is regulated by the Commission and who is required to be fit and proper.

2.10 Securities Company

As defined under the Securities Act, Cap 318A, including companies that trade in securities, brokers, dealers, underwriters, advisers.

2.11 Self-Regulating Organisation (SRO)

As defined under the Securities Act, Cap318A, including an association of securities companies, a clearing agency, a central securities depository or a stock exchange and the Barbados Stock Exchange.

2.12 Senior Officer

A person who directs, control or manage critical functions within the organisation and or are responsible for key aspects of risk management.

2.13 Senior Management

The individuals or body responsible for managing a financial institution on a day-to-day basis in accordance with strategies, policies and procedures set out by the Board, and all persons responsible for key functions within the organisation, for example the Chief Executive Officer or Chief Financial Officer.

2.14 Shareholder

The collective owners of a financial institution (including the members of a credit union unless otherwise indicated).

2.15 Significant Shareholder

Individual or corporate body who has an interest (or interests) in the voting shares in the corporation of 10% or more.

2.16 Specified Enactments/Relevant Legislation

- a) Financial Services Commission Act, 2010
- b) Insurance Act, Cap 310
- c) Securities Act, Cap 318A
- d) Mutual Funds Act, Cap 320B
- e) The Co-operative Societies Act Cap 37A (insofar as it relates to Credit Unions)
- f) The Occupational Pension Benefits Act Cap350B

3. WHO MUST BE FIT AND PROPER?

3.1 In determining those persons that must satisfy fitness and propriety requirements, the Commission considers the person's function and duties, and not merely their position or level of seniority within the financial institution. Emphasis is placed on whether the person's conduct is most likely to have an impact on the sound and prudent management of the financial institution.

3.2 Below is a non-exhaustive list of relevant persons who are required to meet fit and proper requirements under this Guideline:

- a) Persons who apply to the Commission to be registered or licensed to operate a financial services business or participate in a market regulated by the Commission.

- b) Controlling and significant shareholders of a financial institution (10% or more), whether nominally or beneficially, who operate or seek to operate a financial services business or product regulated by the Commission (and the directors and senior officers of controlling and significant shareholders);
- c) Individuals who make up the Board of Directors of any financial institution regulated by the Commission.
- d) The Managing Director, Chief Executive Officer, Principal Representative or heads of any financial institution, (or similarly titled persons) or any other person holding a senior management position or equivalent persons, of any financial institution regulated by the Commission, including those defined by the relevant legislation.
- e) Financial holding companies.
- f) Acquirers of financial institutions.
- g) Adjusters of financial institutions.
- h) Corporate trustees and the directors of corporate trustees of financial institutions (including occupational pension plans).
- i) Associations of underwriters or a foreign financial institution conducting insurance business or financial services business
- j) The principal representative of an association of underwriters or a foreign financial institution conducting insurance business or financial services business.
- k) Individuals who seek to register and/or operate as insurance intermediaries and any person with whom they are associated, whether as a partner or otherwise, in their business as an insurance intermediary. If the insurance intermediary is a company, each person managing or controlling the company, or each partner as the case may be.
- l) Members of the Supervisory Committee and Credit Committee of credit unions.
- m) Directors of mutual funds (if the mutual fund is a company), partners of the mutual fund (if the mutual fund is a partnership) and trustees (if the mutual fund is a registered unit trust).
- n) Directors and senior officers of mutual fund administrator (if the mutual fund is a company or a society) and partners of the mutual fund administrator (if the mutual fund administrator is a partnership).
- o) Persons who seek to be registered as securities companies, brokers, dealers, traders, underwriters or investment advisers.

- p) Directors and senior officers of Self-Regulatory Organisations (SROs).
 - q) Majority shareholders of reporting issuers (>50%), and where there is no majority shareholder, shareholders who hold 10% or more of the issuer's shares; and
 - r) Board members and senior officers of corporate bodies offering custodian services to financial institutions, or products and services regulated by the Commission.
 - s) Senior employees or persons who direct, control or manage critical functions within the organisation and or are responsible for key aspects of risk management; and
 - t) Auditors and actuaries of financial institutions.
- 3.3 Persons are encouraged to seek guidance from the Commission if they are unsure whether a particular person meets the definition of a relevant person for the purposes of this Guideline.

Groups of Companies

- 3.4 If the financial institution is part of a group of companies, the Commission requires a chart depicting the corporate structure of the group which identifies all the related entities so that direct and indirect shareholders of the financial institution can be identified, along with their percentage shareholding.
- 3.5 However, fit and proper documentation will only be required for Ultimate Beneficial Owners who hold 10% or more interest in the financial institution, and the directors and senior officers of the ultimate parent company. Unless specifically requested by the Commission, fit and proper documentation for every intermediate parent company is not required.

4. FIT AND PROPER TEST

- 4.1 The criteria for considering whether a relevant person is fit and proper include but are not limited to the following:
- a) Honesty, integrity and reputation (Sections 4.6 – 4.7).
 - b) Competence and capability (Sections 4.8 – 4.13); and
 - c) Financial soundness (Sections 4.14 – 4.15).
- 4.2 In the case where the relevant person is a corporate body, to establish that it is fit and proper, a financial institution must satisfy the Commission that:
- a) All of its significant shareholders meet the fit and proper criteria of this Guideline.

- b) Each of its directors and Chief Executive Officer, senior officers or equivalent persons, meet the fit and proper criteria of this Guideline.
 - c) It has in place appropriate recruitment policies, adequate internal control systems and procedures that would reasonably ensure that the persons that it employs, authorises or appoints to act on its behalf, in relation to its conduct of the activity regulated under the relevant legislation, meet the fit and proper criteria of this Guideline. This includes persons with senior management responsibilities and those responsible for key aspects of risk management; and
 - d) Has the financial capacity to adequately carry out its intended functions, and to underwrite the risk to which it is exposed.
- 4.3 In the case where the relevant person is a fund management company, to establish that it is fit and proper, it must satisfy the Commission that:
 - a) All of its significant shareholders or equivalent persons and persons who:
 - (i) Control, directly or indirectly, not less than 10% of the voting power or such equivalent decision-making power in the fund management entity; or
 - (ii) Acquire or hold, directly or indirectly, not less than 10% of the issued shares or such equivalent share of ownership of the fund management entity.meet the fit and proper criteria of this Guideline.
 - b) Each of its key officers meet the fit and proper criteria of this Guideline; and
 - c) It has in place appropriate recruitment policies, adequate internal control systems and procedures that would reasonably ensure that the persons that it employs, authorises or appoints to act on its behalf, in relation to its conduct of the activity regulated under the relevant legislation, meet the relevant fit and proper criteria of this Guideline.
- 4.4 When assessing an application for the appointment of a relevant person to senior or critical functions, the Commission may, in addition to fit and proper criteria set out in this Guideline, consider other factors that may be relevant, such as whether the relevant person has a good standing in the profession in respect of which the application is made.
- 4.5 The following factors will be assessed on a holistic basis. One negative indicator may not alone determine a person's fitness or propriety. Consideration will also be given to lapses of time since a negative indicator took place, the duration or reputation of the negative indicator, as well as its severity, in relation to the activity for which the person is seeking registration, and what actions have been taken in response to the negative indicator.

Honesty, Integrity and Reputation

- 4.6 Honesty, integrity and a good reputation are qualities that are demonstrated over time and demand a disciplined and ongoing commitment to high ethical standards.
- 4.7 Though these factors are not exhaustive, in assessing a relevant person's level of honesty, integrity, and reputation, consideration shall be given to whether the person:
- a) Has been refused the right or restricted in its or his right to carry on any trade, business, or profession for which a specific license, registration, or other authorisation is required by law in any jurisdiction.
 - b) Has been issued a prohibition order under any Act administered by the Commission or has been prohibited from operating in any jurisdiction by any financial services' regulatory authority.
 - c) Has been censured, disciplined, suspended, or refused membership or registration by the Commission, any other regulatory authority, an operator of a market, trade repository, or clearing facility, or any professional body or government agency, whether in Barbados or elsewhere.
 - d) Has been the subject of any formal complaint made to a competent authority made reasonably and in good faith, relating to activities that are regulated by the Commission or under any law in any jurisdiction.
 - e) Has been the subject of any proceedings of a disciplinary or criminal nature or has been notified of any potential proceedings or of any investigation which might lead to those proceedings, under any law in any jurisdiction.
 - f) Has been convicted of any offence or is being subject to any pending proceedings (particularly those involving dishonesty, fraud, breach of trust, money laundering, theft, or other financial crime) which may lead to such a conviction under any law in any jurisdiction.
 - g) Has had any judgment (in particular, that associated with a finding of fraud, misrepresentation, or dishonesty) entered against the relevant person in any civil proceedings or is a party to any pending proceedings which may lead to such a judgment, under any law in any jurisdiction.
 - h) Has accepted civil liability for fraud or misrepresentation under any law in any jurisdiction.
 - i) Has had any civil penalty enforcement action taken against it or him by the Commission or any other regulatory authority under any law in any jurisdiction.
 - j) Has contravened or abetted another person in breach of any laws or regulations, business rules or codes of conduct, whether in Barbados or elsewhere.

- k) Has been the subject of any investigations or disciplinary proceedings or been issued a warning or reprimand by the Commission, any other regulatory authority, an operator of a market, trade repository or clearing facility, any professional body or government agency, whether in Barbados or elsewhere.
- l) Has been refused a fidelity or surety bond, whether in Barbados or elsewhere.
- m) Has demonstrated an unwillingness to comply with any regulatory requirement or to uphold any professional and ethical standards, whether in Barbados or elsewhere.
- n) Is showing, or has shown at any time, a strong objection or lack of willingness to maintain effective internal control systems and risk management practices.
- o) Has been untruthful or provided false or misleading information to the Commission or been uncooperative in any dealings with the Commission or any other regulatory authority in any jurisdiction; and
- p) In addition to sub-paragraphs (a) to (o), where the relevant person is an individual:
 - (i) Is or has been a director, partner, significant shareholder, or concerned in the management of a business that has been censured, disciplined, prosecuted, or convicted of a criminal offence or been the subject of any disciplinary or criminal investigation or proceeding, in Barbados or elsewhere, in relation to any matter that took place while the person was a director, partner, significant shareholder or concerned in the management of the business;
 - (ii) Is or has been a director, partner, significant shareholder or concerned in the management of a business that has been suspended or refused membership or registration by the Commission, any other regulatory authority, an operator of a market, trade repository or clearing facility, any professional body or government agency, whether in Barbados or elsewhere.
 - (iii) Has been a director, partner, significant shareholder or concerned in the management of a business that has gone into insolvency, liquidation or administration during the period when, or within a period of one year after, the relevant person was a director, partner, significant shareholder or concerned in the management of the business, whether in Barbados or elsewhere.
 - (iv) Has been dismissed or asked to resign from —
 - (A) office.
 - (B) employment.

(C) a position of trust; or.

(D) a fiduciary appointment or similar position, whether in Barbados or elsewhere.

due to questions related to fitness and propriety.

- (v) Is, or has ever been, involved in any business or other relationship which could materially pose a conflict of interest or interfere with the exercise of good judgment when exercising a regulated function which would be disadvantageous to the interests of the financial institution or conversely advantageous to the relevant person.
- (vi) Is or has been subject to disciplinary proceedings by his current or former employer(s) due to questions of honesty, integrity or reputation, whether in Barbados or elsewhere.
- (vii) Has been disqualified from acting as a director, or disqualified from acting in any managerial capacity, whether in Barbados or elsewhere; and
- (viii) Has been an officer found liable for an offence committed by a body corporate as a result of the offence having proved to have been committed with the consent or connivance of, or neglect attributable to, the officer, whether in Barbados or elsewhere.

Competence and Capability

4.8 Competency and capability are demonstrated when a relevant person possesses the relevant knowledge, experience and ability to understand the technical requirements of the business, objectivity in decision making, as well as keen awareness of the inherent risks and the management processes required to effectively perform a regulated function.

4.9 Though these factors are not exhaustive, in assessing a relevant person's level of competence and capability, consideration shall be given to:

- a) Whether the relevant person has satisfactory past performance or expertise, having regard to the nature of the relevant person's business or duties demonstrated by experience through years of employment and positions held, as the case may be, whether in Barbados or elsewhere.
- b) Whether the relevant person has a high level of understanding in his professional area of expertise and other areas that might affect the business of the financial institution including financial markets, the regulatory and legal environment, strategic and business planning, risk management practices, accounting and auditing, understanding financial statements and corporate governance.

- c) Where the relevant person is an individual who is assuming concurrent responsibilities, whether such responsibilities would give rise to a conflict of interest or otherwise impair his ability to discharge his duties in relation to any activity regulated by the Commission under the relevant legislation.
- d) In relation to a relevant person whose activity is regulated by the Commission under the relevant legislation and where the relevant person is an institution, whether its directors or equivalent persons, Chief Executive Officer or equivalent person, the persons that it employs, authorises or appoints to act on its behalf, in relation to its conduct of the activity regulated under the relevant legislation, where applicable, have satisfactory educational qualifications, training, skills or practical experience, whether in Barbados or elsewhere;
- e) In relation to a relevant person whose activity is regulated by the Commission, whether the representative of the relevant person has satisfactory educational qualification or experience, relevant skills and knowledge, whether in Barbados or elsewhere, having regard to the nature of the duties they are required to perform.
- f) In relation to a relevant person whose activity is regulated by the Commission under the Insurance Act, Cap. 310, whether the broking staff of the relevant person has satisfactory relevant qualification or experience, whether in Barbados or elsewhere, having regard to the nature of the duties he is to perform.

4.10 The above factors will be considered considering:

- a) The main activity conducted by the financial institution;
- b) The nature, complexity and volume of the business;
- c) The jurisdictions in which products and services will be offered; and
- d) The level of responsibility.

4.11 The financial institution's Board, either in whole or delegated to a committee, must comprehensively assess candidates' competence and capability, ensuring they have the appropriate qualifications, training, skills and practical experience to effectively fulfil the roles and responsibilities of the proposed position.

4.12 In assessing the competence and capability of a corporate body (separate from the Board of Directors, significant shareholders and senior officers being assessed individually according to the criteria enumerated above), the Commission will seek to understand the company's corporate structure to ensure it has the right skills and resources in place to execute its responsibilities.

4.13 A relevant person that is a corporate body must provide:

- a) A diagram depicting the group structure (where relevant) showing shareholding percentages.
- b) The corporate body's organisational chart.
- c) Completed Corporate Fitness & Propriety Questionnaire; and
- d) Copies of approved statutory filings regarding ownership of the entity.
- e) Copies of the HR recruitment and retention plan (if relevant), and assessment of its compensation plan to ensure that there are no perverse incentives built into the framework.
- f) A copy of the internal Fitness & Propriety Policy along with related procedures for all relevant persons.

Financial Soundness

- 4.14 The assessment of financial soundness is aimed at determining whether the relevant person can meet its/his personal liabilities when they become due and mitigate financial risks on a continuous basis. Financial integrity and soundness are demonstrated by a person who manages its/his own financial affairs properly and prudently or those of an entity in which he had a controlling interest or was involved at a managerial level. Financial means will not, in itself, be a determining factor in the measure of financial soundness.
- 4.15 Though these factors are not exhaustive, in assessing a relevant person's financial soundness, consideration will be given to whether the relevant person:
- a) Is or has been unable to fulfill any of its or his financial obligations, whether in Barbados or elsewhere;
 - b) Has entered into a compromise or scheme of arrangement with its or his creditors or made an assignment for the benefit of its or his creditors, being a compromise or scheme of arrangement or assignment that is still in operation, whether in Barbados or elsewhere.
 - c) Is subject to a judgment debt which is unsatisfied, either in whole or in part, whether in Barbados or elsewhere.
 - d) Has met applicable capital and/or solvency requirements.
 - e) In addition to sub-paragraphs (a) to (c), in the case where the relevant person is an individual:
 - (i) Is or has been the subject of a bankruptcy petition, whether in Barbados or elsewhere.
 - (ii) Has been adjudicated as bankrupt and the bankruptcy is undischarged, whether in Barbados or elsewhere; or

- (iii) Is or has been subject to any other process outside Barbados that is similar to those referred to in subparagraph (i) and (ii); and
- f) In addition to sub-paragraphs (a) to (c), in the case where the relevant person is a corporate body:
 - (i) Is or has been the subject of a winding up petition, whether in Barbados or elsewhere.
 - (ii) Is in the course of being wound-up or otherwise dissolved, whether in Barbados or elsewhere.
 - (iii) Is or has been a corporation where a receiver, receiver and manager, judicial manager, or such other person having the powers and duties of a receiver, receiver and manager, or judicial manager, has been appointed, in relation to, or in respect of any property of, the corporation, whether in Barbados or elsewhere; or
 - (iv) Is or has been subject to any other process outside Barbados that is similar to those referred to in sub-paragraphs (i) to (iii).

Additional Factors to be Considered

- 4.16 In addition to the factors enumerated above, the following areas will also be considered when assessing persons for appointment to the management body of a financial institution:
- a) *Conflicts of interest*: financial institutions must be guided by Section 6.9 of the Corporate Governance Guideline issued by the Commission, which sets out the responsibilities of the Board and senior management in relation to conflicts of interest. An existing conflict of interest does not itself deem a relevant person unfit or improper for a particular role. Still, any actual or potential conflict must be effectively monitored, managed, and/or mitigated as appropriate to the situation and subject to the internal Conflicts of Interest Policy of the financial institution. The financial institution should reconsider the appointment if a conflict cannot be appropriately managed or mitigated. Information regarding conflicts of interest must be made available to the Commission upon request.
 - b) *Time commitment*: directors of financial institutions must be able to commit sufficient time to their duties. Their current employment impacts this with its related level of responsibility and accountability, the number of directorships or other employments being simultaneously undertaken, the location of these duties, as well as other professional commitments and circumstances. Additional learning and development should also form part of the relevant person's time commitment, as well as their ability to adequately respond to urgent circumstances.

- c) *Collective suitability*: financial institutions must be guided by Section 5 of the Corporate Governance Guideline issued by the Commission which sets out the requirements for the structure and composition of the Board. The Board must have an appropriate mix of skills, knowledge and experience to effectively conduct the financial institution's business. Individuals are therefore required to complement the existing Board and fill any gaps that may exist in these areas.

5. OBLIGATIONS OF THE FINANCIAL INSTITUTION REGARDING FITNESS & PROPRIETY

- 5.1 When a financial institution seeks to appoint or engage a person (whether an individual or a corporate body) to perform a regulated function, it is the responsibility of the financial institution to satisfy the Commission that the person is fit and proper to perform the function for which they are being appointed or engaged. Financial institutions are therefore required to ensure that persons are not appointed to nor continue in positions of responsibility for which they are not fit and proper.
- 5.2 To this end, each financial institution's Board of Directors is required to establish and approve an appropriate internal Fitness & Propriety Policy along with related procedures for all relevant persons. This policy must be in line with the provisions of this Guideline.
- 5.3 The management of each financial institution must then implement this policy and related procedures as outlined by the Board in an effective and comprehensive manner, with the board exercising oversight functions to ensure compliance.
- 5.4 This internal Fitness & Propriety Policy must provide for a detailed assessment of candidates for fitness and propriety at the recruitment stage and on an ongoing basis at least annually. The policy must also require that the financial institution:
 - a) Verifies qualifications, experience, references, and professional memberships;
 - b) Conducts probity checks on criminal history, legal proceedings, sanctions, and similar matters; and
 - c) Otherwise satisfies itself of the candidate's good character, integrity, competence and capability for the particular function.
- 5.5 These assessments must be documented to provide evidence of what was done to determine the candidate's suitability. Internal assessments must be made available to the Commission upon request.
- 5.6 Internal assessments will also assist in ensuring that material disclosures related to fitness and propriety are made to the financial institution, and thereafter to the Commission.
- 5.7 Once a financial institution determines that an individual is not fit and proper for the position, the financial institution must:

- a) Refuse to appoint that person, or if they are already appointed, terminate their appointment; or
 - b) Redefine the person's responsibilities or suspend the appointment until the person receives adequate training or experience or resolves the relevant conflict, as the case may be.
- 5.8 If a financial institution believes that a person has information that is likely to be material to a fit and proper assessment that it has not been able to obtain, it is required to discuss the matter with the Commission.

6. ASSESSMENT OF FITNESS & PROPRIETY BY THE COMMISSION

- 6.1 The onus is on each relevant person to establish that it or he is a fit and proper person. This is a continuing obligation, and relevant persons must demonstrate (by submitting the applicable documentation) that they remain fit and proper for the duration of their appointment or operations.
- 6.2 The Commission will also conduct its own assessment of the fitness and propriety of relevant persons, whether individuals or corporate bodies. Assessment of fitness and propriety by the Commission takes place:
- a) Upon initial application for registration or licensing of the individual or corporate body.
 - b) Upon the appointment of a new director or senior officer of a financial institution.
 - c) When a person acquires a significant interest in a financial institution.
 - d) Whenever there is a material change in circumstances of relevant persons previously deemed fit and proper that may negatively impact their fitness and propriety; and
 - e) Every three (3) years once relevant persons continue to operate or carry out regulated business.
- 6.3 It must be noted that while there are some common criteria, the fit and proper test applied to legal persons such as corporate shareholders and other companies will differ in some respects from that applied to natural persons who perform regulated activities.
- 6.4 The factors set out above will be considered individually and on a cumulative basis according to their relative importance. Failure to meet one factor may not, on its own, constitute a failure to meet the fit and proper criteria.
- 6.5 The Commission's approach will be informed by all available information taken together, including new information as it becomes available.

- 6.6 If the relevant person fails to satisfy the Commission that it or he is fit and proper, the Commission may refuse the person's application, revoke the person's authorisation or exemption, or take other appropriate regulatory action, as may be applicable and necessary.

Assessment of Individuals

- 6.7 This section is required to be complied with by:
- a) Controlling and significant shareholders of a financial institution (whether nominally or beneficially) who operate or seek to operate a financial services business or product regulated by the Commission (and the directors and officers of controlling and significant shareholders if they are corporate bodies).
 - b) Persons who apply to the Commission to be registered or licensed to operate a financial services business or participate in the market regulated by the Commission;
 - c) Individuals who make up the Board of Directors of any financial institution regulated by the Commission.
 - d) The Managing Director, Chief Executive Officer, Principal Representative or heads of any financial institution (or similarly titled persons), regulated by the Commission.
 - e) Senior officers of any financial institution regulated by the Commission as defined by the relevant legislation.
 - f) Board of Directors and senior officers of holding companies.
 - g) Acquirers of financial institutions.
 - h) Adjusters of financial institutions.
 - i) The principal representative of an association of underwriters or of a foreign financial institution conducting insurance business or financial services business.
 - j) Individuals who are registered and/or operate or seek to register and/or operate as insurance intermediaries, and any person with whom they are associated, whether as a partner or otherwise in their business as an insurance intermediary. If the insurance intermediary is a company, each person managing or controlling the company, or each partner as the case may be.
 - k) Members of the Supervisory Committee and Credit Committee of credit unions.
 - l) Directors and senior officers of mutual fund administrators where the administrator is a company.

- m) Individuals who are registered or seek to be registered as securities brokers, dealers, traders, underwriters or investment advisers.
- n) Directors, executives and senior officers of Self-Regulatory Organisations (SROs).
- o) Board members and senior officers of corporate bodies offering custodian services to financial institutions or products and services regulated by the Commission; and
- p) Auditors and actuaries of financial institutions.

Fit & Proper Documentation for Individuals

6.8 The following are required to be filed with the Commission upon prospective appointment or upon initial application for registration or licensing by the above-mentioned individuals:

- a) A completed Individual Fitness & Propriety Questionnaire.
- b) An up-to-date résumé containing details of the professional background of the individual (not required for ultimate beneficial owners).
- c) Certified copies of qualifications listed on résumé.
- d) A certified copy of the individual's passport picture page; and
- e) A valid original Police Certificate of Character (certificate) from every jurisdiction in which the individual has resided in the prior 10 years, or an Affidavit where a certificate cannot be obtained from the country of residence (issued within the last three (3) months).

6.9 Regarding external auditors and actuaries, the Commission will only require a completed Auditor/Actuary Fitness & Propriety Questionnaire.

6.10 The Commission may request additional information on case-by-case basis as part of an enhanced Fitness & Propriety Assessment. This may involve requiring the individual to provide a credit report issued from jurisdictions in which he/she has operated.

Assessment of Corporate Bodies

6.11 This section is required to be complied with by relevant persons which are corporate bodies, including:

- a) Controlling and significant shareholders of a financial institution (10% or more), whether nominally or beneficially, who operate or seek to operate a financial services business or product regulated by the Commission.
- b) Persons who apply to the Commission to be registered or licensed to operate a financial services business or participate in the market regulated by the Commission.

- c) Financial holding companies;
- d) Acquirers of financial institutions.
- e) Adjusters of financial institutions.
- f) Corporate trustees of financial institutions (including occupational pension plans).
- g) Associations of underwriters or a foreign financial institution conducting insurance business or financial services business.
- h) Any company operating or seeking to operate as an insurance intermediary.
- i) Mutual fund administrators that are companies.
- j) Persons who are registered or seek to be registered as securities brokers, dealers or underwriters or investment advisers.
- k) Majority shareholders of reporting issuers (>50%), and where there is no majority shareholder, shareholders who hold 10% or more of the issuer's shares; and
- l) Auditors and actuaries of financial institutions.

6.12 The information gathered during assessment will aid in determining the current solvency position of the company, past performance and financial management, and overall, whether previous business dealings were conducted in a sound and prudent manner.

Fit & Proper Documentation for Corporate Bodies

6.13 The following are required to be filed with the Commission upon application for registration or licensing of a corporate body:

- a) A completed Corporate Fitness & Propriety Questionnaire.
- b) Copies of audited financial statements of the company for the three (3) consecutive years immediately preceding its application or for each year it has been in operation if less than three years.
- c) (For new/proposed relevant persons who are corporate bodies) proforma financial statements for the next three (3) years (Note: The Commission, at its discretion may require that the proposed proforma statements be reviewed by an auditor).
- d) Copies of credit rating reports, business plans, feasibility studies, and due diligence reports if applicable.
- e) Copies of the Management Letters from the external auditors for the past three fiscal periods (if applicable).

- f) Evidence of financial resources such as bank/financial institution statements or source of funds statements where the documents listed in (b) and (d) are not available.
 - g) Copies of the last two reports of examinations conducted by the relevant regulatory authority (if applicable); and
 - h) Any other information the Commission deems necessary.
- 6.14 The Commission may request additional information on a case-by-case basis as part of an enhanced Fitness & Propriety Assessment. This may involve requiring the corporate body to provide a credit report issued from jurisdictions in which it has operated.

Fitness & Propriety Assessment where there is a Material Change in Circumstances

- 6.15 Where there is a material change in information that may negatively impact a relevant person's fitness and propriety, relevant persons must comply with the Commission's Material Changes Guideline.
- 6.16 Where this material change concerns information filed on the Individual Fitness & Propriety Questionnaire or the Corporate Fitness & Propriety Questionnaire, an updated questionnaire must be submitted to the Commission.

Submission of Documentation

- 6.17 Documents submitted in support of an application must be in English. Where the original documents are in a foreign language, an independently authenticated translation must be provided, i.e., a translation by a professional translator with the full name, address, contact information and signature of the translator and the date of the translation.
- 6.18 The completed fit and proper documentation must be submitted to the Commission's Supervision and Regulation Division. In the case of documentation submitted in respect of an application for registration or licensing, the entire application package, together with fit and proper documentation, should be submitted to the Supervision and Regulation Division.
- 6.19 Where a third party is submitting the fit and proper documentation on behalf of a regulated entity or person (for e.g., in the case of a licensing application when an attorney or other representative is submitting the application), the third party shall obtain and submit all relevant information as required and ensure that only complete applications are submitted to the Commission.

Fitness & Propriety Interview

- 6.20 If the Commission has a concern about the fitness and propriety of a particular candidate slated for appointment as a director or officer of a financial institution, the Commission may request an interview with that individual.

- 6.21 Such an interview gives the Commission an opportunity to probe the candidate about his qualifications and practical experience, as well as the extent of his knowledge about the financial institution, relevant market development and his understanding of his role and responsibilities.
- 6.22 These interviews may also be used to explore any issues of integrity and propriety including conflicts of interest, and the Commission may query facts or seek to verify other information to gain more assurance about the specific elements of that person's fitness and propriety.
- 6.23 The Commission may also conduct interviews where it is concerned about a relevant person's ability to perform its or his regulated function, or where it becomes aware of new information that may impact that person's fit and proper assessment. An interview is also the likely next step where additional information requested from the financial institution was not satisfactory to allay the Commission's concerns.
- 6.24 If the Commission determines that an interview should be conducted, it will provide the relevant person and/or the financial institution with reasonable written notice, stating the date, time and location of the requested interview.
- 6.25 As part of the interview process, the Commission may issue the relevant person with a statement detailing the Commission's concerns or issues and providing a timeframe for the person to respond, either verbally or in writing, to the statement. This reply will be considered by the Commission before it makes a final determination as to the person's fitness and propriety.

Whistleblowing

- 6.26 The financial institution must ensure that it does not prohibit any person, directly or indirectly from disclosing information or providing documents to the Commission on the fitness and propriety of a prospective relevant person or a person approved to perform a regulated function.

Confidentiality, Disclosure, and Maintenance of Information

- 6.27 All information submitted or otherwise obtained by the Commission, including documentation, will be maintained in a strictly confidential manner. Internal disclosure of information will be restricted accordingly.
- 6.28 Disclosure of information to external persons will only be undertaken as permitted by the law.
- 6.29 A central database containing details of the persons who have been assessed will be maintained by the Commission's Supervision and Regulation Division. The database eliminates the need for individuals to re-submit documentation multiple times in respect of further applications or approvals. If there has been a material change in the information initially disclosed, further disclosures, including the completion of a revised questionnaire, may be required to update the database.

30th January, 2025

FINANCIAL SERVICES COMMISSION

TECHNOLOGY AND CYBER RISK MANAGEMENT GUIDELINE



Technology and Cyber Risk Management Guideline

**This Guideline was issued on December 1st, 2024
pursuant to Section 53 of the Financial Services Commission Act,
2010-10**

Table of Contents

Purpose and Scope	4
1. Glossary of Terms	5
2. Technology and Cyber Risk Management- Governance and Oversight	8
(A) Role of the Board of Directors and Senior Management	8
(B) The Establishment of Standard Operating Procedures (SOPs)	9
(C) Information Asset Management	10
(D) Outsourcing	10
(E) Competency of Staff and other Personnel	10
(F) IT Security Awareness and Training	11
3. Risk Management Framework- Technology and Cyber Security	12
(A) Risk Management Framework	12
(B) Components of the Technology and Cyber Risk Management Framework	12
i. Technology and Cyber Risk Identification	12
ii. Technology and Cyber Risk Penetration Testing (PT)	12
iii. Technology and Cyber Risk Assessment	13
iv. Technology and Cyber Threat Exercises	13
v. Technology and Cyber Risk Adversarial Attack Simulation Exercise	13
vi. Technology and Cyber Risk Remediation Management	14
vii. Technology and Cyber Risk Monitoring, Review and Reporting	14
viii. Technology and Cyber Risk Intelligence and Information Sharing	15
4. Management of Technology Services	15
(A) Project Management Framework	15
(B) System Acquisition	16
(C) System Development Life Cycle (SDLC)	16
(D) System Requirements Analysis	17
(E) System Design and Implementation	17
(F) System Testing	18
(G) Quality Assurance and Control	18
(H) Technology Configuration and Refresh Management	18
(I) Patch Management	19
(J) Change and Release Management	19
(K) Incident and Problem Management	19
5. Technology Resilience	20
(A) System Availability	20

(B)	Disaster Recovery	21
6.	Access Rights and System Privileges	21
(A)	User Access Rights.....	21
(B)	Privileged Access Rights	22
(C)	Remote Access Rights.....	22
7.	Data and Infrastructure Security	23
(A)	Data Security.....	23
(B)	Network Security	23
(C)	System Security	24
(D)	Electronic Information Assets	25
8.	Online Financial Services	25
(A)	Secure Online Financial Services	25
(B)	Automated Teller Machines (ATMs) and Payment Card Security (Credit and Debit Cards) 26	
(C)	Customer Verification for Online Transactions	26
(D)	Fraudulent Online Transaction Management	27
9.	IT Audit.....	28
(A)	Audit Function	28
10.	Technology and Cyber Security Incident Reporting	28
(A)	Criteria for Reporting to the Commission	28
(B)	Notification Requirements	30
(C)	Failure to Report to the Commission.....	30

Purpose and Scope

This guideline establishes the Financial Services Commission's (the "Commission") regarding technology and cyber risk management. It applies to all financial institutions (FIs) the Commission regulates and aims to develop greater resilience to technology and cyber risks.

The extent and degree to which FIs implement this guideline should be proportional to the level of risk and complexity of the services offered and the technologies supporting such services.

This guideline is effective December 01st 2024

1. Glossary of Terms

Adversarial Attack Simulation Exercise

Planned cyber security assessments that simulate attacks against people, processes and technology underpinning a company's critical business functions or services.

Biometric Technologies

The use of technology to identify a person based on some aspect of their biology such as voice patterns and facial recognition.

Bring Your Own Device (BYOD)

A policy that allows employees in a company to use their personal devices, such as laptops and tablets, to access work-related systems, such as corporate emails and other software applications.

Cyber Event

An actual or suspected unauthorized system access that aims to control a company's online servers through various techniques.

Cyber Incident

A breach of a company's system security policy through methods such as social engineering, man-in-the-middle attacks, and denial of service attacks.
--

Cyber-range

An interactive, simulated representation of a company's system that is connected to a simulated internet environment to facilitate the training of potential cybersecurity professionals.

Cybersecurity Risk

The potential adverse impact on a company's operations through unauthorized access to its IT systems, which can result in the possibility of failure, disruption, modification, or destruction of the company's IT systems and/or the data contained therein.

Data Confidentiality

The protection of sensitive or confidential data such as customer details from unauthorized access and disclosure.
--

Data Loss Prevention (DLP)

Data loss prevention- sometimes called data leak prevention or information loss prevention- is a security solution that identifies and helps prevent unsafe or inappropriate sharing, transfer, or use of sensitive data. It can help your organization monitor and protect sensitive information across on-premises systems, cloud-based locations, and endpoint devices.
--

Denial of Service (DoS) A type of cyber-attack aimed at preventing an authorized user from accessing resources such as networks, websites, or other online services.
Domain name system hijacking (DNS) A cyber-attack technique where a cyber-criminal redirects authorized users to malicious sites.
Endpoint Detection and Response (EDR) Software designed to automatically protect an organization's end users, endpoint devices, and IT assets against cyber threats that get past antivirus software and other traditional endpoint security tools.
Fraudulent Online transactions The unauthorized use of an individual's confidential information to conduct transactions or payments via the Internet.
General-purpose device A device such as a desktop computer, laptop, or mobile device, designed to install software applications.
Hardware The physical aspects of a computer or a related device such as a keyboard, printer, motherboard etc.
Information/Technology Asset The hardware and software within a company's IT environment that supports the provision of its technological services.
Least Privilege A principle where access rights and system privileges are granted based on job responsibility.
Man-in-the-middle attack (MITMA) A type of cyber-attack where cyber criminals secretly intercepts and transmit messages between an authorized user and an application to steal personal information such as account details, credit card numbers etc.
Multi-factor Authentication (MFA) An authentication method that requires an authorized user to provide two or more verification factors to gain access to a company's resources such as online banking.
Online Financial Services

A mechanism that allows authorized users to conduct financial transactions such as online banking and online trading via the Internet.

Segregation of duties

A principle that divides crucial IT functions among the different staff members to ensure that no one individual has enough information or access privileges to execute damaging fraud.

Social Engineering

A process where cyber criminals manipulate innocent persons into disclosing confidential information such as passwords and banking information.

Software

The applications and programs used to operate and execute tasks on computers and other related devices.

System Development life cycle (SDLC)

SDLC is a process that provides a framework for executing a company's system. Its seven steps include planning, system analysis and requirements, system design, development, integrating and testing, implementation, and operations and maintenance.

System Testing

A method used to validate the software specifications through the evaluation of corresponding requirements.

Table-top Exercise

A discussion-based exercise where the participants of a simulated emergency scenario meet to validate the content of the scenario.

Technology Risk

A type of business risk related to the malfunctioning or disruption of a company's IT functions as it relates to the people or processes that enable and support the company's needs and can result in financial loss.

2. Technology and Cyber Risk Management- Governance and Oversight

(A) Role of the Board of Directors and Senior Management

- (1) The board of directors and senior management of FIs should ensure that:
 - a. The tone is set from the top and a strong culture of technology risk awareness and management is cultivated at all levels of staff within the FI.
 - b. Effective internal controls and risk management practices are implemented to achieve security, reliability and resilience of its Information Technology (IT) operating environment.
 - c. A Chief Information Officer, Chief Technology Officer or Head of IT and a Chief Information Security Officer or Head of Information Security with the relevant skill set and experience are appointed. The Chief Executive Officer should minimally approve the appointments.
 - d. The appointed person referred to in point (c) above, should at a minimum:
 - i. Implement and oversee the FI's cyber security program.
 - ii. Manage and monitor Incident Response Activities.
 - iii. Promote a robust information security culture within the FI.
 - iv. Oversee the FI's IT & Cybersecurity personnel and ensure adequate training and awareness of the general staff complement.
 - e. A technology and cyber risk management strategy is established and implemented.
 - f. Key IT decisions are made in accordance with the FI's risk tolerance.
- (2) The board of directors or a committee delegated by it should:
 - a. Ensure that a sound and robust risk management framework is established and maintained to manage technology and cyber risks.
 - b. Ensure that there is a technology and cyber risk management function such as a Risk Officer to govern the technology and cyber risk management framework and strategy, as well as to provide an independent view of the technology and cyber risks faced by the FI.
 - c. Provide senior executives who are responsible for executing the FI's technology and cyber risk management strategy with sufficient authority, resources and access to the board of directors.

- d. Approve the risk tolerance statement that expresses the nature and extent of technology and cyber risks that the FI is willing and able to assume.
- e. Undertake regular periodic reviews of the technology and cyber risk management strategy for continued relevance.
- f. Assess management competencies for managing technology and cyber risk; and
- g. Establish an independent audit function to assess the effectiveness of controls, risk management and governance of the FI and report to the Board.

(3) Senior management is required to:

- a. Establish the technology and cyber risk management framework and strategy.
- b. Manage technology and cyber risks based on the established framework and strategy.
- c. Ensure sound and prudent policies, standards and procedures for managing technology and cyber risks are established and maintained and that standards and procedures are implemented effectively.
- d. Appoint a Risk Officer with the relevant skillset and experience. The role of the risk officer may be carried out by a function or a group of functions within the FI, who should be authorized to manage technology and cyber security risks.
- e. Ensure the roles and responsibilities of staff are outlined clearly in managing technology and cyber risks; and
- f. Notify the board of directors of significant and adverse technology and cyber risk developments and incidents that are likely to have a substantial impact on the FI and its customers.

(B) The Establishment of Standard Operating Procedures (SOPs)

- (1) An FI should establish SOPs and, where applicable, incorporate industry standards and best practices to manage technology risks and safeguard information assets in the FI.
- (2) The SOPs should also be regularly reviewed and updated, taking into consideration the evolving technology and cyber threat landscape.
- (3) The FI should review and assess risks associated with deviations thoroughly. The risk assessment should be approved by senior management, and approved deviations should be reviewed periodically to ensure that residual risks remain at an acceptable level.

- (4) Compliance processes should be implemented to verify that SOPs are observed. These include follow-up processes for non-compliance.

(C) Information Asset Management

- (1) To have an accurate and complete view of its IT operating environment, an FI should establish information asset management practices that include the following:
 - a. Identification of information assets that support the FI's business and delivery of its services.
 - b. Classification of an information asset based on its security classification or criticality.
 - c. Ownership of information assets, and the roles and responsibilities of the staff managing the information assets; and
 - d. Establishment of SOPs to manage information assets according to their security classification or criticality.
- (2) An FI should maintain a log of its information assets. The log should be reviewed regularly and updated whenever there are changes to the quantity of information assets.

(D) Outsourcing

- (1) An FI should assess and manage its exposure to technology and cyber risks that may affect the confidentiality, integrity and availability of its IT systems and data at a third party prior to entering into a contractual agreement or partnership.
- (2) On an ongoing basis, the FI should ensure the third-party service provider employs a high standard of care and diligence in protecting data confidentiality and integrity as well as ensuring system resilience.
- (3) Sub-outsourcing refers to a situation where an FI's service provider under an outsourcing arrangement further transfers a process, service or activity (or parts thereof) to another service provider. In this instance FIs should conduct rigorous due diligence to ensure compliance with regulatory requirements and the FI's IT security policy.

(E) Competency of Staff and other Personnel

- (1) The FI should ensure all staff, including contractors and service providers, have the requisite competence and skills to perform their IT functions and manage technology and cyber risks.
- (2) A background check on all personnel who have access to the FI's data and IT systems should be performed to minimize insider threat.
- (3) The FI should ensure that members of staff, vendors and contractors authorized to access their systems are also in compliance with their information system security policy.

(F) IT Security Awareness and Training

- (1) A comprehensive IT security awareness training program should be established to maintain a high level of awareness among all staff in the FI. The content of the training program should at a minimum include information on the current cyber threat environment and its implications, the FI's SOPs, as well as an individual's responsibility to safeguard information assets.
- (2) All management and staff of the FI should be aware of the applicable laws, regulations, and guidelines pertaining to the use of, and access to, information assets.
- (3) A training program should be undertaken annually for all staff, contractors and service providers who have access to the FI's information assets.
- (4) The board of directors should undergo training to raise their awareness of risks associated with the use of technology and enhance their understanding of technology and cyber risk management practices.
- (5) The training program should be reviewed regularly to ensure its contents remain current and relevant. The review should take into consideration changes in the FI's IT security policies, current and emerging risks, and the evolving cyber threat environment.

3. Risk Management Framework- Technology and Cyber Security

(A) Risk Management Framework

- (1) An FI should establish a risk management framework to manage technology and cyber risks. Appropriate governance structures and processes should be established, with well-defined roles, responsibilities and clear reporting lines across the various organisational functions.
- (2) Effective risk management practices and internal controls should be incorporated to achieve data confidentiality and integrity, system security and reliability as well as stability and resilience in its IT operating environment.
- (3) A risk officer, who is accountable for ensuring proper risk treatment measures are implemented and enforced for specific technology and cyber risks, should be identified.

(B) Components of the Technology and Cyber Risk Management Framework

i. Technology and Cyber Risk Identification

An FI should:

- a. Establish a process to conduct regular vulnerability assessment (VA) on their IT systems to identify security vulnerabilities and ensure risk arising from these gaps are addressed in a timely manner.
- b. Identify any threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third-party service providers.
- c. Perform a VA which should at a minimum include vulnerability discovery, identification of weak security configurations and open network ports as well as application vulnerabilities. For web-based systems, the scope of VA should include checks on common web-based vulnerabilities.

ii. Technology and Cyber Risk Penetration Testing (PT)

- a. An FI should carry out PT after a VA has been conducted to obtain an in-depth evaluation of its technology and cyber security defenses.

- b. PT should be conducted on an FI's production environment to obtain a more accurate assessment of the robustness of their security measures.
- c. The frequency of PT should be determined based on factors such as system criticality and the system's exposure to technology and cyber risk. The FI is expected to conduct PT annually to validate the adequacy of the security controls for systems that are directly accessible from the internet.

iii. Technology and Cyber Risk Assessment

- a. An FI should perform an analysis of the potential impact and consequences of the threats and vulnerabilities on the overall business and operations. When assessing technology and cyber risks, consideration should be given to financial, operational, legal, reputational, and regulatory factors.
- b. To facilitate the prioritisation of technology risks, a set of criteria measuring and determining the likelihood and impact of the risk scenarios should be established.

iv. Technology and Cyber Threat Exercises

- a. An FI should undertake regular scenario-based technology and cyber threat exercises to validate its response and recovery to prevalent and emerging threats. These exercises can include social engineering, table-top or cyber range exercises.
- b. Subject to the exercise objectives, an FI is expected to involve the relevant stakeholders, including the Commission, senior management, business functions, corporate communications, crisis management team, service providers and technical staff responsible for technology and cyber threat detection, response and recovery.

v. Technology and Cyber Risk Adversarial Attack Simulation Exercise

- a. To test and validate the effectiveness of its technology and cyber defense and response plan against popular technology and cyber threats, an FI should perform an adversarial attack simulation exercise.
- b. The objectives, scope and rules of engagement should be defined before the initiation of the exercise, and the exercise should be conducted in a controlled manner under close supervision to ensure the activities undertaken by the testing team are not detrimental to the FI's production systems.

- c. An FI should design the exercise scenario by using threat intelligence relevant to their IT environment to identify threat actors who are most likely to pose a threat to the FI and identify tactics, techniques and procedures most likely to be used in such attacks.

vi. Technology and Cyber Risk Remediation Management

- a. A comprehensive remediation process should be established to track and resolve issues identified from the technology and cyber security assessments or exercises. The process should minimally include the following:
 - i. Severity assessment and classification of an issue
 - ii. Timeframe to remediate issues of different severity; and
 - iii. Risk assessment and mitigation strategies to manage deviation from the framework.
- b. A technology and cyber incident response and management plan should be established to swiftly isolate and neutralise the threat and securely resume affected services.
- c. Information from cyber intelligence and lessons learnt from the technology and cyber incidents should be used to enhance the existing controls or improve the technology and cyber incident management plan.
- d. An FI should develop and implement risk mitigation and control measures that are consistent with the criticality of the information assets and the level of risk tolerance. The IT control and risk mitigation approach should be subject to regular review and update, considering the changing threat landscape and variations in the FI's risk profile.
- e. An FI should assess whether risks have been reduced to an acceptable level after applying the mitigating measures as there are residual risks from threats and vulnerabilities which cannot be fully eliminated. The criteria and approving authorities for risk acceptance should be clearly defined and it should be correspondent with the FI's risk tolerance.
- f. An FI should obtain insurance coverage for various insurable technology and potential cyber risks to reduce the financial impact such as recovery and restitution costs.

vii. Technology and Cyber Risk Monitoring, Review and Reporting

To facilitate continuous monitoring, prompt detection and response to technology and cyber incidents, an FI should:

- a. Establish a security operations centre or acquire managed security services.

- b. Define SOPs for security operations.
- c. Establish a process to collect, process, review and retain system logs to facilitate the FI's security monitoring operations. The logs should be protected against unauthorised access.
- d. Facilitate the identification of anomalies by establishing a baseline profile of each IT system's routine activities and analysing the system activities against the baseline profiles. The profiles should be regularly reviewed and updated.
- e. Ensure timely escalation to relevant stakeholders regarding suspicious or anomalous system activities or user behavior.
- f. Maintain a risk record to facilitate the monitoring and reporting of technology and cyber risks. Significant risks should be monitored closely and reported to the board of directors and senior management. The frequency of monitoring and reporting should be correspondent with the level of risk.
- g. Develop technology risk metrics to highlight information assets that have the highest risk exposure to facilitate risk reporting to management. In determining the technology risk metrics, the FI should consider risk events and audit observations, as well as applicable regulatory requirements by the Commission.

viii. Technology and Cyber Risk Intelligence and Information Sharing

FIs should actively participate in IT & Cyber-Risk information sharing seminars with trusted parties to enable them to identify, assess, monitor, and respond to cyber threats. To maintain good cyber awareness, the FI should:

- a. Establish a process to collect, process and analyse cyber-related information for its relevance and potential impact to the FI's operations and IT environment.
- b. Obtain cyber intelligence monitoring services.
- c. Establish a process to detect and respond to misinformation related to the FI via various communication networks.

4. Management of Technology Services

(A) Project Management Framework

- (1) A project management framework should be established to ensure:

- a. Consistency in project management practices, and delivery of outcomes that meet project objectives and requirements.
 - b. Policies, standards, procedures, processes, and activities are included to manage projects from initiation to closure.
 - c. Detailed IT project plans are established for all IT projects. An IT project plan should set out the scope of the project, as well as the activities, milestones and deliverables to be realised at each phase of the project. The roles and responsibilities of staff involved in the project should be clearly defined in the plan.
 - d. A risk management process is established to identify, assess, treat and monitor the associated risks throughout the project life cycle.
- (2) A project committee consisting of key stakeholders, including the FI's shareholders and IT should be formed to provide guidance and oversight for large and complex projects that impact the operations of the business. This is to ensure milestones are reached and deliverables are realised in a timely manner.
- (3) Risks and issues for large and complex projects, which cannot be resolved at the project management level should be escalated to the project committee and senior management.

(B) System Acquisition

- (1) SOPs should be established to ensure selected vendors are competent to meet project requirements and deliverables.
- (2) The level of assessment and due diligence performed should be correspondent with the criticality of the project deliverables to the FI.
- (3) Vendor access to the FI's IT systems should be controlled and monitored. The FI should ensure rigorous security practices are in place to safeguard any sensitive data that is accessible to the vendor for the duration of the project.

(C) System Development Life Cycle (SDLC)

- (1) SOPs for the various phases of the SDLC should be maintained. The framework should clearly define the processes, procedures, and controls in each phase of the life cycle,

such as initiation/planning, requirements analysis, design, implementation, testing and acceptance.

- (2) In order to minimise system vulnerabilities, security should be incorporated within each phase of the SDLC. An FI should include security specifications in the system design, perform continuous security evaluation and adhere to security practices throughout the SDLC.
- (3) Security requirements should minimally cover key control areas such as access control, authentication, authorisation, data integrity and confidentiality, system activity logging, security event tracking and exception handling.
- (4) The SDLC should, where relevant, involve the IT security function in each phase of the life cycle.

(D) System Requirements Analysis

- (1) Functional requirements for the IT system should be identified, defined, and documented. An FI should also establish and document key requirements such as system performance, resilience, and security controls.
- (2) An FI should assess potential threats and risks regarding the IT system and determine the acceptable level of security required to meet its business operational needs.

(E) System Design and Implementation

- (1) During the design phase an FI should:
 - a. Review the proposed layout and design of the IT system, including the IT controls to be built into the system, to ensure they meet the defined requirements, before implementation.
 - b. Verify that system requirements are met by the current system design and implementation. Any changes to, or deviations from, the defined requirements should be approved by the relevant stakeholders.
 - c. Engage the relevant domain experts to participate in the design review.

(F) System Testing

- (1) An FI should:
 - a. Determine a process for system testing where the scope of testing should cover system function, security controls, business logic and system performance under various conditions. Prior to testing, a test plan should be established and approved.
 - b. Maintain separate physical and logical environments for unit, system integration and user acceptance testing. Access to each environment should be restricted when necessary.
 - c. Perform regression testing for changes such as an enhancement to the existing IT system to verify that the system continues to function after the changes have been made.
 - d. Report major issues that could have an unfavorable impact on the FI's operations to the project committee. Issues identified by testing should also be addressed.
 - e. Ensure the results of all testing that was conducted are documented in the test report and signed by the relevant parties.

(G) Quality Assurance and Control

- (1) An FI should define the expected quality traits and the assessment metrics for the project deliverables based on its quality control standards.
- (2) An independent quality assurance function should be performed to ensure project activities and deliverables comply with the FI's SOPs.

(H) Technology Configuration and Refresh Management

- (1) To effectively control the IT systems, an FI should:
 - a. Implement a configuration management process to ensure accurate information of its hardware and software is maintained.
 - b. Conduct regular reviews and verify the configuration information of its hardware and software is accurate.
 - c. Avoid using outdated and unsupported hardware or software.

- d. Develop a technology refresh plan for the replacement of hardware and software before they expire.
- e. Conduct a risk assessment for hardware and software approaching the expiry date to evaluate the risks of their continued use. Effective risk mitigation measures should also be implemented.

(I) Patch Management

- (1) A patch management process should be implemented to ensure the timely application of patches across FI's IT systems to correct any software errors.
- (2) Patches should be tested before being deployed to the production environment.

(J) Change and Release Management

- (1) An FI should:
 - a. Establish and implement a technology change and release management process to ensure changes to information assets are assessed, tested, reviewed, and approved before deployed.
 - b. Segregate duties in the change management process to prohibit one individual from developing, compiling, and moving software codes from one environment to another.
 - c. Perform a backup of the information asset before implementing the change and establish a rollback plan to revert the information asset to its previous state if a problem arises during the process.
 - d. Implement controls to maintain traceability and integrity for all software codes that are moved between production and non-production IT environments.

(K) Incident and Problem Management

- (1) The occurrence of an IT incident may result in the disruption, malfunction or error on an FI's server, network or end point which can impact its operations and service delivery. FIs should appropriately manage such incidents to understand root causes and appropriate preventative measures to reduce prolonged disruption of IT services or further aggravation.

- (2) It is important that incidents are accorded with the appropriate severity level. As part of incident analysis, FIs may delegate the function of determining and assigning incident severity levels to a centralized technical helpdesk function. FIs should train helpdesk staff to discern incidents of high severity level. In addition, criteria used for assessing severity levels of incidents should be established and documented.
- (3) FIs should establish corresponding escalation and resolution procedures where the resolution timeframe is proportionate with the severity level of the incident. The predetermined escalation and response plan for IT security incidents should be tested on a regular basis.
- (4) An FI should establish an incident and problem management framework to restore affected IT services or systems to a secure and stable condition to ensure minimal impact to business operations.
- (5) The incident and problem management framework should minimally cover:
 - a. SOPs for handling IT incidents or problems
 - b. Maintenance and protection of supporting evidence for the investigation and diagnosis of incidents; and
 - c. The roles and responsibilities of staff and external parties involved in the process.
- (6) An FI should maintain a log of past incidents which should include previous lessons learnt to facilitate the diagnosis and resolution of future incidents with similar characteristics.

5. Technology Resilience

(A) System Availability

- (1) An FI should ensure that their IT systems are designed to achieve the level of system availability that is proportionate to its operational needs. Notwithstanding such, FIs should also establish SOPs to respond to situations when pre-defined thresholds for system resources and system performance have been breached.
- (2) It is vital for FIs to conduct regular system reviews and testing to ensure a robust level of resilience exists to facilitate sustainable business operations. At a minimum, the review should include a mapping of internal and external dependencies of the FI's IT systems to determine any single point of failure.

(B) Disaster Recovery

- (1) An FI should establish a disaster recovery framework inclusive of procedures to recover systems from various disaster scenarios and the roles and responsibilities of relevant personnel in the recovery process.
- (2) The disaster recovery framework should be reviewed annually and updated when there are significant changes to business operations, information assets or environmental factors.
- (3) An FI should perform regular testing of its disaster recovery plan to validate the effectiveness of the plan and ensure its systems are able to meet the recovery objectives.
- (4) An FI should establish a data backup strategy and develop a plan to perform regular backups so that systems and data can be recovered in the event of a system disruption or when data is corrupted or deleted.

6. Access Rights and System Privileges

(A) User Access Rights

- (1) Access rights should be authorised and approved by appropriate parties, such as the owner of the information assets, which can be an FI and its shareholders. SOPs for user access management should be established to provide, change, and revoke access rights to information assets when necessary.
- (2) Principles such as “segregation of duties” and “least privilege” should be applied when granting staff access to information assets to prohibit the access of one person to perform sensitive system functions.
- (3) An FI should ensure a record of user access and user management activities are logged for audit and investigation purposes.
- (4) To enforce solid password controls for users’ access to IT systems, an FI should establish a password policy and SOPs regarding same. At a minimum, the password policy should include minimum password length and history, password complexity and maximum validity period.

- (5) In efforts to safeguard an FI's systems and data from unauthorised access, the FI should implement multi-factor authentication for users with access to sensitive system functions.
- (6) A user access review should be regularly conducted to identify inactive and redundant user accounts, as well as inappropriate access rights. Any issues identified during the review should be promptly resolved.
- (7) The same monitoring restrictions utilised for an FI's staff should be followed by service providers who have access to the FI's information assets.

(B) Privileged Access Rights

- (1) Access to privileged accounts should only be granted on a need-to-use basis, where the activities of these accounts should be logged and reviewed as a component of an FI's ongoing monitoring process.
- (2) A FI should establish SOPs to manage and monitor the use of system and service accounts for suspicious or unauthorised activities.

(C) Remote Access Rights

- (1) Remote access allows users to connect to the FI's internal network via an external network to access the FI's data and systems, such as emails and business applications.
- (2) Remote access infrastructure should be thoroughly tested for vulnerabilities. When utilising cloud infrastructure, the FI should review existing controls and conduct security assessment and testing.
- (3) To safeguard against unauthorised access to the FI's IT environment, multi-factor authentication should be implemented, when possible, for users utilising remote access. Remote connections should be encrypted to prevent data leakage through network sniffing and eavesdropping.
- (4) An FI should ensure remote access to their information assets is only allowed from devices that have been secured according to their security standards.

7. Data and Infrastructure Security

(A) Data Security

- (1) An FI should:
 - a. Develop SOPs to detect and prevent unauthorised access, modification, copying or transmission of confidential data.
 - b. Implement Data Loss Prevention (DLP), as well as unauthorised modification in systems and endpoint devices.
 - c. Ensure systems managed by the FI's service providers have the same level of protection and ensure they are subjected to the same security standards.
 - d. Implement security measures to prevent and detect the use of unauthorised internet services which allow users to communicate or store confidential data.
 - e. Ensure written approval is obtained from senior management in exceptional situations when sensitive production data needs to be used in non-production environments.
 - f. Implement SOPs in non-production environments to manage the access and removal of data to prevent data leakage.
 - g. Permanently delete confidential data from storage media, systems and endpoint devices before they are disposed of or redeployed.

(B) Network Security

- (1) An FI should:
 - a. Secure the network between the FI and the internet, as well as connections with third parties by installing network security devices such as firewalls.
 - b. Deploy effective security mechanisms to protect information assets to minimise the risk of cyber threats, such as insider threats.
 - c. Detect and block malicious network traffic by deploying network intrusion detection and prevention systems in the FI's network.

- d. Prevent unauthorised devices from connecting to its network by implementing network access controls.
- e. Review access control rules in network devices such as firewalls, routers, switches, and access points on a regular basis to ensure they are kept up to date.
- f. Promptly remove outdated rules and insecure network protocols as these can be manipulated to gain unauthorised access to the FI's network and systems.
- g. Implement an effective Denial of Service (DoS) protection to detect and respond to various types of DoS attacks.
- h. Engage DoS mitigation service providers to filter potential DoS traffic before it reaches the FI's network infrastructure.
- i. Regularly conduct a review of the FI's network architecture, including the network security design, as well as system and network interconnections to identify potential cyber security vulnerabilities.

(C) System Security

(1) An FI should:

- a. Outline the security standards for their hardware and software configurations that will minimise their exposure to cyber threats. The standards should be reviewed periodically for relevance and effectiveness.
- b. Establish a process to verify that the standards are applied uniformly on systems and to identify deviations from the standards. Risks arising from deviations should be addressed in a timely manner.
- c. Implement End Point Detection and Response (EDR) software which will regularly scans and monitors systems for malicious files or anomalous activities.
- d. Implement security measures, such as application whitelisting to ensure only authorised software is allowed to be installed on the FI's systems.
- e. Conduct a comprehensive risk assessment and ensure appropriate measures are implemented to secure its Bring Your Own Device (BYOD) environment before allowing staff to use their personal device to access the corporate network.

(D) Electronic Information Assets

- (1) Electronic information assets refer to devices such as smartphones, multi-function printers and security cameras which can be connected to an FI's network or the internet. An FI should:
 - a. Maintain a record of all its electronic devices, including information such as the networks which they are connected to and their physical locations.
 - b. Implement controls to prevent unauthorised access to their devices.
 - c. Implement SOPs to mitigate risks arising from electronic devices, since most of these devices are designed with minimal security controls.
 - d. Monitor their electronic devices for suspicious or anomalous system activities so that compromised devices can be promptly isolated.
 - e. Host electronic devices in a separate secured network segment from the network that hosts the FI's systems and confidential data to prevent a cyber threat actor from accessing the FI's network.

8. Online Financial Services

(A) Secure Online Financial Services

- (1) When delivering online financial services, an FI should:
 - a. Implement security and control measures which are proportionate with the risk involved to ensure the security of data and online services.
 - b. Secure its communications channels to protect customer data. This can be achieved through data encryption and digital signatures.
 - c. Take adequate measures to minimize their exposure of online financial services to common attack vectors such as man-in-the-middle attack (MITMA), domain name system (DNS) hijacking and distributed denial of service (DDoS) attacks.
 - d. Implement specific measures aimed at addressing the risks of mobile applications if the online financial services are accessible via a mobile device.

- e. Make mobile applications or software available to customers through official mobile application stores, or other secure delivery channels.
- f. Actively monitor for phishing campaigns targeting the FI and its customers. Immediate action should be taken to report phishing attempts to service providers to facilitate the removal of malicious content.
- g. Alert its customers of such campaigns and advise them of security measures to adopt to protect against phishing.

(B) Automated Teller Machines (ATMs) and Payment Card Security (Credit and Debit Cards)

- (1) To facilitate consumer protection and enforce consumers' confidence regarding the use of ATMs, the FI should at a minimum:
 - a. Conduct video surveillance of activities at the machines utilising quality CCTV systems.
 - b. Install anti-skimming solutions on the machines to detect the presence of foreign devices placed around the perimeter of the card entry slot.
 - c. Implement tamper-resistant keypads to ensure that customers' PINs are encrypted during transmission.
 - d. Install detection mechanisms and send alerts to the FI to foster remediation management.
- (2) FIs should also ensure mechanisms are in place to prevent debit and credit card fraud. When issuing cards, the FI should follow best practices to institute payment card security such as EMV chip technology and other technological enhancements.

(C) Customer Verification for Online Transactions

- (1) To secure customer activity on the online environment, an FI should:
 - a. Utilise multi-factor authentication at login for online financial services to protect the customer verification process.

- b. Safeguard the confidentiality of customer passwords by verifying them in a hardened or tamper-resistant system.
- c. Protect the integrity of customer accounts' data and transaction details through the implementation of digital signatures to permit high-risk activities. High-risk activities include changes to the customer's mailing address, email address, high-value funds transfers and revision of funds transfer limits.
- d. Implement suitable risk-based authentication that provides customers with verification options that are proportionate with the risk level of the transaction and sensitivity of the data.
- e. Establish short and practicable validity periods when implementing time-based one-time passwords (OTPs), to lower the risk of a stolen OTP being used for fraudulent transactions.
- f. Ensure biometric-related data and verification credentials are encrypted in storage where biometric technologies and customer passwords are used for customer verification.
- g. Detect and terminate hijacked sessions to reduce the risk of an attacker maintaining a hijacked session indefinitely. Throughout the interaction with the customer, the FI should ensure the authenticated session, together with its encryption protocol, remains intact.
- h. Perform a security risk assessment of alternate controls and processes, implemented for corporate customers to authorise transactions, to ensure they are proportionate with the risk of the activities undertaken.

(D) Fraudulent Online Transaction Management

- (1) To detect and block suspicious or fraudulent online transactions, an FI should implement real-time fraud monitoring systems. SOPs should be established to investigate suspicious transactions or payments and to ensure issues are adequately and promptly addressed.
- (2) FIs should inform customers of the security best practices that they should adopt when using online financial services. This includes measures to take to secure their electronic devices and identity information that is used to access online financial services.
- (3) Customers should be alerted on a timely basis regarding new cyber threats so that they can take precautionary measures.

- (4) FIs should advise their customers on the methods to detect unauthorised transactions and to promptly report security issues, suspicious activities or suspected fraud to the FI.
- (5) FIs should also notify affected customers in writing of suspicious activities or funds transferred above a threshold that is defined by the FI or its customers.

9. IT Audit

(A) Audit Function

- (1) FIs should:
 - a. Perform an audit to provide the board of directors and senior management with an independent and objective opinion of the adequacy and effectiveness of the FI's risk management, governance and internal controls relative to its existing and emerging technology and cyber security risks.
 - b. Identify a comprehensive set of auditable areas such as IT operations, functions and SOPs so that an effective risk assessment could be performed during audit planning.
 - c. Ensure the frequency of IT audits are proportionate with the criticality of, and risk posed by the IT information asset, function or process.
 - d. Ensure its IT auditors are competent to effectively assess and evaluate the adequacy of the IT SOPs and controls implemented.

10. Technology and Cyber Security Incident Reporting

(A) Criteria for Reporting to the Commission

- (1) Reportable incidents (*see Appendix I*) may have one or more than one of the following characteristics:
 - a. Potential consequences to other FIs or the Barbadian financial system
 - b. Impact on the FI's systems affecting financial market settlement, confirmations or payments (e.g., Financial Market Infrastructure), or impact to payment services.

- c. Impact to the FI's operations, infrastructure, data and/or systems, including but not limited to the confidentiality, integrity or availability of customer information.
 - d. Disruptions to business systems and/or operation, including but not limited to utility or data centre outages or loss or degradation of connectivity.
 - e. Operational impact to key/critical systems, infrastructure or data
 - f. Disaster recovery teams or plans have been activated, or a disaster declaration has been made by a third-party vendor that impacts the FI.
 - g. Operational impact to internal users, and that poses an impact to external customers or business operations.
 - h. The amount of impacted external customers is increasing; negative reputational impact is imminent (e.g., public and/or media disclosure)
 - i. Impact on a third party affecting the FI.
 - j. The FI's technology or cyber incident management team or protocols have been activated.
 - k. An incident has been reported to:
 - i. A local government department
 - ii. Other local or foreign supervisory or regulatory organisations or agencies
 - iii. Any law enforcement agencies
 - iv. Has invoked internal or external counsel.
 - l. An incident for which a cyber insurance claim has been initiated.
 - m. An incident assessed by an FI to be of a high or critical severity.
 - n. Technology or cyber security incidents that breach internal risk appetite or thresholds.
- (2) For incidents that do not align with or contain the specific criteria listed above, or when an entity is uncertain, notification to the Commission is encouraged as a precaution.

(B) Notification Requirements

- (1) FIs should inform the Commission within four (4) hours after an incident is classified, noting that an incident should be classified within the first twenty-four (24) hours of its detection. An incident is classified as major if it satisfies the requisite criteria in the Classification Matrix found in the *Instructions for the completion of the forms*.
- (2) Cybersecurity events that have a reasonable likelihood of materially harming any part of the normal operation(s) of the FI, should also be reported via the Cyber Incident Reporting Forms to the Commission.
- (3) Annually each FI should revise their Cybersecurity program where it has identified areas, systems or processes that require material improvement, updating or redesign. FIs should document the identification, and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the Commission.
- (4) FIs should keep customers informed of any major incident or data breach where their data has potentially been compromised. They should also assess the effectiveness of the mode of communication, including informing the general public, where necessary.
- (5) As incidents may stem from numerous factors, FIs should perform a root cause and impact analysis for major incidents which result in disruption of critical IT services. FIs should take remediation actions to prevent the recurrence of similar incidents and security breaches.
- (6) FIs should seek further guidance regarding the completion of the forms from *Instructions for the completion of the Major Cyber Incident Reporting Forms* which is accessible on the Commission's website.

(C) Failure to Report to the Commission

Failure to report incidents to the Commission as outlined above may result in increased supervisory oversight including but not limited to enhanced monitoring activities, watch-listing or staging of the FI pursuant to the Commission's ladder of intervention.

30th January, 2025

FINANCIAL SERVICES COMMISSION

DOMESTIC NON-BANK SYSTEMICALLY IMPORTANT FINANCIAL INSTITUTIONS GUIDELINE



**FINANCIAL SERVICES
COMMISSION**

DOMESTIC NON-BANK SYSTEMICALLY IMPORTANT FINANCIAL INSTITUTIONS GUIDELINE

**This Guideline was issued on December 1st, 2024
pursuant to Section 53 of the Financial Services Commission Act,
2010-10**

Table of Contents

PURPOSE	3
1. CRITERIA FOR DETERMINING SYSTEMIC IMPORTANCE.....	4
1.1 Size	4
1.2 Substitutability	4
1.3 Interconnectedness	5
2. REGULATORY AND SUPERVISORY REQUIREMENTS FOR DNB-SIFIs.....	6
2.1 Capital.....	6
2.2 Liquidity and Large Exposures	7
2.3 Reporting and Disclosure.....	8
2.4 Corporate Governance.....	8
2.5 Fitness and Propriety	9
2.6 Risk Management	12
2.7 Business Recovery Planning	13
2.8 Resolution Planning.....	15
2.9 Expert Reviews and Reports.....	15
3. SANCTIONS	16
4. APPENDIX 1.....	17

PURPOSE

This guideline outlines the standards and requirements for financial institutions designated as Domestic Non-bank Systemically Important Financial Institutions (DNB-SIFIs).

These measures are intended to mitigate the risk posed by such entities to the financial system and broader economy. DNB-SIFIs are expected to adopt and implement robust risk-based capital, liquidity, risk management, governance, business continuity, and resolution standards. DNB-SIFIs will be subject to enhanced disclosure and reporting requirements to enable timely and effective responses to emerging risks.

1. CRITERIA FOR DETERMINING SYSTEMIC IMPORTANCE

Consistent with criteria established by the Basel Committee on Banking Supervision (2012)¹, the Financial Services Commission (Commission) defines a Domestic Non-Bank Systemically Important Financial Institution (DNB-SIFI) as a non-bank financial institution (FI) whose distress or disorderly failure would cause significant disruption to the broader financial system and economic activity because of its size, substitutability, and systemic interconnectedness.

1.1 Size

The ability of a financial institution to impact on the financial system and the broader economy in the event of its failure is directly correlated with its size. A large financial institution whose activities comprise a significant share of the domestic system and economy will have a significant negative impact on the system and economy if it fails.

The Commission considers a number of factors in evaluating the size of a financial institution and its potential impact, including but not limited to the following:

- Total assets of the financial entity relative to other similar entities in the market,
- Total assets relative to the overall financial sector
- Size of off-balance sheet exposures.

1.2 Substitutability

Substitutability is determined by how much a financial institution can be replaced by another

¹ In document titled “A Framework for Dealing with Domestic Systemically Important Banks”, published in October 2012.

market participant and financial services provider. The more significant the FI's role as a market participant and a financial services provider, the greater the risk of a significant disruption following its failure, given the limited capacity and ability of other FIs to address the service gaps in a timely manner.

The Commission employs the following indicators to assess the substitutability of a FI.

- Total funds held in a fiduciary capacity,
- Total deposits accepted from non-FI customers,
- Total loans extended to non-FI customers
- The number of institutions providing the registered activity or capable of providing the registered activity.
- The importance of the entity as a financial marketplace (settlements facilitator).
- The volume and value of premiums written relative to the life market.

1.3 Interconnectedness

In a financial institution, interconnectedness refers to the complex relationships and dependencies between entities, systems, and processes within the institution and with external partners, markets, and regulatory bodies. The higher the level of interconnectedness, the greater the risk that a financial institution's failure will spread to other financial institutions and the broader economy.

The Commission utilizes the following indicators to capture the interconnectedness of a FI:

- Total intra-financial assets and intra-off-balance sheet exposures held by the FI,
- Total intra-financial assets and off-balance sheet exposures held by the FI relative to total financial sector assets.
- The extent to which assets in the FI or group (including off-balance sheet assets) are highly integrated with the key aspects of the real sector such that the loss of the assets will cause significant economic stress to the system.

2. REGULATORY AND SUPERVISORY REQUIREMENTS FOR DNB-SIFIs

FIs designated as DNB-SIFIs are subject to enhanced regulatory and supervisory measures and mechanisms. These measures and mechanisms are intended to monitor, assess, and respond to emerging risks and developments within and in respect of the institution.

The requirements for designated DNB-SIFI are as follows:

2.1 Capital

A designated DNB-SIFI is required to:

- i. maintain such capital as may be determined by the Commission. This may include additional capital buffers, limitations on the type of instruments accepted as capital, limitations on the jurisdiction in which the capital may be held, etc.
- ii. create, implement, and maintain a capital management plan that outlines, among other

things, the FI's capital adequacy assessment process, including the frequency of internal capital assessment reviews, capital buffers that are in excess of minimum regulatory capital requirements, and a capital restoration plan. Where the financial institution is a part of a group, it is required to have an enterprise-wide capital plan in addition to its individual plan.

- iii. In clear, documented terms, illustrate that the FI's capital levels and targets align with the Board of Directors' risk appetite, strategic plans, and initiatives. The FI's capital is required to be adequate to support the complexity of the FI's business and risk exposure.
- iv. Assess and update its capital management plan at least annually and at other times as necessary.

2.2 Liquidity and Large Exposures

- i. A DNB-SIFI is required to establish and monitor its liquidity risk tolerance and maintain a contingency funding plan and liquidity buffers to manage liquidity stress events when normal funding sources may not be available. A DNB-SIFI must ensure its ongoing ability to meet its short-term (thirty-day) obligations by maintaining a liquidity coverage ratio such that its assets can sufficiently fund cash outflows for a thirty-day period. Additionally, a DNB-SIFI is expected to maintain its capacity to meet its obligations in the long term (twelve months) by maintaining a net stable funding ratio such that its funding structure is deemed sustainable.

2.3 Reporting and Disclosure

- i. A DNB-SIFI is required to file reports and make disclosures related to, among other things: its business, financial condition, internal controls, and risk management when requested by the Commission.
- ii. A DNB-SIFI is required to file the reports outlined in **Appendix 1** with the Commission in accordance with stated periods or such other times as the Commission may require.

2.4 Corporate Governance

- i. The Board of a DNB-SIFI is an oversight role. It has ultimate responsibility for promoting and approving the FI's business and strategic objectives, governance, risk management and compliance frameworks, control functions, and corporate culture. The Board is required to ensure management has effectively implemented the policies and standards set. The Board may delegate some of its functions, though not its responsibilities, to board committees where appropriate, subject to effective Board oversight and ratification of key decisions that materially impact the FI's operations. The Board of a DNB-SIFI shall NOT be an Executive Board and shall not be engaged in the day-to-day operations of the FI. As provided in the Corporate Governance guideline, DNB-SIFIs are required to adopt higher standards and are expected to have an Asset Liability Committee (ALCO), a subcommittee of the Board.
- ii. The Board must be sufficiently large, based on the size, risk profile, and complexity of the FI, to ensure that it can adequately and effectively oversee the FI but should not be so large as to make oversight challenging. It is recommended that the Board of a DNB-SIFI be

between 7-13 members and comprises members with sufficient experience and expertise to facilitate effective oversight. Board qualification is an ongoing requirement, and members should be and remain qualified, individually and collectively, with a sufficient breadth of understanding of the FI's business for their positions. They should understand their oversight and corporate governance role and be able to exercise sound, objective judgment about the affairs of the FI.

- iii. The Board must develop, document, and regularly review the criteria and skill sets required by its members, individually and collectively.
- iv. The Board should comprise individuals with diverse skills, backgrounds, experience, and expertise who collectively possess the necessary qualifications commensurate with the FI's size, complexity, and risk profile. Their skills and expertise should include, inter alia, capital markets, financial analysis, financial stability issues, financial reporting, information technology, strategic planning, risk management, compensation, regulation, corporate governance, and management. Take note that this list is not intended to be exhaustive.
- v. The Board should collectively have a reasonable understanding of local, regional, and global economic and market forces and the legal and regulatory environment.

2.5 Fitness and Propriety

- i. All candidates for the Board of Directors, elected committees, committees to whom the

Board has delegated authority, and Senior Management/Officers, including acting appointees or any person responsible for executing major policy decisions of the Board, must be vetted and approved by the Commission before assuming office. Where this requirement has been contravened, the Commission may exercise its power to remove that person.

- ii. The Board should have a precise, rigorous, and documented process for identifying, assessing, and selecting Board candidates.

The selection process should include an assessment of whether the Board candidates:

- i. Demonstrate the requisite knowledge, skills, experience, and independence of mind (for independent directors), considering their responsibilities on the Board and the financial institution's business and risk profile.
- ii. Bring a unique skill set when combined with the existing Board members' capabilities.
- iii. Enhances the overall competence of the Board.
- iv. Meet the "fit and proper" criteria, ensuring they are suitable for their role.
- v. Have sufficient time and availability to carry out their responsibilities effectively.
- vi. Facilitate smooth interaction and collaboration among Board members.

- iii. When a regulated entity seeks to appoint or engage a person to perform a regulated function, it is the responsibility of the regulated entity to satisfy the Commission that the person is fit and proper and consistent with the Commission's Fit and Proper Guideline to perform the function for which they are being appointed or engaged.
- iv. It is expected that the assessment conducted by the FI will take place at the recruitment stage, and on an ongoing basis, and that the regulated entity will make every effort to verify qualifications, experience, references and membership in professional bodies. The regulated entity is also expected to conduct probity checks on criminal history, sanctions, legal proceedings, and other similar matters. The regulated entity should be able to satisfy the Commission that the person acting or proposing to act in a regulated function possesses good character, integrity, competence, and capability for the particular function and is financially sound.
- v. Assessments conducted by the regulated entity to determine the fitness and propriety of persons seeking to conduct a regulated function must be documented to evidence what was done to determine the applicant's suitability for the position. Such internal assessments must be made available to the Commission upon request.
- vi. The Commission expects that when a third party is submitting the fit and proper documentation on behalf of a regulated entity or person (e.g., in the case of a licensing application when an attorney or other representative is submitting the application), the third party shall obtain and submit all relevant information as required and ensure that only complete applications are submitted to the Commission.

- vii. The responsibilities of the Board of a regulated entity with respect to fitness and propriety are as follows:
- Ensuring that the regulated entity develops and implements fit and proper policies and procedures, including an assessment process. Such policies, procedures, and processes shall be approved by the Boards and reviewed at least annually.
 - Either alone or through its Nominating Committee, conduct fit and proper assessments of directors, the CEO, and the company secretary, subject to regulatory requirements, and make decisions on their appointments.

2.6 Risk Management

- i. A DNB-SIFI is required to establish a risk committee responsible for approving and periodically reviewing the risk management policies of the financial institution. Where the DNB-SIFI is a part of a group, the committee should oversee the enterprise-wide risk management framework.
- ii. A DNB-SIFI is required to create and maintain an enterprise-wide risk management framework commensurate with its size, activities, structure, risk profile, and complexity.
- iii. The framework should address, at a minimum:
- the policies and procedures for determining its risk management governance,
 - processes and infrastructure to identify, mitigate, and report risk management deficiencies and failures, as well as emerging risks,

- processes and infrastructure to ensure timely, effective action is taken to address emerging risks and risk management failures/deficiencies,
- the responsibilities of the board, management, and employees in the risk management process and framework,
- that the policies, processes, and infrastructure are established to safeguard the risk management function's independence.

2.7 Business Recovery Planning

- i. Each DNB-SIFI should have a robust and credible recovery plan which the Board approves.
- ii. The recovery plan serves as a guide to restoring a distressed DNB-SIFI. During the recovery phase, the financial institution has not yet met the conditions for resolution or entered the resolution regime. If appropriate recovery measures are taken, there should be a reasonable prospect of recovery. The recovery plan should include measures to reduce the institution's risk profile and conserve capital, as well as strategic options, such as the divestiture of business lines and balance sheet restructuring.
- iii. The recovery plan should consider the institution's specific circumstances and reflect its nature, complexity, interconnectedness, level of substitutability, and size.
- iv. The underlying assumptions of the recovery plan and stress scenarios should be sufficiently severe. Organization (group) specific stress scenarios, including idiosyncratic, market-wide risk, and system-wide stress scenarios, should be

considered. The stress scenarios should consider the potential impact of contagion in crisis scenarios and simultaneous stress situations. Upon request, a DNB-SIFI is required to provide strategy and scenario analysis.

- v. The recovery plan should guide the DNB-SIFI and the Commission in a recovery or resolution scenario. It does not imply that the Commission would be obliged to implement or prevent them from implementing a different strategy if the organisation needs to be resolved.
- vi. The responsibility for developing, maintaining, and executing the recovery plan where necessary lies with the institution's senior management. This includes periodic simulation of scenario exercises to assess whether the recovery plans are feasible and credible. The Commission will review the recovery plan as part of the overall supervisory process, assessing its credibility and ability to be effectively implemented.
- vii. DNB-SIFIs must regularly update their recovery plan and whenever events significantly affect the organization's structure, operations, strategy, or overall risk exposure. They are expected to regularly review the assumptions by informing the recovery plans and assess their relevance and applicability on an ongoing basis. If necessary, DNB-SIFIs should adapt their recovery plan accordingly.
- viii. DNB-SIFIs are required to have a robust governance structure in place and sufficient resources to support the recovery planning process. This includes clear responsibilities for business units, senior managers, and Board members. It also includes identifying a

senior-level executive responsible for ensuring the organization complies with recovery plan requirements and ensuring recovery planning is integrated into the organization's overall governance processes.

- ix. DNB-SIFIs are expected to have systems in place to generate timely information required to support the recovery planning process. This will enable both the institution and the Commission to effectively carry out recovery and resolution planning and, where necessary, implement the recovery or resolution plan.

2.8 Resolution Planning

- i. Each designated DNB-SIFI must develop, and the Board must approve resolution plans, also known as “living wills,” which detail how the entity will resolve itself in an orderly manner if it is no longer able to continue as a “going concern,” to minimize the impact of the failure on customers, stakeholders, other FIs and the broader economy. These plans must be reviewed annually and updated to consider changes in the entity's circumstances or operating environment.

2.9 Expert Reviews and Reports

A DNB-SIFI is required to have reviews conducted and reports provided by experts such as actuaries, accountants, and members of other professional bodies, as the Commission may require.

3. SANCTIONS

Failure to comply with this guideline is a breach of the Financial Services Commission Act (FSCA). It can result in sanctions and penalties, including limitations on the licence and allowed activities.

4. APPENDIX 1

Domestic Non-bank Systemically Important Financial Institutions

Frequency	Filing deadline	Report type
Annual	Within 30 days of the end of the institution's financial year-end.	• Corporate Structure • Annual business plan and objectives • Internal Audit Reports • Reports on Internal control failures • Auditor's management letter
Bi-annual	Within 30 days of the end of the second and fourth quarters.	• Stress testing reports
Quarterly	Within 30 days of the end of each quarter.	• Liquidity report • Large exposure report • Cash flow statements • Loan report • Delinquency report • Report regarding affiliated entities, including their parent or holding company and subsidiaries
Monthly	Within 15 days of the end of each month.	Board minutes and related Board papers and packages.