

VII. APPENDICES



THIS PAGE INTENTIONALLY LEFT BLANK

A. KEY STATISTICS

FDIC ACTIONS ON FINANCIAL INSTITUTIONS APPLICATIONS 2016–2018			
	2018	2017	2016
Deposit Insurance	17	12	7
Approved ¹	17	12	7
Denied	0	0	0
New Branches	533	500	507
Approved	533	500	507
Denied	0	0	0
Mergers	224	218	245
Approved	224	218	245
Denied	0	0	0
Requests for Consent to Serve²	120	104	167
Approved	120	104	164
Section 19	7	1	9
Section 32	113	103	155
Denied	0	0	3
Section 19	0	0	0
Section 32	0	0	3
Notices of Change in Control	21	17	14
Letters of Intent Not to Disapprove	21	17	14
Disapproved	0	0	0
Brokered Deposit Waivers	5	12	14
Approved	5	11	13
Denied	0	1	1
Savings Association Activities³	0	1	0
Approved	0	1	0
Denied	0	0	0
State Bank Activities/Investments⁴	9	2	5
Approved	9	2	5
Denied	0	0	0
Conversion of Mutual Institutions	2	5	5
Non-Objection	2	5	5
Objection	0	0	0

¹ Includes deposit insurance application filed on behalf of (1) newly organized institutions, (2) existing uninsured financial services companies seeking establishment as an insured institution, and (3) interim institutions established to facilitate merger or conversion transactions, and applications to facilitate the establishment of thrift holding companies.

² Under Section 19 of the Federal Deposit Insurance (FDI) Act, an insured institution must receive FDIC approval before employing a person convicted of dishonesty or breach of trust. Under Section 32, the FDIC must approve any change of directors or senior executive officers at a state nonmember bank that is not in compliance with capital requirements or is otherwise in troubled condition.

³ Section 28 of the FDI Act, in general, prohibits a federally-insured state savings association from engaging in an activity not permissible for a federal savings association and requires notices or applications to be filed with the FDIC.

⁴ Section 24 of the FDI Act, in general, prohibits a federally-insured state bank from engaging in an activity not permissible for a national bank and requires notices or applications to be filed with the FDIC.

COMBINED RISK AND CONSUMER ENFORCEMENT ACTIONS

2016–2018

	2018	2017	2016
Total Number of Actions Initiated by the FDIC	177	231	259
Termination of Insurance	8	9	5
Involuntary Termination	0	0	0
Sec. 8a For Violations, Unsafe/Unsound Practices or Conditions	0	0	0
Voluntary Termination	8	9	5
Sec. 8a By Order Upon Request	0	0	0
Sec. 8p No Deposits	7	8	5
Sec. 8q Deposits Assumed	1	1	0
Sec. 8b Cease-and-Desist Actions	23	26	30
Notices of Charges Issued	1	0	2
Orders to Pay Restitution	5	4	0
Consent Orders	17	14	26
Personal Cease and Desist Orders	0	8	2
Sec. 8e Removal/Prohibition of Director or Officer	52	65	97
Notices of Intention to Remove/Prohibit	2	7	8
Consent Orders	50	58	89
Sec. 8g Suspension/Removal When Charged With Crime	0	0	0
Civil Money Penalties Issued	25	47	37
Sec. 7a Call Report Penalties	0	0	0
Sec. 8i Civil Money Penalties	23	42	34
Sec. 8i Civil Money Penalty Notices of Assessment	2	5	3
Sec. 10c Orders of Investigation	6	9	10
Sec. 19 Waiver Orders	59	71	72
Approved Section 19 Waiver Orders	59	71	72
Denied Section 19 Waiver Orders	0	0	0
Sec. 32 Notices Disapproving Officer/Director's Request for Review	0	0	1
Truth-in-Lending Act Reimbursement Actions	91	135	83
Denials of Requests for Relief	0	0	0
Grants of Relief	0	0	0
Banks Making Reimbursement*	91	135	83
Suspicious Activity Reports (Open and closed institutions)*	193,585	182,647	222,836
Other Actions Not Listed	4	4	7

* These actions do not constitute the initiation of a formal enforcement action and, therefore, are not included in the total number of actions initiated.

**ESTIMATED INSURED DEPOSITS AND THE DEPOSIT INSURANCE FUND,
DECEMBER 31, 1934, THROUGH SEPTEMBER 30, 2018¹**

Dollars in Millions (except Insurance Coverage)

Year	Insurance Coverage ²	Deposits in Insured Institutions ²			Insurance Fund as a Percentage of		
		Total Domestic Deposits	Est. Insured Deposits	Percentage of Domestic Deposits	Deposit Insurance Fund	Total Domestic Deposits	Est. Insured Deposits
2018	\$250,000	\$12,368,002	\$7,376,566	59.6	\$100,204.0	0.81	1.36
2017	250,000	12,129,503	7,159,748	59.0	92,747.5	0.76	1.30
2016	250,000	11,693,371	6,917,928	59.2	83,161.5	0.71	1.20
2015	250,000	10,952,922	6,519,449	59.5	72,600.2	0.66	1.11
2014	250,000	10,410,687	6,195,554	59.5	62,780.2	0.60	1.01
2013	250,000	9,825,479	5,998,238	61.0	47,190.8	0.48	0.79
2012	250,000	9,474,720	7,402,053	78.1	32,957.8	0.35	0.45
2011	250,000	8,782,291	6,973,483	79.4	11,826.5	0.13	0.17
2010	250,000	7,887,858	6,301,542	79.9	(7,352.2)	(0.09)	(0.12)
2009	250,000	7,705,354	5,407,773	70.2	(20,861.8)	(0.27)	(0.39)
2008	100,000	7,505,408	4,750,783	63.3	17,276.3	0.23	0.36
2007	100,000	6,921,678	4,292,211	62.0	52,413.0	0.76	1.22
2006	100,000	6,640,097	4,153,808	62.6	50,165.3	0.76	1.21
2005	100,000	6,229,753	3,890,930	62.5	48,596.6	0.78	1.25
2004	100,000	5,724,621	3,622,059	63.3	47,506.8	0.83	1.31
2003	100,000	5,223,922	3,452,497	66.1	46,022.3	0.88	1.33
2002	100,000	4,916,078	3,383,598	68.8	43,797.0	0.89	1.29
2001	100,000	4,564,064	3,215,581	70.5	41,373.8	0.91	1.29
2000	100,000	4,211,895	3,055,108	72.5	41,733.8	0.99	1.37
1999	100,000	3,885,826	2,869,208	73.8	39,694.9	1.02	1.38
1998	100,000	3,817,150	2,850,452	74.7	39,452.1	1.03	1.38
1997	100,000	3,602,189	2,746,477	76.2	37,660.8	1.05	1.37
1996	100,000	3,454,556	2,690,439	77.9	35,742.8	1.03	1.33
1995	100,000	3,318,595	2,663,873	80.3	28,811.5	0.87	1.08
1994	100,000	3,184,410	2,588,619	81.3	23,784.5	0.75	0.92
1993	100,000	3,220,302	2,602,781	80.8	14,277.3	0.44	0.55
1992	100,000	3,275,530	2,677,709	81.7	178.4	0.01	0.01
1991	100,000	3,331,312	2,733,387	82.1	(6,934.0)	(0.21)	(0.25)
1990	100,000	3,415,464	2,784,838	81.5	4,062.7	0.12	0.15
1989	100,000	3,412,503	2,755,471	80.7	13,209.5	0.39	0.48
1988	100,000	2,337,080	1,756,771	75.2	14,061.1	0.60	0.80
1987	100,000	2,198,648	1,657,291	75.4	18,301.8	0.83	1.10
1986	100,000	2,162,687	1,636,915	75.7	18,253.3	0.84	1.12

**ESTIMATED INSURED DEPOSITS AND THE DEPOSIT INSURANCE FUND,
DECEMBER 31, 1934, THROUGH SEPTEMBER 30, 2018¹ (continued)**

Dollars in Millions (except Insurance Coverage)

Year	Insurance Coverage ²	Deposits in Insured Institutions ²			Insurance Fund as a Percentage of		
		Total Domestic Deposits	Est. Insured Deposits	Percentage of Domestic Deposits	Deposit Insurance Fund	Total Domestic Deposits	Est. Insured Deposits
1985	100,000	1,975,030	1,510,496	76.5	17,956.9	0.91	1.19
1984	100,000	1,805,334	1,393,421	77.2	16,529.4	0.92	1.19
1983	100,000	1,690,576	1,268,332	75.0	15,429.1	0.91	1.22
1982	100,000	1,544,697	1,134,221	73.4	13,770.9	0.89	1.21
1981	100,000	1,409,322	988,898	70.2	12,246.1	0.87	1.24
1980	100,000	1,324,463	948,717	71.6	11,019.5	0.83	1.16
1979	40,000	1,226,943	808,555	65.9	9,792.7	0.80	1.21
1978	40,000	1,145,835	760,706	66.4	8,796.0	0.77	1.16
1977	40,000	1,050,435	692,533	65.9	7,992.8	0.76	1.15
1976	40,000	941,923	628,263	66.7	7,268.8	0.77	1.16
1975	40,000	875,985	569,101	65.0	6,716.0	0.77	1.18
1974	40,000	833,277	520,309	62.4	6,124.2	0.73	1.18
1973	20,000	766,509	465,600	60.7	5,615.3	0.73	1.21
1972	20,000	697,480	419,756	60.2	5,158.7	0.74	1.23
1971	20,000	610,685	374,568	61.3	4,739.9	0.78	1.27
1970	20,000	545,198	349,581	64.1	4,379.6	0.80	1.25
1969	20,000	495,858	313,085	63.1	4,051.1	0.82	1.29
1968	15,000	491,513	296,701	60.4	3,749.2	0.76	1.26
1967	15,000	448,709	261,149	58.2	3,485.5	0.78	1.33
1966	15,000	401,096	234,150	58.4	3,252.0	0.81	1.39
1965	10,000	377,400	209,690	55.6	3,036.3	0.80	1.45
1964	10,000	348,981	191,787	55.0	2,844.7	0.82	1.48
1963	10,000	313,304	177,381	56.6	2,667.9	0.85	1.50
1962	10,000	297,548	170,210	57.2	2,502.0	0.84	1.47
1961	10,000	281,304	160,309	57.0	2,353.8	0.84	1.47
1960	10,000	260,495	149,684	57.5	2,222.2	0.85	1.48
1959	10,000	247,589	142,131	57.4	2,089.8	0.84	1.47
1958	10,000	242,445	137,698	56.8	1,965.4	0.81	1.43
1957	10,000	225,507	127,055	56.3	1,850.5	0.82	1.46
1956	10,000	219,393	121,008	55.2	1,742.1	0.79	1.44
1955	10,000	212,226	116,380	54.8	1,639.6	0.77	1.41
1954	10,000	203,195	110,973	54.6	1,542.7	0.76	1.39
1953	10,000	193,466	105,610	54.6	1,450.7	0.75	1.37

**ESTIMATED INSURED DEPOSITS AND THE DEPOSIT INSURANCE FUND,
DECEMBER 31, 1934, THROUGH SEPTEMBER 30, 2018¹ (continued)**

Dollars in Millions (except Insurance Coverage)

Year	Insurance Coverage ²	Deposits in Insured Institutions ²			Insurance Fund as a Percentage of		
		Total Domestic Deposits	Est. Insured Deposits	Percentage of Domestic Deposits	Deposit Insurance Fund	Total Domestic Deposits	Est. Insured Deposits
1952	10,000	188,142	101,841	54.1	1,363.5	0.72	1.34
1951	10,000	178,540	96,713	54.2	1,282.2	0.72	1.33
1950	10,000	167,818	91,359	54.4	1,243.9	0.74	1.36
1949	5,000	156,786	76,589	48.8	1,203.9	0.77	1.57
1948	5,000	153,454	75,320	49.1	1,065.9	0.69	1.42
1947	5,000	154,096	76,254	49.5	1,006.1	0.65	1.32
1946	5,000	148,458	73,759	49.7	1,058.5	0.71	1.44
1945	5,000	157,174	67,021	42.6	929.2	0.59	1.39
1944	5,000	134,662	56,398	41.9	804.3	0.60	1.43
1943	5,000	111,650	48,440	43.4	703.1	0.63	1.45
1942	5,000	89,869	32,837	36.5	616.9	0.69	1.88
1941	5,000	71,209	28,249	39.7	553.5	0.78	1.96
1940	5,000	65,288	26,638	40.8	496.0	0.76	1.86
1939	5,000	57,485	24,650	42.9	452.7	0.79	1.84
1938	5,000	50,791	23,121	45.5	420.5	0.83	1.82
1937	5,000	48,228	22,557	46.8	383.1	0.79	1.70
1936	5,000	50,281	22,330	44.4	343.4	0.68	1.54
1935	5,000	45,125	20,158	44.7	306.0	0.68	1.52
1934	5,000	40,060	18,075	45.1	291.7	0.73	1.61

¹For 2018, figures are as of September 30; all other prior years are as of December 31. Prior to 1989, figures are for the Bank Insurance Fund (BIF) only and exclude insured branches of foreign banks. For 1989 to 2005, figures represent the sum of the BIF and Savings Association Insurance Fund (SAIF) amounts; for 2006 to 2018, figures are for DIF. Amounts for 1989-2018 include insured branches of foreign banks. Prior to year-end 1991, insured deposits were estimated using percentages determined from June Call and Thrift Financial Reports.

²The year-end 2008 coverage limit and estimated insured deposits do not reflect the temporary increase to \$250,000 then in effect under the Emergency Economic Stabilization Act of 2008. The Dodd-Frank Wall Street Reform and Consumer Protection (Dodd-Frank) Act made this coverage limit permanent. The year-end 2009 coverage limit and estimated insured deposits reflect the \$250,000 coverage limit. The Dodd-Frank Act also temporarily provided unlimited coverage for non-interest bearing transaction accounts for two years beginning December 31, 2010. Coverage for certain retirement accounts increased to \$250,000 in 2006. Initial coverage limit was \$2,500 from January 1 to June 30, 1934.

**INCOME AND EXPENSES, DEPOSIT INSURANCE FUND, FROM BEGINNING OF OPERATIONS,
SEPTEMBER 11, 1933, THROUGH DECEMBER 31, 2018**

Dollars in Millions

Year	Income					Expenses and Losses					
	Total	Assessment Income	Assessment Credits	Investment and Other	Effective Assessment Rate ¹	Total	Provision for Ins. Losses	Admin. and Operating Expenses ²	Interest & Other Ins. Expenses	Funding Transfer from the FSLIC Resolution Fund	Net Income/ (Loss)
TOTAL	\$253,463.9	\$185,121.7	\$11,392.9	\$79,735.1		\$150,511.3	\$107,728.6	\$33,313.7	\$9,469.1	\$139.5	\$103,092.1
2018	11,170.8	9,526.7	0.0	1,644.1	0.0627%	1,205.2	(562.6)	1,764.7	3.1	0	9,965.6
2017	11,663.7	10,594.8	0.0	1,068.9	0.0716%	1,558.2	(183.1)	1,739.4	2.0	0	10,105.5
2016	10,674.1	9,986.6	0.0	687.5	0.0699%	150.6	(1,567.9)	1,715.0	3.5	0	10,523.5
2015	9,303.5	8,846.8	0.0	456.7	0.0647%	(553.2)	(2,251.3)	1,687.2	10.9	0	9,856.7
2014	8,965.1	8,656.1	0.0	309.0	0.0663%	(6,634.7)	(8,305.5)	1,664.3	6.5	0	15,599.8
2013	10,458.9	9,734.2	0.0	724.7	0.0775%	(4,045.9)	(5,659.4)	1,608.7	4.8	0	14,504.8
2012	18,522.3	12,397.2	0.2	6,125.3	0.1012%	(2,599.0)	(4,222.6)	1,777.5	(153.9)	0	21,121.3
2011	16,342.0	13,499.5	0.9	2,843.4	0.1115%	(2,915.4)	(4,413.6)	1,625.4	(127.2)	0	19,257.4
2010	13,379.9	13,611.2	0.8	(230.5)	0.1772%	75.0	(847.8)	1,592.6	(669.8)	0	13,304.9
2009	24,706.4	17,865.4	148.0	6,989.0	0.2330%	60,709.0	57,711.8	1,271.1	1,726.1	0	(36,002.6)
2008	7,306.3	4,410.4	1,445.9	4,341.8	0.0418%	44,339.5	41,838.8	1,033.5	1,467.2	0	(37,033.2)
2007	3,196.2	3,730.9	3,088.0	2,553.3	0.0093%	1,090.9	95.0	992.6	3.3	0	2,105.3
2006	2,643.5	31.9	0.0	2,611.6	0.0005%	904.3	(52.1)	950.6	5.8	0	1,739.2
2005	2,420.5	60.9	0.0	2,359.6	0.0010%	809.3	(160.2)	965.7	3.8	0	1,611.2
2004	2,240.3	104.2	0.0	2,136.1	0.0019%	607.6	(353.4)	941.3	19.7	0	1,632.7
2003	2,173.6	94.8	0.0	2,078.8	0.0019%	(67.7)	(1,010.5)	935.5	7.3	0	2,241.3
2002	2,384.7	107.8	0.0	2,276.9	0.0023%	719.6	(243.0)	945.1	17.5	0	1,665.1
2001	2,730.1	83.2	0.0	2,646.9	0.0019%	3,123.4	2,199.3	887.9	36.2	0	(393.3)
2000	2,570.1	64.3	0.0	2,505.8	0.0016%	945.2	28.0	883.9	33.3	0	1,624.9
1999	2,416.7	48.4	0.0	2,368.3	0.0013%	2,047.0	1,199.7	823.4	23.9	0	369.7
1998	2,584.6	37.0	0.0	2,547.6	0.0010%	817.5	(5.7)	782.6	40.6	0	1,767.1
1997	2,165.5	38.6	0.0	2,126.9	0.0011%	247.3	(505.7)	677.2	75.8	0	1,918.2
1996	7,156.8	5,294.2	0.0	1,862.6	0.1622%	353.6	(417.2)	568.3	202.5	0	6,803.2
1995	5,229.2	3,877.0	0.0	1,352.2	0.1238%	202.2	(354.2)	510.6	45.8	0	5,027.0
1994	7,682.1	6,722.7	0.0	959.4	0.2192%	(1,825.1)	(2,459.4)	443.2	191.1	0	9,507.2
1993	7,354.5	6,682.0	0.0	672.5	0.2157%	(6,744.4)	(7,660.4)	418.5	497.5	0	14,098.9
1992	6,479.3	5,758.6	0.0	720.7	0.1815%	(596.8)	(2,274.7)	614.8 ³	1,063.1	35.4	7,111.5
1991	5,886.5	5,254.0	0.0	632.5	0.1613%	16,925.3	15,496.2	326.1	1,103.0	42.4	(10,996.4)
1990	3,855.3	2,872.3	0.0	983.0	0.0868%	13,059.3	12,133.1	275.6	650.6	56.1	(9,147.9)
1989	3,494.8	1,885.0	0.0	1,609.8	0.0816%	4,352.2	3,811.3	219.9	321.0	5.6	(851.8)
1988	3,347.7	1,773.0	0.0	1,574.7	0.0825%	7,588.4	6,298.3	223.9	1,066.2	0	(4,240.7)
1987	3,319.4	1,696.0	0.0	1,623.4	0.0833%	3,270.9	2,996.9	204.9	69.1	0	48.5
1986	3,260.1	1,516.9	0.0	1,743.2	0.0787%	2,963.7	2,827.7	180.3	(44.3)	0	296.4
1985	3,385.5	1,433.5	0.0	1,952.0	0.0815%	1,957.9	1,569.0	179.2	209.7	0	1,427.6
1984	3,099.5	1,321.5	0.0	1,778.0	0.0800%	1,999.2	1,633.4	151.2	214.6	0	1,100.3
1983	2,628.1	1,214.9	164.0	1,577.2	0.0714%	969.9	675.1	135.7	159.1	0	1,658.2
1982	2,524.6	1,108.9	96.2	1,511.9	0.0769%	999.8	126.4	129.9	743.5	0	1,524.8

**INCOME AND EXPENSES, DEPOSIT INSURANCE FUND, FROM BEGINNING OF OPERATIONS,
SEPTEMBER 11, 1933, THROUGH DECEMBER 31, 2018 (continued)**

Dollars in Millions

Year	Income					Expenses and Losses					
	Total	Assessment Income	Assessment Credits	Investment and Other	Effective Assessment Rate ¹	Total	Provision for Ins. Losses	Admin. and Operating Expenses ²	Interest & Other Ins. Expenses	Funding Transfer from the FSLIC Resolution Fund	Net Income/ (Loss)
1981	2,074.7	1,039.0	117.1	1,152.8	0.0714%	848.1	320.4	127.2	400.5	0	1,226.6
1980	1,310.4	951.9	521.1	879.6	0.0370%	83.6	(38.1)	118.2	3.5	0	1,226.8
1979	1,090.4	881.0	524.6	734.0	0.0333%	93.7	(17.2)	106.8	4.1	0	996.7
1978	952.1	810.1	443.1	585.1	0.0385%	148.9	36.5	103.3	9.1	0	803.2
1977	837.8	731.3	411.9	518.4	0.0370%	113.6	20.8	89.3	3.5	0	724.2
1976	764.9	676.1	379.6	468.4	0.0370%	212.3	28.0	180.4 ⁴	3.9	0	552.6
1975	689.3	641.3	362.4	410.4	0.0357%	97.5	27.6	67.7	2.2	0	591.8
1974	668.1	587.4	285.4	366.1	0.0435%	159.2	97.9	59.2	2.1	0	508.9
1973	561.0	529.4	283.4	315.0	0.0385%	108.2	52.5	54.4	1.3	0	452.8
1972	467.0	468.8	280.3	278.5	0.0333%	65.7	10.1	49.6	6.0 ⁵	0	401.3
1971	415.3	417.2	241.4	239.5	0.0345%	60.3	13.4	46.9	0.0	0	355.0
1970	382.7	369.3	210.0	223.4	0.0357%	46.0	3.8	42.2	0.0	0	336.7
1969	335.8	364.2	220.2	191.8	0.0333%	34.5	1.0	33.5	0.0	0	301.3
1968	295.0	334.5	202.1	162.6	0.0333%	29.1	0.1	29.0	0.0	0	265.9
1967	263.0	303.1	182.4	142.3	0.0333%	27.3	2.9	24.4	0.0	0	235.7
1966	241.0	284.3	172.6	129.3	0.0323%	19.9	0.1	19.8	0.0	0	221.1
1965	214.6	260.5	158.3	112.4	0.0323%	22.9	5.2	17.7	0.0	0	191.7
1964	197.1	238.2	145.2	104.1	0.0323%	18.4	2.9	15.5	0.0	0	178.7
1963	181.9	220.6	136.4	97.7	0.0313%	15.1	0.7	14.4	0.0	0	166.8
1962	161.1	203.4	126.9	84.6	0.0313%	13.8	0.1	13.7	0.0	0	147.3
1961	147.3	188.9	115.5	73.9	0.0323%	14.8	1.6	13.2	0.0	0	132.5
1960	144.6	180.4	100.8	65.0	0.0370%	12.5	0.1	12.4	0.0	0	132.1
1959	136.5	178.2	99.6	57.9	0.0370%	12.1	0.2	11.9	0.0	0	124.4
1958	126.8	166.8	93.0	53.0	0.0370%	11.6	0.0	11.6	0.0	0	115.2
1957	117.3	159.3	90.2	48.2	0.0357%	9.7	0.1	9.6	0.0	0	107.6
1956	111.9	155.5	87.3	43.7	0.0370%	9.4	0.3	9.1	0.0	0	102.5
1955	105.8	151.5	85.4	39.7	0.0370%	9.0	0.3	8.7	0.0	0	96.8
1954	99.7	144.2	81.8	37.3	0.0357%	7.8	0.1	7.7	0.0	0	91.9
1953	94.2	138.7	78.5	34.0	0.0357%	7.3	0.1	7.2	0.0	0	86.9
1952	88.6	131.0	73.7	31.3	0.0370%	7.8	0.8	7.0	0.0	0	80.8
1951	83.5	124.3	70.0	29.2	0.0370%	6.6	0.0	6.6	0.0	0	76.9
1950	84.8	122.9	68.7	30.6	0.0370%	7.8	1.4	6.4	0.0	0	77.0
1949	151.1	122.7	0.0	28.4	0.0833%	6.4	0.3	6.1	0.0	0	144.7
1948	145.6	119.3	0.0	26.3	0.0833%	7.0	0.7	6.3 ⁶	0.0	0	138.6
1947	157.5	114.4	0.0	43.1	0.0833%	9.9	0.1	9.8	0.0	0	147.6
1946	130.7	107.0	0.0	23.7	0.0833%	10.0	0.1	9.9	0.0	0	120.7
1945	121.0	93.7	0.0	27.3	0.0833%	9.4	0.1	9.3	0.0	0	111.6
1944	99.3	80.9	0.0	18.4	0.0833%	9.3	0.1	9.2	0.0	0	90.0

INCOME AND EXPENSES, DEPOSIT INSURANCE FUND, FROM BEGINNING OF OPERATIONS, SEPTEMBER 11, 1933, THROUGH DECEMBER 31, 2018 (continued)

Dollars in Millions

Year	Income					Expenses and Losses					
	Total	Assessment Income	Assessment Credits	Investment and Other	Effective Assessment Rate ¹	Total	Provision for Ins. Losses	Admin. and Operating Expenses ²	Interest & Other Ins. Expenses	Funding Transfer from the FSLIC Resolution Fund	Net Income/ (Loss)
1943	86.6	70.0	0.0	16.6	0.0833%	9.8	0.2	9.6	0.0	0	76.8
1942	69.1	56.5	0.0	12.6	0.0833%	10.1	0.5	9.6	0.0	0	59.0
1941	62.0	51.4	0.0	10.6	0.0833%	10.1	0.6	9.5	0.0	0	51.9
1940	55.9	46.2	0.0	9.7	0.0833%	12.9	3.5	9.4	0.0	0	43.0
1939	51.2	40.7	0.0	10.5	0.0833%	16.4	7.2	9.2	0.0	0	34.8
1938	47.7	38.3	0.0	9.4	0.0833%	11.3	2.5	8.8	0.0	0	36.4
1937	48.2	38.8	0.0	9.4	0.0833%	12.2	3.7	8.5	0.0	0	36.0
1936	43.8	35.6	0.0	8.2	0.0833%	10.9	2.6	8.3	0.0	0	32.9
1935	20.8	11.5	0.0	9.3	0.0833%	11.3	2.8	8.5	0.0	0	9.5
1933-34	7.0	0.0	0.0	7.0	N/A	10.0	0.2	9.8	0.0	0	(3.0)

¹ The effective assessment rate is calculated from annual assessment income (net of assessment credits), excluding transfers to the Financing Corporation (FICO), Resolution Funding Corporation (REFCORP) and FSLIC Resolution Fund, divided by the average assessment base. Figures represent only BIF-insured institutions prior to 1990, and BIF- and SAIF-insured institutions from 1990 through 2005. After 1995, all thrift closings became the responsibility of the FDIC and amounts are reflected in the SAIF. Beginning in 2006, figures are for the DIF.

The annualized assessment rate for 2018 is based on full year assessment income divided by a four quarter average of 2018 quarterly assessment base amounts. The assessment base for fourth quarter 2018 was estimated using the third quarter 2018 assessment base and an assumed quarterly growth rate of one percent.

Historical Assessment Rates:

<p>1934 – 1949 The statutory assessment rate was 0.0833 percent.</p> <p>1950 – 1984 The effective assessment rates varied from the statutory rate of 0.0833 percent due to assessment credits provided in those years.</p> <p>1985 – 1989 The statutory assessment rate was 0.0833 percent (no credits were given).</p> <p>1990 The statutory rate increased to 0.12 percent.</p> <p>1991 – 1992 The statutory rate increased to a minimum of 0.15 percent. The effective rates in 1991 and 1992 varied because the FDIC exercised new authority to increase assessments above the statutory minimum rate when needed.</p> <p>1993 – 2006 Beginning in 1993, the effective rate was based on a risk-related premium system under which institutions paid assessments in the range of 0.23 percent to 0.31 percent. In May 1995, the BIF reached the mandatory recapitalization level of 1.25 percent. As a result, BIF assessment rates were reduced to a range of 0.04 percent to 0.31 percent of assessable deposits, effective June 1995, and assessments totaling \$1.5 billion were refunded in September 1995. Assessment rates for the BIF were lowered again to a range of 0 to 0.27 percent of assessable</p>	<p>deposits, effective the start of 1996. In 1996, the SAIF collected a one-time special assessment of \$4.5 billion. Subsequently, assessment rates for the SAIF were lowered to the same range as the BIF, effective October 1996. This range of rates remained unchanged for both funds through 2006.</p> <p>2007 – 2008 As part of the implementation of the Federal Deposit Insurance Reform Act of 2005, assessment rates were increased to a range of 0.05 percent to 0.43 percent of assessable deposits effective at the start of 2007, but many institutions received a one-time assessment credit (\$4.7 billion in total) to offset the new assessments.</p> <p>2009 – 2011 For the first quarter of 2009, assessment rates were increased to a range of 0.12 percent to 0.50 percent of assessable deposits. On June 30, 2009, a special assessment was imposed on all insured banks and thrifts, which amounted in aggregate to approximately \$5.4 billion. For 8,106 institutions, with \$9.3 trillion in assets, the special assessment was 5 basis points of each insured institution's assets minus tier one capital; 89 other institutions, with assets of \$4.0 trillion, had their special assessment capped at 10 basis points of their second quarter assessment base. From the second quarter of 2009 through the first quarter of 2011, initial assessment rates ranged between 0.12 percent and 0.45 percent of assessable deposits. Initial rates are subject to further adjustments.</p>
--	---

2011 – 2016	Beginning in the second quarter of 2011, the assessment base changed to average total consolidated assets less average tangible equity (with certain adjustments for banker's banks and custodial banks), as required by the Dodd-Frank Act. The FDIC implemented a new assessment rate schedule at the same time to conform to the larger assessment base. Initial assessment rates were lowered to a range of 0.05 percent to 0.35 percent of the new base. The annualized assessment rates averaged approximately 17.6 cents per \$100 of assessable deposits for the first quarter of 2011 and 11.1 cents per \$100 of the new base for the last three quarters of 2011 (which is shown in the table).	2016	Beginning July 1, 2016, initial assessment rates were lowered from a range of 5 basis points to 35 basis points to a range of 3 basis points to 30 basis points, and an additional surcharge was imposed on large banks (generally institutions with \$10 billion or more in assets) of 4.5 basis points of their assessment base (after making adjustments).
		2018	The 4.5 basis point surcharge imposed on large banks ended effective October 1, 2018. The annualized assessment rates averaged approximately 7.2 cents per \$100 of the assessable base for the first three quarters of 2018 and 3.5 cents per \$100 of the assessment base for the last quarter of 2018. The full year annualized assessment rate averaged 6.3 cent per \$100 (which is shown in the table).

² These expenses, which are presented as operating expenses in the Statement of Income and Fund Balance, pertain to the FDIC in its corporate capacity only and do not include costs that are charged to the failed bank receiverships that are managed by the FDIC. The receivership expenses are presented as part of the "Receivables from Resolutions, net" line on the Balance Sheet. The narrative and graph presented on page 91 of this report shows the aggregate (corporate and receivership) expenditures of the FDIC.

³ Includes \$210 million for the cumulative effect of an accounting change for certain postretirement benefits (1992).

⁴ Includes a \$106 million net loss on government securities (1976).

⁵ This amount represents interest and other insurance expenses from 1933 to 1972.

⁶ Includes the aggregate amount of \$81 million of interest paid on capital stock between 1933 and 1948.

RECOVERIES AND LOSSES BY THE DEPOSIT INSURANCE FUND ON DISBURSEMENTS FOR THE PROTECTION OF DEPOSITORS, 1934 - 2018

Dollars in Thousands

Bank and Thrift Failures¹

Year ²	Number of Banks/Thrifts	Total Assets ³	Total Deposits ³	Funding ⁴	Recoveries ⁵	Estimated Additional Recoveries	Final and Estimated Losses ⁶
	2,623	\$946,643,412	\$712,938,506	\$586,979,457	\$416,409,979	\$63,951,764	\$106,617,718
2018	0	-	-	-	-	-	-
2017	8	5,081,737	4,683,360	4,589,179	1,712,445	1,724,535	1,152,198
2016	5	277,182	268,516	262,017	12,907	204,981	44,129
2015	8	6,706,038	4,574,170	4,564,024	848,530	2,858,451	857,043
2014	18	2,913,503	2,691,485	2,682,954	475,347	1,815,118	392,489
2013	24	6,044,051	5,132,246	5,022,388	323,205	3,470,020	1,229,163
2012	51	11,617,348	11,009,630	11,041,622	1,782,176	6,822,310	2,437,136
2011	92	34,922,997	31,071,862	30,714,170	3,267,259	20,988,008	6,458,902
2010 ⁷	157	92,084,988	78,290,185	82,305,089	55,641,718	10,456,842	16,206,529
2009 ⁷	140	169,709,160	137,835,121	136,081,390	95,397,606	14,071,401	26,612,383
2008 ⁷	25	371,945,480	234,321,715	205,833,992	184,490,213	3,204,012	18,139,767
2007	3	2,614,928	2,424,187	1,920,159	1,474,822	285,662	159,676
2006	0	0	0	0	0	0	0
2005	0	0	0	0	0	0	0
2004	4	170,099	156,733	139,244	134,978	349	3,917
2003	3	947,317	901,978	883,772	812,933	8,192	62,647
2002	11	2,872,720	2,512,834	1,567,805	1,711,173	(557,357)	413,989
2001	4	1,821,760	1,661,214	21,131	1,138,677	(1,410,011)	292,465
2000	7	410,160	342,584	297,313	265,175	0	32,138
1999	8	1,592,189	1,320,573	1,308,316	718,057	4,233	586,027
1998	3	290,238	260,675	293,117	69,575	1,937	221,606
1997	1	27,923	27,511	25,546	20,520	0	5,026
1996	6	232,634	230,390	201,533	140,918	0	60,615
1995	6	802,124	776,387	609,043	524,571	0	84,472
1994	13	1,463,874	1,397,018	1,224,769	1,045,718	0	179,051
1993	41	3,828,939	3,509,341	3,841,658	3,209,012	0	632,646
1992	120	45,357,237	39,921,310	14,541,476	10,866,760	567	3,674,149
1991	124	64,556,512	52,972,034	21,501,749	15,496,730	2,512	6,002,507
1990	168	16,923,462	15,124,454	10,812,484	8,040,995	0	2,771,489
1989	206	28,930,572	24,152,468	11,443,281	5,247,995	0	6,195,286
1988	200	38,402,475	26,524,014	10,432,655	5,055,158	0	5,377,497
1987	184	6,928,889	6,599,180	4,876,994	3,014,502	0	1,862,492
1986	138	7,356,544	6,638,903	4,632,121	2,949,583	0	1,682,538
1985	116	3,090,897	2,889,801	2,154,955	1,506,776	0	648,179
1984	78	2,962,179	2,665,797	2,165,036	1,641,157	0	523,879
1983	44	3,580,132	2,832,184	3,042,392	1,973,037	0	1,069,355
1982	32	1,213,316	1,056,483	545,612	419,825	0	125,787
1981	7	108,749	100,154	114,944	105,956	0	8,988
1980	10	239,316	219,890	152,355	121,675	0	30,680
1934 - 1979	558	8,615,743	5,842,119	5,133,173	4,752,295	0	380,878

**RECOVERIES AND LOSSES BY THE DEPOSIT INSURANCE FUND ON DISBURSEMENTS
FOR THE PROTECTION OF DEPOSITORS, 1934 - 2018 (continued)**

Dollars in Thousands

Assistance Transactions¹

Year ²	Number of Banks/ Thrifts	Total Assets ³	Total Deposits ³	Funding ⁴	Recoveries ⁵	Estimated Additional Recoveries	Final and Estimated Losses ⁶
	154	\$3,317,099,253	\$1,442,173,417	\$11,630,356	\$6,199,875	\$0	\$5,430,481
2018	0	0	0	0	0	0	0
2017	0	0	0	0	0	0	0
2016	0	0	0	0	0	0	0
2015	0	0	0	0	0	0	0
2014	0	0	0	0	0	0	0
2013	0	0	0	0	0	0	0
2012	0	0	0	0	0	0	0
2011	0	0	0	0	0	0	0
2010	0	0	0	0	0	0	0
2009 ⁸	8	1,917,482,183	1,090,318,282	0	0	0	0
2008 ⁸	5	1,306,041,994	280,806,966	0	0	0	0
2007	0	0	0	0	0	0	0
2006	0	0	0	0	0	0	0
2005	0	0	0	0	0	0	0
2004	0	0	0	0	0	0	0
2003	0	0	0	0	0	0	0
2002	0	0	0	0	0	0	0
2001	0	0	0	0	0	0	0
2000	0	0	0	0	0	0	0
1999	0	0	0	0	0	0	0
1998	0	0	0	0	0	0	0
1997	0	0	0	0	0	0	0
1996	0	0	0	0	0	0	0
1995	0	0	0	0	0	0	0
1994	0	0	0	0	0	0	0
1993	0	0	0	0	0	0	0
1992	2	33,831	33,117	1,486	1,236	0	250
1991	3	78,524	75,720	6,117	3,093	0	3,024
1990	1	14,206	14,628	4,935	2,597	0	2,338
1989	1	4,438	6,396	2,548	252	0	2,296
1988	80	15,493,939	11,793,702	1,730,351	189,709	0	1,540,642

**RECOVERIES AND LOSSES BY THE DEPOSIT INSURANCE FUND ON DISBURSEMENTS
FOR THE PROTECTION OF DEPOSITORS, 1934 - 2018 (continued)**

Dollars in Thousands

Assistance Transactions¹ (continued)

Year ²	Number of Banks/ Thrifts	Total Assets ³	Total Deposits ³	Funding ⁴	Recoveries ⁵	Estimated Additional Recoveries	Final and Estimated Losses ⁶
1987	19	2,478,124	2,275,642	160,877	713	0	160,164
1986	7	712,558	585,248	158,848	65,669	0	93,179
1985	4	5,886,381	5,580,359	765,732	406,676	0	359,056
1984	2	40,470,332	29,088,247	5,531,179	4,414,904	0	1,116,275
1983	4	3,611,549	3,011,406	764,690	427,007	0	337,683
1982	10	10,509,286	9,118,382	1,729,538	686,754	0	1,042,784
1981	3	4,838,612	3,914,268	774,055	1,265	0	772,790
1980	1	7,953,042	5,001,755	0	0	0	0
1934-1979	4	1,490,254	549,299	0	0	0	0

¹ Institutions for which the FDIC is appointed receiver, including deposit payoff, insured deposit transfer, and deposit assumption cases.

² For 1990 through 2005, amounts represent the sum of BIF and SAIF failures (excluding those handled by the RTC); prior to 1990, figures are only for the BIF. After 1995, all thrift closings became the responsibility of the FDIC and amounts are reflected in the SAIF. For 2006 to 2018, figures are for the DIF.

³ Assets and deposit data are based on the last Call Report or TFR filed before failure.

⁴ Funding represents the amounts provided by the DIF to receiverships for subrogated claims, advances for working capital, and administrative expenses paid on their behalf. Beginning in 2008, the DIF resolves failures using whole-bank purchase and assumption transactions, most with an accompanying shared-loss agreement (SLA). The DIF satisfies any resulting liabilities by offsetting receivables from resolutions when receiverships declare a dividend and/or sending cash directly to receiverships to fund an SLA and other expenses.

⁵ Recoveries represent cash received and dividends (cash and non-cash) declared by receiverships.

⁶ Final losses represent actual losses for unreimbursed subrogated claims of inactivated receiverships. Estimated losses generally represent the difference between the amount paid by the DIF to cover obligations to insured depositors and the estimated recoveries from the liquidation of receivership assets.

⁷ Includes amounts related to transaction account coverage under the Transaction Account Guarantee Program (TAG). The estimated losses as of December 31, 2018, for TAG accounts in 2010, 2009, and 2008 are \$372 million, \$1.1 billion, and \$12 million, respectively.

⁸ Includes institutions where assistance was provided under a systemic risk determination.

**NUMBER, ASSETS, DEPOSITS, LOSSES, AND LOSS TO FUNDS OF INSURED
THRIFTS TAKEN OVER OR CLOSED BECAUSE OF FINANCIAL DIFFICULTIES,
1989 THROUGH 1995¹**
Dollars in Thousands

Year	Number of Institutions	Assets	Deposits	Final Receivership Loss ²	Loss to Fund ³
Total	748	\$393,986,574	\$318,328,770	\$75,977,846	\$81,580,554
1995	2	423,819	414,692	28,192	27,750
1994	2	136,815	127,508	11,472	14,599
1993	10	6,147,962	5,708,253	267,595	65,212
1992	59	44,196,946	34,773,224	3,286,908	3,832,145
1991	144	78,898,904	65,173,122	9,235,967	9,734,263
1990	213	129,662,498	98,963,962	16,062,685	19,257,578
1989 ⁴	318	134,519,630	113,168,009	47,085,027	48,649,007

¹ Beginning in 1989 through July 1, 1995, all thrift closings were the responsibility of the Resolution Trust Corporation (RTC). Since the RTC was terminated on December 31, 1995, and all assets and liabilities transferred to the FSLIC Resolution Fund (FRF), all the results of the thrift closing activity from 1989 through 1995 are now reflected on the FRF's books. Year is the year of failure, not the year of resolution.

² The Final Receivership Loss represents the loss at the fund level from receiverships for unreimbursed subrogated claims of the FRF-RTC and unpaid advances to receiverships from the FRF-RTC.

³ The Loss to Fund represents the total resolution cost of the failed thrifts in the FRF-RTC fund. In addition to the receivership losses, this includes corporate revenue and expense items such as interest expense on Federal Financing Bank debt, interest expense on escrowed funds, administrative expenses, and interest revenue on advances to receiverships.

⁴ Total for 1989 excludes nine failures of the former FSLIC.

B. MORE ABOUT THE FDIC

FDIC Board of Directors

Jelena McWilliams



Jelena McWilliams is the 21st Chairman of the FDIC. She was nominated by President Donald J. Trump on November 30, 2017, and confirmed by the Senate on May 24,

2018, to serve a six-year term on the FDIC Board of Directors, and designated as Chairman for a term of five years.

Ms. McWilliams was Executive Vice President, Chief Legal Officer, and Corporate Secretary for Fifth Third Bank in Cincinnati, Ohio. Prior to joining Fifth Third Bank, Ms. McWilliams worked in the United States Senate for six years, most recently as Chief Counsel and Deputy Staff Director with the Senate Committee on Banking, Housing and Urban Affairs, and previously as Assistant Chief Counsel with the Senate Small Business and Entrepreneurship Committee. From 2007 to 2010, Ms. McWilliams served as an attorney at the Federal Reserve Board of Governors. Before entering public service, she practiced corporate and securities law at Morrison & Foerster LLP in Palo Alto, California, and Hogan & Hartson LLP (now Hogan Lovells LLP) in Washington, D.C.

Ms. McWilliams graduated with highest honors from the University of California at Berkeley with a B.S. in political science, and earned her law degree from U.C. Berkeley School of Law.

Martin J. Gruenberg



Martin J. Gruenberg is the 20th Chairman of the FDIC, receiving Senate confirmation on November 15, 2012, for a five-year term. Mr. Gruenberg served as Vice Chairman and Member of the FDIC Board of Directors from August 22, 2005, until his confirmation

as Chairman. He served as Acting Chairman from July 9, 2011, to November 15, 2012, and also from November 16, 2005, to June 26, 2006.

Mr. Gruenberg joined the FDIC Board after broad congressional experience in the financial services and regulatory areas. He served as Senior Counsel to Senator Paul S. Sarbanes (D-MD) on the staff of the Senate Committee on Banking, Housing, and Urban Affairs from 1993 to 2005. Mr. Gruenberg advised the Senator on issues of domestic and international financial regulation, monetary policy, and trade. He also served as Staff Director of the Banking Committee's Subcommittee on International Finance and Monetary Policy from 1987 to 1992. Major legislation in which Mr. Gruenberg played an active role during his service on the Committee includes the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA); the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA); the Gramm-Leach-Bliley Act; and the Sarbanes-Oxley Act of 2002.

Mr. Gruenberg served as Chairman of the Executive Council and President of the International Association of Deposit Insurers (IADI) from November 2007 to November 2012.

Mr. Gruenberg holds a J.D. from Case Western Reserve Law School and an A.B. from Princeton University, Woodrow Wilson School of Public and International Affairs.

Kathleen L. Kraninger



Kathy Kraninger became Director of the Consumer Financial Protection Bureau (CFPB) in December, 2018. From her early days as a Peace Corps volunteer, to her role establishing the Department of Homeland Security (DHS), to her policy

work at the Office of Management and Budget (OMB) to the CFPB, Director Kraninger has dedicated her career to public service.

Director Kraninger came to the CFPB from OMB, where as a Policy Associate Director she oversaw the budgets for executive branch agencies including the Departments of Commerce, Justice, DHS, Housing and Urban Development, Department of Transportation (DOT), and the Department of Treasury, in addition to 30 other government agencies.

Previously she worked in the U.S. Senate, where she was the Clerk for the Senate Appropriations Subcommittee on Homeland Security, which provides DHS with its \$40 billion discretionary budget. On Capitol Hill, she also worked for the House Appropriations Subcommittee on Homeland Security as well as the Senate Homeland Security and Governmental Affairs Committee.

Ms. Kraninger also served in executive branch posts with DOT. There, after the terrorist attacks on September 11, 2001, she volunteered to join the leadership team that set up the newly created DHS.

Her work at DHS led to awards including the Secretary of Homeland Security's Award of Exceptional Service, the International Police and Public Safety 9/11 Medal, and the Meritorious Public Service Award from the United States Coast Guard.

Ms. Kraninger graduated magna cum laude from Marquette University and earned a law degree from Georgetown University Law Center. She served as a U.S. Peace Corps Volunteer in Ukraine.

Joseph M. Otting



Joseph M. Otting was sworn in as the 31st Comptroller of the Currency on November 27, 2017.

The Comptroller of the Currency is the administrator of the federal banking system and chief officer of the Office of the Comptroller of the Currency (OCC).

The OCC supervises nearly 1,400 national banks, federal savings associations, and federal branches and agencies of foreign banks operating in the United States. The mission of the OCC is to ensure that national banks and federal savings associations operate in a safe and sound manner, provide fair access to financial services, treat customers fairly, and comply with applicable laws and regulations.

The Comptroller also serves as a director of the Federal Deposit Insurance Corporation and member of the Financial Stability Oversight Council and the Federal Financial Institutions Examination Council.

Prior to becoming Comptroller of the Currency, Mr. Otting was an executive in the banking industry. He served as President of CIT Bank and Co-President of CIT Group.

Mr. Otting previously was President, Chief Executive Officer, and a member of the Board of Directors of OneWest Bank, N.A. Prior to joining OneWest

Bank, he served as Vice Chairman of U.S. Bancorp, where he managed the Commercial Banking Group and served on the Bancorp's executive management committee. He also served as a member of U.S. Bank's main subsidiary banks' Board of Directors.

From 1986 to 2001, Mr. Otting was with Union Bank of California, where he was Executive Vice President and Group Head of Commercial Banking. Before joining Union Bank, he was with Bank of America and held positions in branch management, preferred banking, and commercial lending.

Mr. Otting has played significant roles in charitable and community development organizations. He has served as a board member for the California Chamber of Commerce, the Killebrew-Thompson Memorial foundation, the Associated Oregon Industries, the Oregon Business Council, the Portland Business Alliance, the Minnesota Chamber of Commerce, and Blue Cross Blue Shield of Oregon. He was also a member of the Financial Services Roundtable, the Los Angeles Chamber of Commerce, and the Board and Executive Committee of the Los Angeles Economic Development Corporation.

Mr. Otting holds a bachelor of arts in management from the University of Northern Iowa and is a graduate of the School of Credit and Financial Management, which was held at Dartmouth College in Hanover, New Hampshire.

Mick Mulvaney



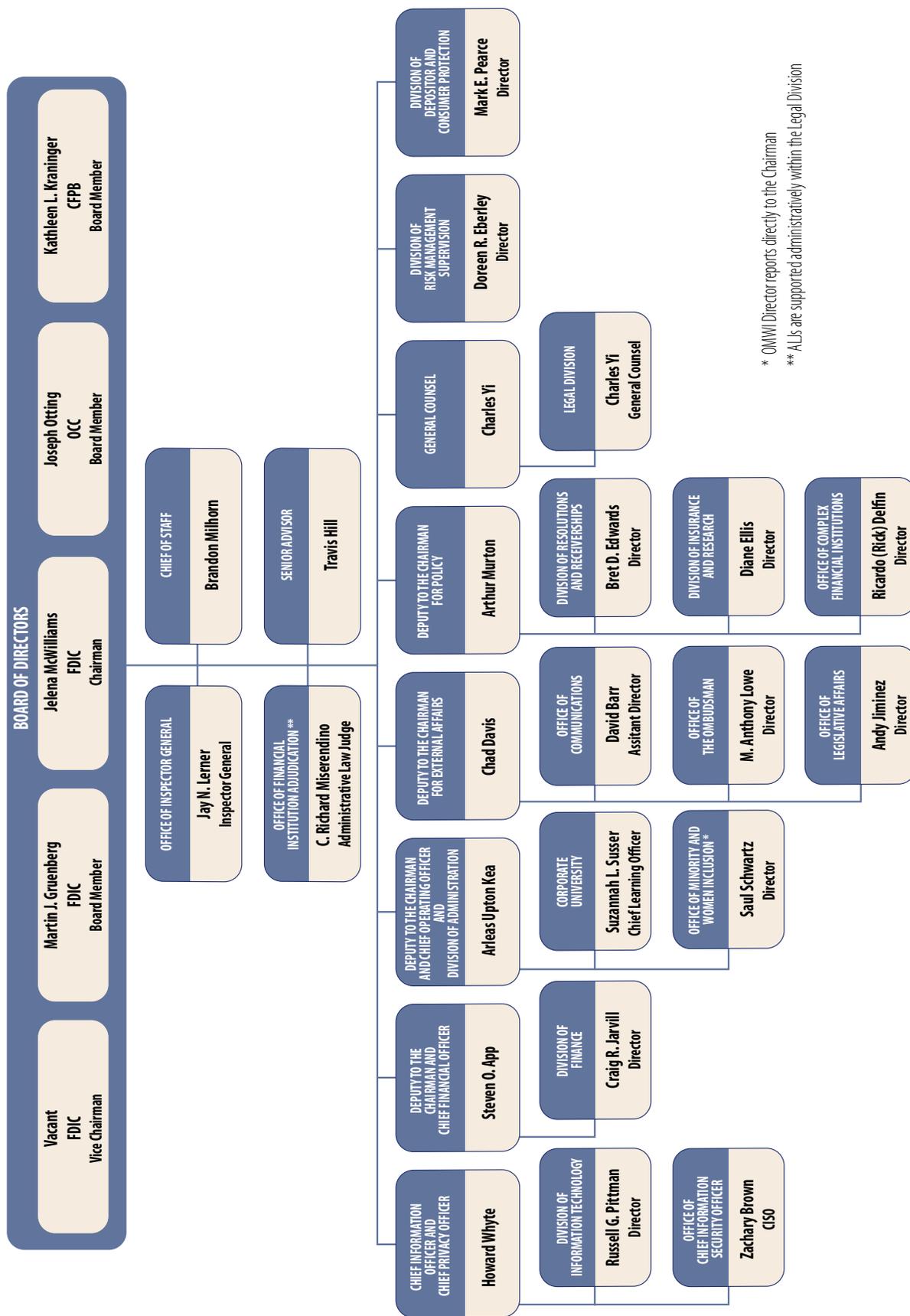
Mick Mulvaney, former Acting Director of the Consumer Financial Protection Bureau, resigned from the FDIC Board of Directors as of December 11, 2018. Mr. Mulvaney had been a Board member since November 25, 2017.

Thomas M. Hoenig



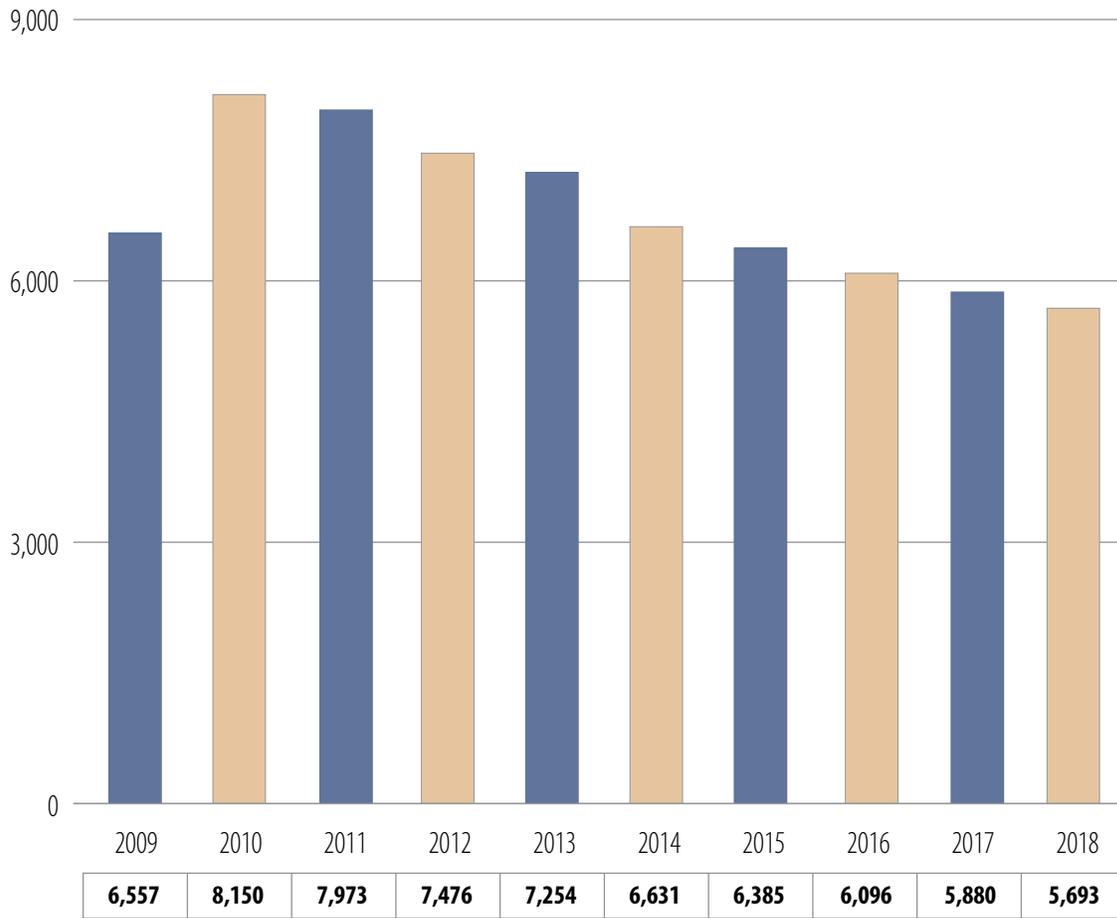
Thomas M. Hoenig, former Vice Chairman, resigned on April 30, 2018. Mr. Hoenig served a six-year term as FDIC Vice Chairman and member of the Board of Directors.

FDIC ORGANIZATION CHART/OFFICIALS



* OMI Director reports directly to the Chairman
 ** ALJs are supported administratively within the Legal Division

**CORPORATE STAFFING
STAFFING TRENDS 2009-2018**



FDIC Year-End On-Board Staffing

Notes: 2009-2018 staffing totals reflect year-end full time equivalent staff.

NUMBER OF EMPLOYEES BY DIVISION/OFFICE 2017 AND 2018 (YEAR-END)¹

Division or Office:	Total		Washington		Regional	
	2018	2017	2018	2017	2018	2017
Division of Risk Management Supervision	2,499	2,558	207	197	2,293	2,361
Division of Depositor and Consumer Protection	816	831	122	120	694	711
Division of Resolutions and Receiverships	387	457	119	134	268	323
Legal Division	474	506	314	326	160	180
Division of Administration	353	358	246	246	108	112
Division of Information Technology	280	276	216	219	64	57
Corporate University	204	217	197	211	7	6
Division of Insurance and Research	204	194	168	157	36	37
Division of Finance	164	166	160	162	4	4
Office of the Chief Information Security Officer ²	37	36	37	36	0	0
Office of Inspector General	126	126	80	78	46	48
Office of Complex Financial Institutions	62	62	49	48	13	14
Executive Offices ³	20	26	20	26	0	0
Executive Support Offices ⁴	67	68	60	60	7	8
TOTAL	5,693	5,880	1,994	2,019	3,699	3,861

¹ The FDIC reports staffing totals using a full-time equivalent methodology, which is based on an employee's scheduled work hours. Division/Office staffing has been rounded to the nearest whole FTE. Totals may not foot due to rounding.

² Formerly known as the Information Security and Privacy Staff.

³ Includes the Offices of the Chairman, Vice Chairman, Director (Appointive), Chief Operating Officer, Chief Financial Officer, Chief Policy Officer, External Affairs, and Chief Information Officer.

⁴ Includes the Offices of Legislative Affairs, Communications, Ombudsman, Financial Adjudication, and Minority and Women Inclusion.

SOURCES OF INFORMATION

FDIC Website

www.fdic.gov

A wide range of banking, consumer, and financial information is available on the FDIC's website. This includes the FDIC's Electronic Deposit Insurance Estimator (EDIE), which estimates an individual's deposit insurance coverage; the Institution Directory, which contains financial profiles of FDIC-insured institutions; Community Reinvestment Act evaluations and ratings for institutions supervised by the FDIC; Call Reports, which are bank reports of condition and income; and *Money Smart*, a training program to help individuals outside the financial mainstream enhance their money management skills and create positive banking relationships. Readers also can access a variety of consumer pamphlets, FDIC press releases, speeches, and other updates on the agency's activities, as well as corporate databases and customized reports of FDIC and banking industry information.

FDIC Call Center

Phone: 877-275-3342 (877-ASK-FDIC)
703-562-2222

Hearing Impaired: 800-925-4618
703-562-2289

The FDIC Call Center in Washington, DC, is the primary telephone point of contact for general questions from the banking community, the public, and FDIC employees. The Call Center directly, or with other FDIC subject-matter experts, responds to questions about deposit insurance and other consumer issues and concerns, as well as questions about FDIC programs and activities. The Call Center also refers callers to other federal and state agencies as needed. Hours of operation are 8:00 a.m. to 8:00 p.m., Eastern Time, Monday – Friday, and 9:00 a.m. to 5:00 p.m., Saturday – Sunday. Recorded information about deposit insurance and other topics is available 24 hours a day at the same telephone number.

As a customer service, the FDIC Call Center has many bilingual Spanish agents on staff and has access to a translation service, which is able to assist with over 40 different languages.

Public Information Center

3501 Fairfax Drive
Room E-1021
Arlington, VA 22226

Phone: 877-275-3342 (877-ASK-FDIC),
703-562-2200

Fax: 703-562-2296

FDIC Online Catalog: <https://catalog.fdic.gov>

E-mail: publicinfo@fdic.gov

Publications such as *FDIC Quarterly and Consumer News* and a variety of deposit insurance and consumer pamphlets are available at www.fdic.gov or may be ordered in hard copy through the FDIC online catalog. Other information, press releases, speeches and congressional testimony, directives to financial institutions, policy manuals, and FDIC documents are available on request through the Public Information Center. Hours of operation are 9:00 a.m. to 4:00 p.m., Eastern Time, Monday – Friday.

Office of the Ombudsman

3501 Fairfax Drive
Room E-2022
Arlington, VA 22226

Phone: 877-275-3342 (877-ASK-FDIC)

Fax: 703-562-6057

E-mail: ombudsman@fdic.gov

The Office of the Ombudsman (OO) is an independent, neutral, and confidential resource and liaison for the banking industry and the general public. The OO responds to inquiries about the FDIC in a fair, impartial, and timely manner. It researches questions and fields complaints from bankers and bank customers. OO representatives are present at all bank closings to provide accurate information to bank customers, the media, bank employees, and the general public. The OO also recommends ways to improve FDIC operations, regulations, and customer service.

REGIONAL AND AREA OFFICES

Atlanta Regional Office

Michael J. Dean, Regional Director
10 Tenth Street, NE
Suite 800
Atlanta, Georgia 30309
(678) 916-2200

Alabama
Florida
Georgia
North Carolina
South Carolina
Virginia
West Virginia

Dallas Regional Office

Kristie K. Elmquist, Regional Director
1601 Bryan Street
Dallas, Texas 75201
(214) 754-0098

Colorado
New Mexico
Oklahoma
Texas

Kansas City Regional Office

James D. LaPierre, Regional Director
1100 Walnut Street
Suite 2100
Kansas City, Missouri 64106
(816) 234-8000

Iowa
Kansas
Minnesota
Missouri
Nebraska
North Dakota
South Dakota

Chicago Regional Office

John P. Conneely, Regional Director
300 South Riverside Plaza
Suite 1700
Chicago, Illinois 60606
(312) 382-6000

Illinois
Indiana
Kentucky
Michigan
Ohio
Wisconsin

Memphis Area Office

Kristie K. Elmquist, Director
6060 Primacy Parkway
Suite 300
Memphis, Tennessee 38119
(901) 685-1603

Arkansas
Louisiana
Mississippi
Tennessee

New York Regional Office

John F. Vogel, Regional Director
350 Fifth Avenue
Suite 1200
New York, New York 10118
(917) 320-2500

Delaware
District of Columbia
Maryland
New Jersey
New York
Pennsylvania
Puerto Rico
Virgin Islands

Boston Area Office

John F. Vogel, Director
15 Braintree Hill Office Park
Suite 100
Braintree, Massachusetts 02184
(781) 794-5500

Connecticut
Maine
Massachusetts
New Hampshire
Rhode Island
Vermont

San Francisco Regional Office

Kathy L. Moe, Regional Director
25 Jessie Street at Ecker Square
Suite 2300
San Francisco, California 94105
(415) 546-0160

Alaska
American Samoa
Arizona
California
Federated States of Micronesia
Guam
Hawaii
Idaho
Montana
Nevada
Oregon
Utah
Washington
Wyoming

C. OFFICE OF INSPECTOR GENERAL'S ASSESSMENT OF THE MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE FDIC



Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

February 2019



Federal Deposit Insurance Corporation
Office of Inspector General

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT

INTRODUCTION

Each year, Federal Inspectors General are required to identify and report on the top challenges facing their respective agencies, pursuant to the Reports Consolidation Act of 2000. The Office of Inspector General (OIG) is therefore issuing this report, which identifies the Top Management and Performance Challenges (TMPC) facing the Federal Deposit Insurance Corporation (FDIC).

This TMPC report is based upon the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and other relevant literature, perspectives from Government agencies and officials, and information from private-sector entities. We considered this body of information in light of the current operating environment and circumstances and our independent judgment.

The FDIC faces Challenges in several critical areas, a number of which remain from previous years:

- Enhancing Oversight of Banks' Cybersecurity Risk;
- Adapting to Financial Technology Innovation;
- Strengthening FDIC Information Security Management;
- Preparing for Crises;
- Maturing Enterprise Risk Management;
- Sharing Threat Information with Banks and Examiners;
- Managing Human Capital;
- Administering the Acquisitions Process; and
- Improving Measurement of Regulatory Costs and Benefits.

We believe that the FDIC should focus its attention on these Challenges, and we hope that this document informs policymakers, including the FDIC and Congressional oversight bodies, and the American public about the programs and operations at the FDIC and the Challenges it faces.

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

1 | ENHANCING OVERSIGHT OF BANKS' CYBERSECURITY RISK

Cybersecurity continues to be a critical risk facing the financial sector. Cyber risks can affect the safety and soundness of institutions and lead to the failure of banks, thus causing losses to the FDIC's Deposit Insurance Fund. For example, a cybersecurity incident could disrupt services at a bank, resulting in the exploitation of personal information in fraudulent or other illicit schemes, and an incident could start a contagion that spreads through established interconnected banking relationships. Despite increased spending on cybersecurity, banks are encountering difficulties in getting ahead of the increased frequency and sophistication of cyberattacks. The FDIC's information technology (IT) examinations should ensure strong management practices within financial institutions and at their service providers.

According to the Group of 7 industrialized countries, "cybersecurity risks to the global financial system are of critical concern," and attacks in cyberspace are "increasing in sophistication, frequency, and persistence, cyber risks are growing more dangerous and diverse, threatening to disrupt our interconnected global financial systems and the institutions that operate and support those systems."¹ The Office of the Comptroller of the Currency (OCC) echoed this sentiment in its *Semiannual Risk Perspective* (Fall 2018), finding that cybersecurity threats "target operational vulnerabilities that could expose large quantities of personally identifiable information and proprietary intellectual property, facilitate misappropriation of funds and data at the retail and wholesale levels, corrupt information, and disrupt business activities."² The Financial Stability Oversight Council (FSOC) similarly recognized in its 2018 Annual Report that as financial institutions increase their reliance on technology, there is an increased risk that a cybersecurity event could have "severe negative consequences, potentially entailing systemic implications for the financial sector and the U.S. economy."³

In February 2018, the White House Council of Economic Advisors estimated that the United States economy loses between \$57 and \$109 billion per year to malicious cyber activity. Cyberattacks—such as distributed denial of service and ransomware—may be global in nature and have disrupted financial services in several countries around the world.⁴ Verizon Communications conducted its annual review of global data breaches across multiple sectors, including the financial sector, and reported that there were more than 53,000 security incidents and 2,200 data breaches across 65 countries between April 2017 and April 2018.⁵ This review also found that these cyberattacks happen very quickly, and often surreptitiously; nearly

¹ Group of 7, *Fundamental Elements of Cybersecurity for the Financial Sector*, (October 2016). The Group of 7—Canada, France, Germany, Italy, Japan, The United Kingdom, and the United States—meet annually to discuss issues of global economic governance.

² OCC *Semiannual Risk Perspective*, (Fall 2018), 16.

³ The *Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010* established the FSOC, which has responsibility for identifying risks and responding to emerging threats to financial stability. The FSOC brings together the expertise of Federal financial regulators (including the FDIC), an independent insurance expert, and state regulators.

⁴ World Bank Group, *Financial Sector's Cybersecurity: Regulations and Supervision* (2018), 1.

⁵ Verizon Communications Inc., *2018 Verizon Communications Data Breach Investigations Report*, 11th Edition (April 2018).

**OFFICE OF INSPECTOR GENERAL'S
ASSESSMENT (continued)**

90 percent of the reported breaches occurred within seconds, and about 70 percent went undiscovered for months.

The American Bankers Association also noted that “as businesses ramp up their cybersecurity efforts, threat vectors such as ransomware have become more frequent and potent, affecting companies in nearly every sector and posing significant risk to financial institutions.”⁶ One study by the U.S. Chamber of Commerce and FICO (Fair Isaac Corporation) evaluated the cyber risk at 2,574 U.S. firms across ten sectors, including the financial sector. This study provided cybersecurity ranking scores from 300 (high risk) to 850 (low risk) for each sector as well as a national average. The cyber risks faced by the finance and banking sector exceeded eight other sectors and the national average, as shown in Figure 1.

Figure 1: Cyber Risk Scores Across Ten Sectors



Source: U.S. Chamber of Commerce and FICO, *Assessment of Business Cybersecurity (Q4 2018)*.

IT Examination Programs and Resources

The FDIC Rules and Regulations, Part 364, Appendix B contains *Interagency Guidelines Establishing Information Security Standards* for bank regulators that state that an insured financial institution must “implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities.”⁷ The FDIC and other regulators conduct IT examinations using the Uniform Rating System for Information

⁶ American Bankers Association Journal, *Top Bank Risks in 2018* (December 11, 2017).

⁷ 12 C.F.R. Part 364, Appendix B. The FDIC, OCC, and Board of Governors of the Federal Reserve issued the *Interagency Guidelines Establishing Information Security Standards*.

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

Technology created by the Federal Financial Institutions Examination Council (FFIEC).⁸ The primary purpose of the rating system is to assess risks introduced by information technology at institutions and service providers, and to identify those institutions requiring supervisory attention.⁹ When examinations identify risks and weak management practices at institutions, regulators may use enforcement procedures to address such risks.¹⁰

The FDIC uses the Information Technology Risk Examinations (InTREx) work program to conduct IT examinations at financial institutions. The FDIC introduced InTREx in 2016 to enhance IT supervision by providing examiners with more efficient and risk-focused examination procedures.¹¹ From January 2016 through October 2018, FDIC examiners conducted more than 3,000 InTREx examinations by reviewing bank documentation, interviewing key personnel, testing controls, and observing. According to the Division of Risk Management Supervision (RMS) officials, FDIC personnel and other regulators are considering InTREx enhancements to increase the effectiveness of the work program. One example would be using data to review and understand cybersecurity risks across all institutions.

InTREx examinations required more hours than the prior examination methodology and impacted the FDIC's ongoing challenge to ensure that it has an appropriate number of IT examiners. For example, the New York Regional Office stated that the InTREx examination process increased an average of 67 percent over the prior IT examinations, thus adding an extra 80 hours to the examination. In its operating budget for 2019, the FDIC added 23 positions to its IT examination workforce in recognition of growing cybersecurity risks, including those posed by TSPs.

Another challenge is keeping examiner skills current and up-to-date. The FDIC aims to match examiner skills with the complexity and sophistication of IT environments at banks. Changes in technology can affect the risk profile of an individual bank. For example, in the planning phase of an IT examination, the FDIC may find that the risk profile of a bank has increased and is greater than previous FDIC projections. Therefore, the FDIC may be required to shift examination staffing resources on short notice. We have work underway to review IT examination staffing and the effectiveness of IT examinations.

Third-Party Service Providers

In addition, banks frequently hire third-party Technology Service Providers (TSP) to perform operational functions on behalf of the bank—such as IT operations and business product lines.

⁸ The FFIEC was established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Public Law 95-630. The Council is an interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the FDIC, the National Credit Union Administration, the OCC, and the Bureau of Consumer Financial Protection and to make recommendations to promote uniformity in the supervision of financial institutions.

⁹ FFIEC, *Uniform Rating System for Information Technology*, 64 Fed. Reg. 3109 (January 20, 1999).

¹⁰ FDIC, *Risk Management Manual of Examination Policies*, Part I 1.1 Basic Examination Concepts and Guidelines and Part IV Administrative Enforcement Actions.

¹¹ Financial Institution Letter-43-2016, *Information Technology Risk Examination (InTREx) Program* (June 30, 2016).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

TSPs may further sub-contract services to other vendors. According to the OCC, banks are increasingly reliant upon TSPs and sub-contractors, and such dependence creates a high level of risk for the banking industry.¹² The OCC indicates that TSPs are increasingly targets for cybercrimes and espionage and may provide avenues for bad actors to exploit a bank's systems and operations. For example, on December 20, 2018, two Chinese nationals were charged with computer intrusion offenses related to more than 45 service providers whose clients included the banking and finance industry and the U.S. Government. The hackers targeted service providers in order to gain unauthorized access to the computer networks of their clients and steal intellectual property and confidential business information.¹³

A financial institution must manage the interconnections, system interfaces, and systems access of TSPs and sub-contractors and must implement appropriate controls.¹⁴ Significant consolidation among TSPs caused large numbers of banks—especially community banks supervised by the FDIC—to rely on a few large service providers for core systems and operations support.¹⁵ As a result, a cybersecurity incident at one TSP has the potential to affect multiple financial institutions.¹⁶

FDIC examiners assess financial institutions' management of TSP risk through InTREx IT examinations.¹⁷ The *Interagency Guidelines Establishing Information Security Standards* require that financial institutions:

- Exercise appropriate due diligence in selecting TSPs;
- Require TSPs to implement appropriate measures to meet the Interagency Guidelines objectives related to protecting against unauthorized access to, or use of, sensitive customer information; and
- Monitor contract compliance by the TSPs, including service provider audits, test results summaries, or other evaluations.¹⁸

A financial institution's Board of Directors and senior managers are responsible for the oversight of activities conducted by a TSP on their behalf to the same extent as if the activity were handled within the institution.¹⁹

¹² The FFIEC described the term TSP to include "independent third parties, joint venture/limited liability corporations, and bank and credit union service corporations that provide processing services to financial institutions." [Supervision of Technology Service Providers, FFIEC IT Examination Handbook InfoBase.](#)

¹³ Department of Justice Press Release, [Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information](#) (December 20, 2018).

¹⁴ OCC *Semiannual Risk Perspective* (Spring 2018), 18.

¹⁵ OCC *Semiannual Risk Perspective* (Spring 2018), 18.

¹⁶ OCC *Semiannual Risk Perspective* (Spring 2018), 18.

¹⁷ TSPs are also subject to interagency examination by Federal regulators, including the FDIC. See Federal Regulatory Agencies' Administrative Guidelines, Implementation of Interagency Programs for the Supervision of Technology Service Providers (October 2012).

¹⁸ These Interagency Guidelines can be found in the FDIC Rules and Regulations, Part 364, Appendix B.

¹⁹ Financial Institution Letter 44-2008, *Guidance for Managing Third-Party Risk* (June 6, 2008).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

In our prior OIG report entitled [Technology Service Provider Contracts with FDIC-Supervised Institutions](#) (2017), we did not see evidence, in the form of risk assessments or contract due diligence, that sampled financial institutions fully considered and assessed the potential impact and risk of TSPs. We made two recommendations to the FDIC. Although both remain unimplemented at the time of completion of this Top Challenges report, the FDIC has been working to address the recommendations.²⁰ We plan to conduct additional work in this area to assess whether FDIC programs ensure that institutions are properly managing risks associated with third-party relationships.

The FDIC plays an important role in addressing financial institutions' cybersecurity risk which, if left unchecked, could threaten the safety and soundness of institutions as well as the stability of the financial system. The FDIC must ensure that IT examinations assess how financial institutions manage cybersecurity risks, including risks associated with TSPs, and address such risks through effective supervisory strategies.

2 | ADAPTING TO FINANCIAL TECHNOLOGY INNOVATION

FDIC policymakers and examiners must keep pace with the adoption of new financial technology to assess its impact on the safety and soundness of institutions and the stability of the banking system. The pace of change and breadth of innovation requires that the FDIC create agile and nimble regulatory processes, so that it can respond to, and adjust policies, examination processes, supervisory strategies, preparedness and readiness, and resolution approaches, as needed.

The Group of Twenty's Financial Stability Board (FSB) defined financial technology as "innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services."²¹ Financial technology innovation includes, for example, mobile wallets, digital currencies, and digital financial advice.²² The rapid pace of financial technology is being driven

²⁰ The [FDIC's OIG's Report on Unimplemented Recommendations](#) contains information about recommendations from our audits and evaluations that the OIG has not closed because our Office has not determined that the FDIC has fully implemented recommended corrective actions. The status of each recommendation is subject to change due to the FDIC's ongoing efforts to implement them, and the OIG's independent review of information about those efforts. The Unimplemented Recommendations listing is updated monthly.

²¹ *Financial Stability Implications from FinTech, Supervisory and Regulatory Issues That Merit Authorities' Attention*, (June 27, 2017), 7. The FSB was chartered by the Group of Twenty (G20) on September 25, 2009. The G20 Members include Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Republic of Korea, Mexico, Russia, Saudi Arabia, South Africa, Turkey, the United Kingdom, the United States, and the European Union (plus Hong Kong, Singapore, Spain and Switzerland). The FSB charter aims to promote global financial stability by coordinating the development of regulatory, supervisory, and other financial sector policies and conducts outreach to non-member countries. The G20 members represent about two-thirds of the world's population, 85 percent of global gross domestic product, and over 75 percent of global trade.

²² Basel Committee on Banking, *Sound Practices – Implications of Fintech Developments for Banks and Bank Supervisors* (February 2018).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

by capital investment, demand for speed and convenience, and digitization.²³ According to the Department of the Treasury (Treasury Department), from 2010 to 2017, more than 3,330 new technology companies were formed to serve the financial industry.²⁴ The Treasury Department also estimated that one-third of online U.S. consumers use at least two financial technology services—including financial planning, savings and investment, online borrowing, or some form of money transfer and payment.²⁵ Further, KPMG estimated that global investment in financial technology was \$57.9 billion in just the first 6 months of 2018.²⁶

Regulators Need Nimble Approach to Financial Innovation

The Treasury Department encouraged “an agile approach to regulation that can evolve with innovation” and stated that regulators, including the FDIC, must be nimble to adapt regulatory approaches to banks’ adoption and use of emerging technology, without creating barriers to innovation.²⁷ According to the Basel Committee on Banking Supervision, financial technology innovation poses three main risks to the banking sector and consumers.²⁸

Cybersecurity Risk – Financial technology companies are interconnected with IT systems at banks, yet these technology companies may not be subjected to regulatory requirements for safety and soundness and may not be examined by financial regulators. Certain banks reported that between 20 and 40 percent of online banking logins are attributable to financial technology companies, and many banks represented that they cannot distinguish among computer logins, as to whether they originate from consumers, data aggregators, or even malicious actors.²⁹ IT system interconnections may provide a pathway for a cybersecurity incident at a financial technology company to infect the banking system.

Operational Risk – When institutions have multiple technology services and relationships, they face ambiguity and uncertainty as to the applicability of certain privacy rules, the Bank Secrecy Act (BSA) provisions and regulations, and Anti-Money Laundering (AML) standards. Banks may be unsure as to whether they or the service provider implement rules, regulations, and requirements. Moreover, financial institutions face challenges to have sufficient skilled staff and capabilities to monitor these risks and

²³ Department of the Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (July 2018); Basel Committee on Banking, *Sound Practices – Implications of Fintech Developments for Bank and Bank Supervisors* (February 2018).

²⁴ *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (July 2018).

²⁵ *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (July 2018).

²⁶ KPMG, *The Pulse of Fintech 2018: Biannual Global Analysis of Investment in Fintech* (July 2018). KPMG is a professional services company.

²⁷ *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*, 9 and 13; and *Sound Practices – Implications of Fintech Developments for Banks and Bank Supervisors* (February 2018), 24.

²⁸ Basel Committee on Banking, *Sound Practices – Implications of Fintech Developments for Banks and Bank Supervisors* (February 2018).

²⁹ Lael Brainard, Member, Board of Governors of the Federal Reserve System, *Where Do Banks Fit in the Fintech Stack?* Remarks delivered at the Northwestern Kellogg Public-Private Interface Conference on “New Developments in Consumer Finance: Research & Practice” (April 29, 2017).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

operations of financial technology companies. In addition, banks may find it difficult to authenticate customers under the BSA/AML requirements (“know your customer”), due to increased automation and distribution of services and products. Such opacity may lead to inadequate and deficient compliance with legal standards and requirements.

Strategic Risk – Traditional banks risk losing substantial market share and profits due to financial innovation. For example, large-scale use of distributed ledger technology³⁰ to process payments, such as the use of blockchain and Bitcoin, has the potential to disrupt the banking sector’s payment system.

The FDIC should ensure that banks have proper governance and risk management practices around these technologies. The FDIC may need to increase training and adjust staffing to ensure examiners have the skills to effectively supervise the risks involved with new technology. Further, the FDIC may need to modify examination policies and procedures that pre-date financial innovation to improve supervision of financial innovation risk. The FDIC also must monitor for potential disruption to the banking sector from technological change and anticipate losses to the Deposit Insurance Fund.

The FDIC Chairman noted in October 2018 that “[w]hat is different today is the speed and tremendous impact of technological innovation *in* and *on* banking, and the potential for technology to disrupt not just an institution or two, but banking as we know it.” As such, the FDIC Chairman announced that the agency was planning to set up an Office of Innovation, which would review how the FDIC can promote technological development at community banks, while still providing a safe regulatory environment.³¹ We will continue to monitor the developments and activities of this new Office at the FDIC.

Financial technology innovation continues to grow and impact the banking system. Institutions must have robust and effective governance and management practices to mitigate risks associated with adoption of financial technology. The FDIC should evaluate the impact of these innovations on banks, assess emerging risks, and expeditiously adjust its processes and supervisory strategies.

³⁰ According to the National Institute of Standards and Technology (NIST), distributed ledgers, such as blockchains, are tamper-resistant digital records of transactions that once established cannot be changed. Blockchain Technology Overview, NIST Internal Report 8202.

³¹ FDIC Chairman McWilliams noted her plans for an Office of Innovation in remarks at the Federal Reserve Bank of Philadelphia, “Fintech and the New Financial Landscape” (November 13, 2018).

**OFFICE OF INSPECTOR GENERAL'S
ASSESSMENT (continued)****3 | STRENGTHENING FDIC INFORMATION SECURITY MANAGEMENT**

The FDIC maintains thousands of terabytes of sensitive data within its IT systems and has more than 180 IT systems that collect, store, or process Personally Identifiable Information (PII) of FDIC employees; bank officials at FDIC-supervised institutions; and bank customers, depositors, and bank officials associated with failed banks. FDIC systems also hold sensitive supervisory data about the financial health of banks, bank resolution strategies, and resolution activities. The FDIC must continue to strengthen its implementation of governance and security controls around its IT systems to ensure that information is safeguarded properly.

The U.S. Computer Emergency Readiness Team (US-CERT) reported 35,277 information security incidents for Federal Executive Branch civilian agencies in 2017. In May 2018, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) conducted a review of Federal cybersecurity capabilities at 96 civilian agencies across 76 metrics to determine each agency's ability to identify, detect, respond, and recover from cyber incidents. The review found that 74 percent (71 agencies) had cybersecurity programs that were either "At Risk" or "High Risk."³²

As a bank regulator, the FDIC collects and maintains a significant volume of sensitive PII, such as names, home addresses, Social Security Numbers, dates and places of birth, bank account numbers, and credit card information.³³ The FDIC also maintains business proprietary information that is sensitive, including banks' internal operations regarding counterparties, vendors, suppliers, and contractors.

The FDIC has encountered a number of information security incidents over the last several years. In August 2011, the FDIC began to experience a sophisticated, targeted attack on its own network whereby an entity gained unauthorized access to the network, escalated its privileges, and maintained an ongoing presence in the network. The attacker penetrated more than 90 workstations or servers within the FDIC's network over a significant period of time, including computers used by a former Chairman and other senior FDIC officials, and gained unauthorized access to a significant quantity of sensitive data.

During late 2015 and early 2016, the FDIC experienced eight additional incidents as departing employees improperly took sensitive information shortly before leaving the FDIC. Seven incidents involved PII, including Social Security Numbers, and thus constituted data breaches. In the eighth incident, the departing employee took highly sensitive components of resolution

³² *Federal Cybersecurity Risk Determination Report and Action Plan* (May 2018). "At Risk" meant that some essential policies, processes, and tools were in place to mitigate overall cybersecurity risk, but significant gaps remained; and "High Risk" meant that fundamental cybersecurity policies, processes, and tools were either not in place or not deployed sufficiently.

³³ PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

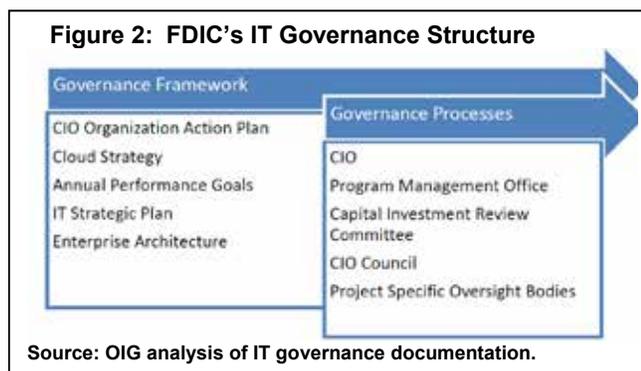
OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

plans submitted by certain large systemically important financial institutions without authorization; this former FDIC employee was recently convicted for theft of government property.³⁴ Our [OIG Special Inquiry](#)³⁵ regarding these breaches revealed systemic weaknesses that hindered the FDIC's ability to respond to multiple information security incidents and breaches efficiently and effectively. We made 13 recommendations in our [OIG Special Inquiry report](#); of these recommendations, 5 remained unimplemented at the time of completion of this Top Challenges report.

IT Governance

The FDIC relies extensively on IT to accomplish its mission and must subject its IT initiatives to appropriate governance and oversight. IT governance provides organizations with a structured process to support IT investment decisions while promoting accountability, due diligence, and the efficient and economic delivery of IT services.³⁶ As illustrated in Figure 2, the FDIC's IT governance structure consists of two principal elements:

- **The Governance Framework.** Reflects the goals and priorities of the FDIC through multiple components, including the IT Strategic Plan and Enterprise Architecture.
- **The Governance Processes.** Consist of controls and procedures to make IT capital investments and oversee individual projects.



In our OIG report entitled [The FDIC's Governance of Information Technology Initiatives](#) (July 2018), we found that the FDIC faced a number of challenges and risks related to the governance of its IT initiatives. For example, the FDIC did not fully develop a strategy to move IT services and applications to the cloud or obtain the acceptance of key FDIC stakeholders before taking steps to initiate cloud migration projects. The FDIC also had not implemented an effective Enterprise Architecture to guide the three IT initiatives we reviewed or the FDIC's broader transition of IT services to the cloud. An ineffective Enterprise Architecture limited the FDIC's ability to communicate to business stakeholders how it intended to implement its new IT strategies. In turn, this caused stakeholders to question the decision to adopt new cloud technologies and the impact on business processes. We made eight recommendations to

³⁴ United States Attorney's Office, Eastern District of New York, Department of Justice Press Release, [Former Senior Employee at FDIC Convicted of Embezzling Confidential Documents](#) (December 11, 2018).

³⁵ OIG Special Inquiry Report, [The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches](#) (April 2018).

³⁶ OIG Report, [The FDIC's Governance of Information Technology Initiatives](#) (July 2018).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

improve the FDIC's governance processes, two of which remained unimplemented at the time of completion of this Top Challenges report.

Information Security Controls

In our annual Federal Information Security Modernization Act (FISMA) audit report, [The FDIC's Information Security Program – 2018](#) (October 2018), we identified security control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. Although the FDIC was working to address previously identified control weaknesses, the FDIC had not yet completed corrective actions for eight prior recommendations (as of December 2018). We made four additional recommendations in this report. The following briefly describes the highest risk areas and weaknesses that can be described in a public report:

- **Information Security Risk Management.** The FDIC had not fully defined or implemented an enterprise-wide and integrated approach to identifying, assessing, and addressing the full spectrum of internal and external risks, including those related to cybersecurity and the operation of information systems. Notably, the FDIC had not finalized a Risk Appetite, Risk Tolerance Level, and Risk Profile. Without these fundamental elements, the FDIC faced difficulties integrating risk into its budget, strategic planning, performance reporting, and internal controls.
- **Enterprise Security Architecture.** The FISMA audit report issued in 2017 recommended that the FDIC develop an enterprise security architecture and integrate it into an enterprise architecture consistent with the Federal Government's enterprise architecture requirements and the FDIC's business and mission requirements. According to NIST, an enterprise security architecture describes the structure and processes of an organization's security processes, information security systems, and responsibilities of personnel and units, and shows their alignment with the organization's mission and strategic plans. The lack of an effective enterprise security architecture increases the risk that the FDIC's information systems could be developed with inconsistent security controls that are costly to maintain. In July 2018, the FDIC provided the OIG with documentation describing its enterprise security architecture. The OIG is reviewing the corrective actions undertaken by the FDIC at the time of this Top Challenges report.
- **Security Control Assessments.** FISMA requires agencies to test and evaluate their information security controls periodically to ensure they are effectively implemented. We identified instances in which security control assessments performed by contractors did not include testing of security control implementation. Instead, assessors relied on narrative descriptions of the controls in FDIC policies, procedures, and system security plans and/or interviews of FDIC or contractor personnel. Without actual testing, assessors did not have a basis for concluding on the effectiveness of security controls. Moreover, we found that the FDIC did not

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

have adequate oversight of security control assessments performed by contractor personnel.

- **Patch Management.** Software vendors release patches as needed or on a periodic basis to address faults in operating systems or applications. Vendors may also issue patches to alter functionality, address new security threats, or modify software configurations to improve security. Effective patch management is, therefore, critical to maintaining the integrity, availability, and security of the FDIC's IT infrastructure and the data that resides within it. We found that the FDIC's patch management processes were not always effective in ensuring that the FDIC implemented patches within defined timeframes. Unpatched systems increase the risk of exposing the FDIC's network to a security incident.
- **Backup and Recovery.** Our FISMA audit report issued in 2017 noted that the FDIC's IT restoration capabilities were limited, and that the FDIC had not taken timely action to address limitations in its ability to maintain or restore critical IT systems and applications during a disaster. The FDIC will continue to have limited assurance that it can maintain and restore mission-essential functions within applicable timeframes during an emergency, until the completion of the Backup Data Center Migration Project in 2019.

The FDIC has increased the 2019 Operating Budget for the Office of the Chief Information Security Officer by approximately \$650,000 (1.3 percent), up to a total of \$51 million. The increased funding is intended to enhance the protection of the FDIC's applications systems and databases from breaches and intrusions, and improve the FDIC's responsiveness and resilience.

In another OIG report entitled [Controls over System Interconnections with Outside Organizations](#), (December 2018), we reviewed the FDIC's controls for managing system interconnections³⁷ with Federal agencies and non-governmental entities. We found that the FDIC's policies and procedures did not define the types of technologies and configurations that constituted a system interconnection and, therefore, required a written agreement. In addition, the FDIC's policies and procedures did not articulate the roles and responsibilities for all stakeholders involved in managing system interconnections. Also, the FDIC did not establish documentation requirements for key activities, and it did not create written agreements to govern several of its system interconnections. Further, we identified instances in which written agreements governing system interconnections had expired, even though the underlying connections remained enabled. We made seven recommendations to improve the FDIC's policies, procedures, and contracts governing system interconnections.

³⁷ NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, defines a "system interconnection" as a direct connection of two or more information technology systems for the purpose of sharing data and other information resources.

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

We have a number of planned and ongoing audits of the FDIC's internal IT operations, including the FDIC's privacy program and practices; security of a system that supports the FDIC's bank supervision and consumer compliance; and security of mobile devices.

The FDIC must safeguard information held within its IT systems, much of which contains sensitive information about banks, depositors, and FDIC employees. Unauthorized access and disclosure of this information could cause significant harm to individuals, banks, and the FDIC. The FDIC must remain vigilant in its efforts to institute necessary controls and properly protect the information entrusted to it.

4 | PREPARING FOR CRISES

Central to the FDIC's mission is readiness to address crises in the banking system. The FDIC must be prepared for a broad range of crises that could impact the banking sector. These readiness activities should help to ensure the safety and soundness of institutions, as well as the stability and integrity of our nation's banking system.

Crisis readiness requires advanced preparation, regardless of whether the crisis results from financial disruption in the markets, economic turmoil, a cyber attack, natural disaster, or other event. "When the unexpected, enterprise-threatening crisis strikes, it is too late to begin the planning process. Events will quickly spin out of control, further adding to the loss of reputation and avoidable costs necessary to survive and recover with minimal damage."³⁸

Although crises may be different in their cause or complexity, implementation of fundamental principles allows agencies, such as the FDIC, to plan and prepare for such events. Figure 3 illustrates the Crisis Management Preparedness Cycle, which includes the following five components:³⁹

Figure 3: Crisis Management Preparedness Continuous Cycle



Source: Federal Emergency Management Agency.

³⁸ Hastings Business Law Journal, *The Board's Responsibility for Crisis Governance* (Spring 2017), 290.

³⁹ Federal Emergency Management Agency National Incident Management System.

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

- **Plan** – Supports effective operations by identifying objectives, describing organizational structures, assigning tasks to achieve objectives, identifying responsibilities to accomplish tasks, and contributing to the goals.
- **Organize** – Identifies necessary skillsets and technical capabilities.
- **Train** – Provides personnel with the knowledge, skills, and abilities to respond to a crisis.
- **Exercise** – Identifies strengths and weaknesses through an assessment of gaps and shortfalls with plans, policies, and procedures to respond to a crisis.
- **Evaluate and Improve** – Compiles lessons learned, develops improvement plans, and tracks corrective actions to address gaps and deficiencies identified.

Early Risk Identification and Mitigation

The Financial Crisis Inquiry Commission stated that financial regulators “had ample power in many arenas [to protect the financial system], and they chose not to use it,” thus rejecting the regulators’ claim that they did not have the necessary authorities.⁴⁰ The current FDIC Director (former FDIC Chairman) noted that when banks are profitable, as in 2018, the FDIC and other regulators must maintain supervisory vigilance.⁴¹

In 2011, the FDIC developed a Forward-Looking Supervision initiative as part of the lessons learned from the financial crisis. The goal of the initiative was to “identify and assess the potential impact of an institution’s new and/or growing risks and ensure early mitigation if necessary.”⁴² In our OIG evaluation report, [Forward-Looking Supervision](#) (August 2018), we found that the FDIC did not have a comprehensive policy guidance document on Forward-Looking Supervision and should clarify guidance associated with its purpose, goals, roles, and responsibilities. We also found that examiners identified overall concentration risk management conclusions and concerns in the examination report; however, only 27 percent of reports sampled elevated concerns to the financial institution’s board of directors.

In addition, the FDIC uses other systems and risk-monitoring tools to identify financial institution emerging risks. For example, the Offsite Review Program (ORP) analyzes quarterly financial institution data against benchmark indicators developed by the FDIC. When an institution falls outside these benchmarks, FDIC examiners must review the bank’s information, document the risks, and select an appropriate supervisory strategy to address the risks. We are currently conducting a review to examine the extent to which the ORP identifies supervisory concerns and potential problems, and appropriately adjusts supervisory strategies.

⁴⁰ Financial Crisis Inquiry Commission, *Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States* (January 21, 2011). The Financial Crisis Inquiry Commission was established as part of the Fraud Enforcement and Recovery Act (Public Law 111-21) to examine the causes of the financial crisis.

⁴¹ “Financial Regulation: A Post-Crisis Perspective”, Remarks by Martin J. Gruenberg, then-Chairman of the FDIC, Brookings Institution (November 14, 2017).

⁴² FDIC RMS Perspectives, Vol 1, Issue 2, (Second Quarter 2014).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

Crisis Preparedness and Planning

According to the FDIC's analysis of the 2008-2011 financial crisis, the events unfolded more quickly than the FDIC expected and were more severe than the FDIC's planning efforts anticipated.⁴³ For example, in July 2008, the FDIC resolved IndyMac, the most expensive FDIC failure, estimated to cost about \$12.3 billion, and in September 2008, Washington Mutual, the sixth-largest FDIC-insured institution, also failed. The FDIC had not planned for several large and small banks to fail at the same time, and these failures occurred at a quicker pace than in previous crises.

Consequently, the FDIC needed to hire staff quickly to manage the escalating workload associated with what would ultimately be nearly 500 failed banks. To address its staffing shortfall, the FDIC authorized funding for additional personnel during the crisis but faced challenges expediting the hiring process to on-board needed staff. For example, in September 2008, the Division of Resolutions and Receiverships had an authorized staff of 825, but only 259 staff was on board.⁴⁴

The FDIC also faced challenges dealing with the increased volume of contracts needed. During the financial crisis, the FDIC awarded over 6,000 contracts totaling more than \$8 billion. The size of its acquisition staff was initially insufficient, which resulted in delays to modify existing contracts and issue new contracts. The FDIC needed to rapidly hire and train personnel to oversee the contracts.

Over the past several years, the FDIC developed goals and objectives to prioritize certain crisis readiness planning activities. According to the FDIC 2018-2022 Strategic Plan, the agency aims to "develop, test, and maintain contingency plans to ensure it is prepared to handle a wide range of potential failure scenarios, including the failure of a large financial institution; simultaneous, multiple failures; the failure of an institution with large international holdings; and the failure of an insured institution that operates primarily through the internet." The FDIC is developed a draft "surge staffing" plan that addresses resources needs for concurrent community bank failures in conjunction with the failure of a moderately large (\$25 to \$50 billion) bank.

We are conducting an evaluation to assess the FDIC's preparedness efforts to address future crises. The scope of our evaluation includes examining the FDIC's crisis readiness plans, its tools and mechanisms to implement the plans, roles and responsibilities, training on crisis response, and actions to evaluate and improve readiness.

The FDIC's ability to mitigate risk and resolve failed banks affects the safety and soundness of institutions as well as the stability of the banking system. The FDIC should maintain robust processes to plan, prepare, train, exercise, and maintain readiness for scenarios that could lead to crises.

⁴³ FDIC, *Crisis and Response, An FDIC History, 2008-2013* (November 30, 2017).

⁴⁴ *Crisis and Response, An FDIC History, 2008-2013*.

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

5 | MATURING ENTERPRISE RISK MANAGEMENT

Enterprise Risk Management (ERM) is a critical part of an agency's governance, as it can inform prudent decision-making at an agency, including strategic planning, budget formulation, and capital investment. ERM program requirements include identifying risks that could affect the organization (Risk Profile and Inventory), establishing the amount of risk an organization is willing to accept (Risk Appetite), prioritizing strategies to address risks in the proper sequence, and responding to and mitigating the risks. The FDIC established an ERM program office in 2011, but has neither developed the underlying ERM program requirements nor realized the benefits of a mature ERM program.

According to FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program*, "Congress, the Office of Management and Budget (OMB), and the Government Accountability Office (GAO) have directed attention to the need for federal agencies to adopt [Enterprise Risk Management (ERM)]." OMB introduced ERM through revised government-wide circulars, including OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. The FDIC Directive states that while not legally obligated to follow executive directives, the FDIC "embrace[s] the spirit of ERM as outlined in OMB Circular No. A-123."⁴⁵

According to OMB Circular No. A-123, Federal agencies face internal and external risks to achieving their missions, including "economic, operational, and organizational change factors, all of which would negatively impact an Agency's ability to meet goals and objectives if not resolved."⁴⁶ OMB Circular No. A-123 further requires that agencies take risk into account when designing internal controls. ERM should be an element of the agency's overall governance process that focuses specifically on the identification, assessment, and management of risk, and it should include these elements:

- A risk management governance structure;
- A methodology for developing a risk profile; and
- A process, guided by an organization's senior leadership, to consider risk appetite and risk tolerance levels that serves as a guide to establish strategy and select objectives.

OMB urges agencies to adopt an enterprise-wide view of ERM—a "big picture" perspective—thus synthesizing the management of risks into the very fabric of the organization; it should not be viewed in "silos" among different divisions or offices. ERM should integrate risk management into the agency's processes for budgeting, including strategic planning, performance planning, and performance reporting practices.

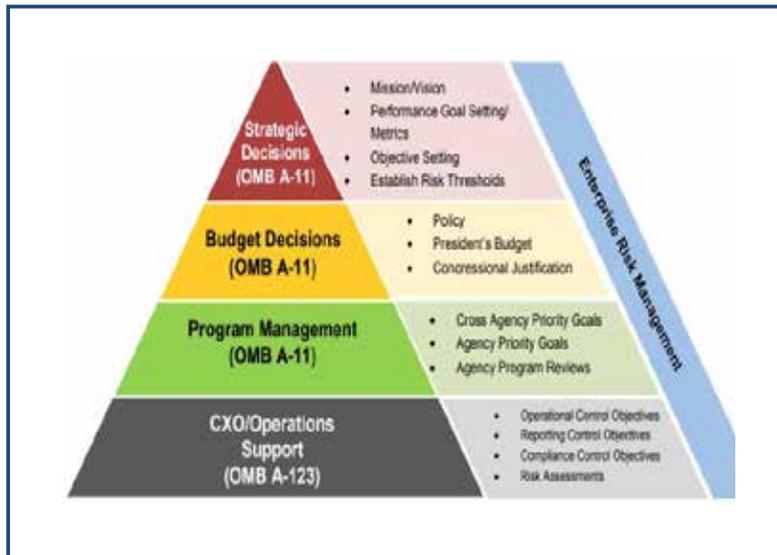
⁴⁵ OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, (July 15, 2016).

⁴⁶ OMB Circular No. A-123 (July 5, 2016), 7.

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

Figure 4 illustrates the manner in which ERM should be implemented in an organization, and the junctures at which it should be considered when making decisions concerning the agency's strategy, budget, program management, and operations. Effective ERM implementation starts with an agency establishing a customized ERM program that fits its organizational mission, culture, operating environment, and business processes.

Figure 4: Enterprise Risk Management Program



Source: Playbook: Enterprise Risk Management for the U.S. Federal Government.

GAO identified six essential elements to assist Federal agencies' implementation of ERM, including:⁴⁷

1. **Align the ERM process to agency goals and objectives** – Ensuring that ERM contributes to achieving mission and results.
2. **Identify Risks** – Assembling a list of risks and opportunities that could affect the agency from achieving its goals and objectives.
3. **Assess Risks** – Prioritizing risk responses based on an assessment of the likelihood and impact of a risk on the agency's mission.
4. **Select Risk Response** – Selecting a strategy to respond to or mitigate risk based on management's risk appetite, such as acceptance, avoidance, reduction sharing, or transfer of risk.
5. **Monitor Risks** – Determining whether risks are changing and if responses are successful.
6. **Report on Risks** – Communicating with management and other stakeholders on the status of addressing risks.

The FDIC's Enterprise Risk Management Program

In June 2010, the FDIC hired a consulting firm to address five key issues regarding its ERM program: Identification and management of risks; Organizational structure; Risk management activities and processes; Capabilities and infrastructure for risk management; and Actionable transparency. The consulting report identified gaps in all five areas, recommended that the FDIC establish a Chief Risk Officer (CRO), and submitted several organizational options to be evaluated by the FDIC. In response to the firm's recommendations, the then-FDIC Chairman

⁴⁷ GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, GAO-17-63 (December 1, 2016).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

appointed a Risk Steering Committee to evaluate alternatives and recommend an organizational structure for risk management.

The Risk Steering Committee recommended to the FDIC Board the establishment of an Office of Corporate Risk Management (OCRM), headed by a CRO, with total staffing of 16. The Board approved changes recommended by the Risk Steering Committee in January 2011. The changes were intended to provide an office within the FDIC that was assigned to review internal risks with a system-wide perspective; facilitate sharing of information regarding existing, emerging, and potential risks; and instill risk governance as part of the FDIC's culture.

By May 2016, the CRO had retired and only five staff remained in OCRM by 2017. Consequently, in 2017, the FDIC initiated an organizational review of its existing ERM program to assess whether changes to the program should be made based on its experience-to-date with its ERM framework. In June 2017, the FDIC placed the CRO under the Division of Finance (DOF) as a Deputy Director, and combined OCRM with the Corporate Management Control Branch, to form a newly constituted Risk Management and Internal Controls Branch (RMIC) within DOF. RMIC responsibilities included not only ERM, but also internal control as well as management of risks in individual programs and projects.

The FDIC, in its 2018 Performance Goals, identified enterprise risk as a priority initiative.⁴⁸ However, as noted above, we reported in our recent FISMA audit, [The FDIC's Information Security Program – 2018](#) (October 2018) that the FDIC had not fully defined or implemented an enterprise-wide and integrated approach to identifying, assessing, and addressing the full spectrum of internal and external risks. The FDIC had not finalized its Risk Appetite, Risk Tolerance Level, and Risk Profile. Without these key fundamental elements, the FDIC faced difficulties integrating risk into its budget, strategic planning, performance reporting, and internal controls. In addition, FDIC Divisions and Offices were not able to evaluate risk determinations in the context of the agency's overall risk levels, tolerance, and profile. As a result, the FDIC could not be sure that its resources were being allocated toward addressing the most significant risks in achieving strategic objectives.

The FDIC issued its revised *Enterprise Risk Management and Internal Control Program Policy* (ERM Policy) in October 2018.⁴⁹ This ERM Policy aims to “identify, assess, and address major risks (including emerging risks) that have a potential broad impact to the FDIC's ability to achieve its goals, objectives, and mission.” The ERM Policy indicates that the agency's ERM would be implemented through the FDIC's existing structure, and that FDIC Divisions and Offices would identify key activities and risks, and take actions to address these risks.

The FDIC's ERM Policy identified key requirements for the program, including establishing a Risk Appetite and Risk Profile. The ERM Policy also requires that the FDIC establish a Risk Inventory which is a “comprehensive, detailed list of risks that could affect the FDIC's ability to

⁴⁸ 2018 FDIC Performance Goals, Priority 2018 Initiatives, Goal 6: Identify and address enterprise risk.

⁴⁹ FDIC, *Enterprise Risk Management and Internal Control Program*, Directive 4010.3 (October 25, 2018).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

meet its strategic objectives,” and that the ERM program includes the following essential elements:

- Process Alignment to Goals and Objectives;
- Risk Identification;
- Risk Assessment;
- Risk Response Selection;
- Risk Monitoring; and
- Communication and Reporting.

We are initiating an evaluation of the FDIC’s ERM program to assess the extent to which the FDIC has implemented an effective ERM program consistent with guidance and best practices.

The FDIC should develop an integrated approach to ERM. This ERM program should synthesize the management of risks into the FDIC’s organizational culture, so that these risks may be considered and incorporated into the FDIC’s budget, strategic planning, performance reporting, and internal controls for the agency as a whole.

6 | SHARING THREAT INFORMATION WITH BANKS AND EXAMINERS

Federal Government agencies and private-sector entities share information about threats to U.S. critical infrastructure sectors, including the financial sector. Sharing actionable and relevant threat information among Federal and private-sector participants protects the financial system by building threat awareness and allowing for informed decision-making. The FDIC must ensure that relevant threat information is shared with its supervised institutions and examiners as needed, in a timely manner, so that actions can be taken to address the threats. Threat information also provides FDIC examiners with context to evaluate banks’ processes for risk identification and mitigation strategies.

Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, identified the financial services sector as one of 16 critical infrastructure sectors vital to public confidence and the nation’s safety, prosperity, and well-being. The FFIEC recognized that financial institutions should be prepared to address a variety of threats, including terrorists attacks, pandemics, and cybersecurity.⁵⁰ For example, cyberattacks at financial institutions prevented public access to websites, compromised personal information of tens of millions of customers, and millions of dollars were lost due to systems breaches where criminals transferred funds from customer accounts and from automated teller machines.⁵¹ Further, information such as that provided by the Centers for Disease Control and Prevention allows financial institutions to monitor potential

⁵⁰ FFIEC, *Business Continuity Planning* (February 2015).

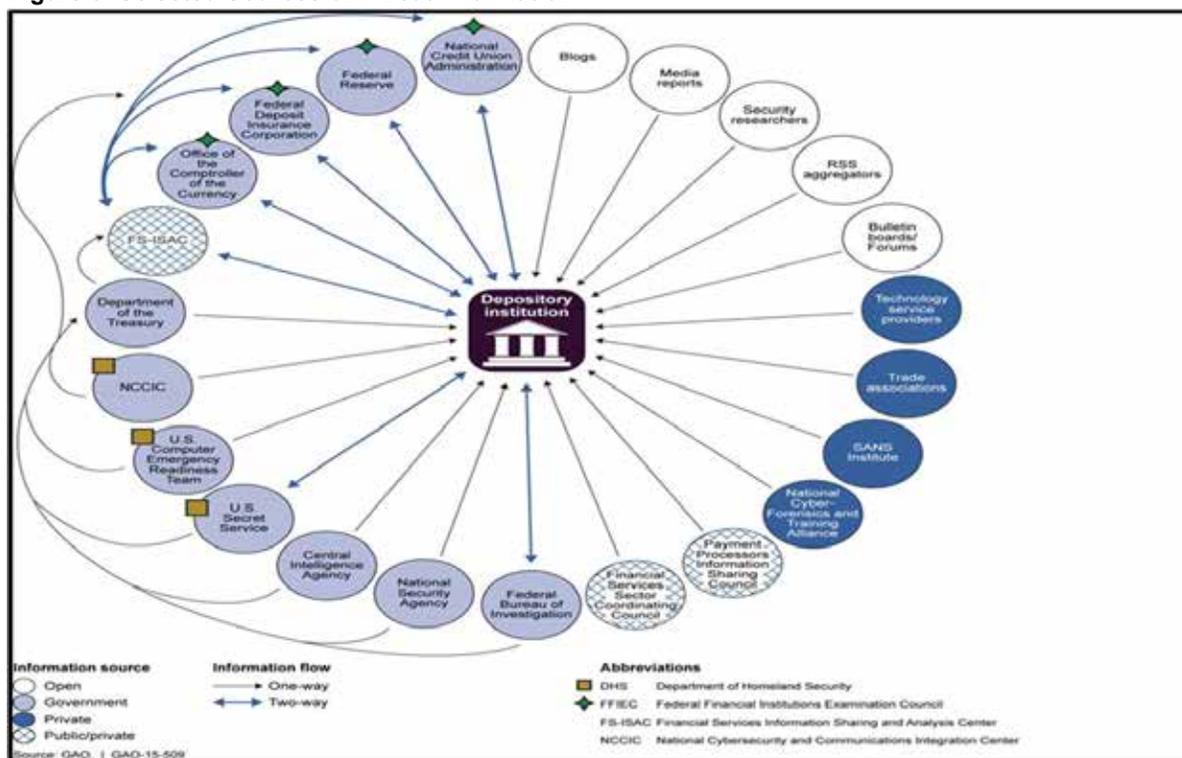
⁵¹ GAO, *Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information*, GAO-15-509 (July 2015).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

pandemic health outbreaks to ensure institutions have the capability to continue critical operations when large numbers of staff are unavailable for prolonged periods of time.⁵²

FSOC noted, in its 2018 Annual Report, the critical importance of sharing timely and actionable threat information among the Federal Government and the private sector. FSOC stated that Federal agencies should consider how to share information and when possible “declassify (or downgrade classification) of information to the extent practicable, consistent with national security needs.”⁵³ GAO also identified various sources of threat information that could be shared with financial institutions. Figure 5 illustrates how GAO captured threat information flows from multiple sources.

Figure 5: Selected Sources of Threat Information



In July 2018, DHS launched a new initiative called the National Risk Management Center (NRMC). According to DHS, the NRMC was established in response to “the increasingly complex threat environment and corresponding demand from industry for greater integrated support from the U.S. federal government.”⁵⁴ The NRMC will work across industry sectors and Federal agencies, including the banking sector, so that participants can have a more comprehensive perspective on systemic risk; the goal is to promote collaborative risk strategies.

⁵² Centers for Disease Control and Prevention *Pandemic Intervals Framework*, (September 26, 2014); and FFIEC, *Business Continuity Planning*, Appendix D: Pandemic Planning.

⁵³ FSOC 2018 Annual Report, 7.

⁵⁴ DHS, National Risk Management Center [Fact Sheet](#) (July 2018).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

According to the FDIC's 2017 Annual Report, the FDIC continues to engage with the Financial and Banking Information Infrastructure Committee, Financial Services Sector Coordinating Council for Critical Infrastructure Protection, DHS, and other regulatory agencies and law enforcement to share information and coordinate responses.

Banks' Access to and Use of Threat Information

In November 2014, the FDIC and other FFIEC members encouraged financial institutions to join the Financial Services Information Sharing and Analysis Center (FS-ISAC), through its *Statement on Cybersecurity Threat and Vulnerability Monitoring and Sharing (Cybersecurity Sharing Statement)*.⁵⁵ FS-ISAC is a group of 7,000 member organizations, and its purpose is to share timely, relevant, and actionable security threat information. The *Cybersecurity Sharing Statement* also suggested using other resources such as the Federal Bureau of Investigation's (FBI) InfraGard,⁵⁶ U.S. Computer Emergency Readiness Team,⁵⁷ and Secret Service Electronic Crimes Task Force.⁵⁸

According to the FFIEC, financial institutions should have business continuity plans that "[a]nalyze threats based upon the impact to the institution, its customers, and the financial market it serves."⁵⁹ Further, the FFIEC notes that financial institutions should have "a means to collect data on potential threats that can assist management in its identification of information security risks."⁶⁰ FDIC-supervised institutions are links of the chain in the financial services system interconnections; an incident involving one community bank has the potential to affect the broader financial sector.⁶¹ Therefore, as part of its examination process, the FDIC must ensure that supervised institutions can receive and access threat information, and that they have business continuity plans to address such threats.

FDIC and Examiners' Access to and Use of Threat Information

FDIC Headquarters staff has access to significant amounts of threat information held by the U.S. Government, and much of the information is confidential and highly sensitive. The FDIC should develop sound practices to review threat information and take necessary actions based upon such information. In doing so, the agency should ensure that it develops and maintains processes to assess the sensitivity and classification of this information.

⁵⁵ FFIEC, *Statement on Cybersecurity Threat and Vulnerability Monitoring and Sharing*.

⁵⁶ InfraGard is a web-based portal that provides collaboration between the FBI and the private sector to exchange information about critical infrastructure.

⁵⁷ US-CERT is a component of the Department of Homeland Security; its mission is to reduce the nation's risk of systemic cybersecurity and communications challenges.

⁵⁸ The Electronic Crimes Task Force is a nationwide network designed to support and assist state, local, and Federal law enforcement agencies in order to combat criminal activity involving the use of new technology.

⁵⁹ FFIEC, Business Continuity Planning Booklet, *Risk Assessment*, (Available on the FFIEC website).

⁶⁰ FFIEC IT Examination Handbook Infobase, Information Security Booklet, II, *Information Security Program Management* (Available on the FFIEC website).

⁶¹ Departments of the Treasury and of Homeland Security, *Financial Services Sector-Specific Plan* (2015), 9.

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

In addition, the FDIC should ensure that the threat information can be disseminated to specific examiners as needed, and that such examiners are authorized to receive access to sensitive threat information. For example, if the FDIC has access to threat information about a particular FDIC-supervised bank, the examiners overseeing this institution should have access to such threat information. Given the volume of information, the FDIC faces challenges to analyze, distill, and convey relevant and actionable threat information from FDIC Headquarters to examiners in the FDIC's Regional and Field Offices.

Threat information can assist FDIC examiners in prioritizing and focusing their work on emerging issues, and modifying the depth or scope of an examination. Understanding the nature of threats provides context for examiners when evaluating financial institutions' processes for identifying and considering relevant risks and implementing risk mitigation strategies. Further, threat information may result in changes to examination policy or procedures to address emerging issues.

RMS instituted *Regional Cyber Incident Reporting and Response Guides* (Reporting and Response Guides) to outline the steps to be taken by Regional and Field Offices when banks report threats and incidents. These steps include gathering information about an incident; providing advice to the affected entity; determining whether the incident warrants escalation to FDIC Headquarters; and conducting ongoing monitoring and communications. RMS also has a *Cyber Incident Response Plan* for use by FDIC Headquarters staff to evaluate threats and incidents reported by banks through the Field and Regional Offices. The Plan uses predetermined criteria and thresholds to determine when threat and incident information should be escalated to FDIC senior management.

Neither the RMS *Cyber Incident Response Plan* nor the Reporting and Response Guides provide procedures for the FDIC to disseminate information to its Regional and Field Offices and examiners. RMS officials stated that they review threat information from multiple sources and regularly convey relevant information to Regional and Field Office examiners, depending upon the criticality and sensitivity of the information.

Based on our research, as of the end of 2018, the FDIC did not have a policy that (i) defined criteria for selecting relevant, actionable threat information, or (ii) outlined the process to share such threat information among Headquarters, Regional Offices, and examiner personnel. Without policies to guide those processes, information selection and dissemination is left to the discretion of individuals, which may lead to inconsistencies, uncertainty, and a lack of uniformity in sharing threat information. We have work planned to evaluate the effectiveness of the FDIC's procedures for the collection and dissemination of threat information.

Sharing threat information allows for the consideration of these risks in developing and examining bank mitigation strategies and continuity plans. Absent such threat information, financial institutions and examiners may not have a full understanding of the risks facing the banks, and thus, risk mitigation and supervisory strategies might have gaps which could affect the safety and soundness of institutions.

**OFFICE OF INSPECTOR GENERAL'S
ASSESSMENT (continued)**

7 | MANAGING HUMAN CAPITAL

The FDIC relies on skilled personnel to fulfill its mission, and about 63 percent of the FDIC’s operating budget for 2019 (\$2 billion) was for salaries and associated benefits for employees. Forty-two percent of FDIC employees are eligible to retire within 5 years, which may lead to knowledge and leadership gaps. To ensure mission readiness, the FDIC should find ways to manage this impending shortfall. In addition, the FDIC should seek to hire individuals with advanced technical skills needed for IT examinations and supervision of large and complex banks.

GAO has identified human capital management as a high risk since 2001 and noted that “[m]ission-critical skills gaps within the federal workforce pose a high risk to the nation.”⁶² GAO noted that such gaps, if left unaddressed, can “impede the federal government from cost-effectively serving the public and achieving results.” The percentage of FDIC employees eligible to retire more than doubles (2.3 times) over the next 5 years, increasing from 18 percent in 2018 to 42 percent in 2023, as shown in Figure 6.

Figure 6: FDIC Employees Eligible for Retirement between December 2018 and December 2023



Source: OIG analysis of FDIC employee information as of July 31, 2018.

These figures could lead to a wave of retirements at the FDIC in the near term. As recognized by GAO, retirement waves can result in leadership voids, which could impede the capabilities of any agency to achieve its mission, unnecessarily delay decision-making, and reduce program management and oversight.⁶³ According to GAO, such agencies may face gaps in skillsets, which could result in the agency not being able to complete its mission-critical work in a timely manner. Further, retirements might have financial implications for the FDIC’s budget, since the FDIC would be required to expend lump-sum payments based on accumulated annual leave.⁶⁴ The FDIC should be prepared to address any resultant budget issues and gaps in skillsets and leadership.

In addition, the FDIC faces an even higher rate of potential retirements among seasoned senior and mid-level managers. As of July 31, 2018, approximately two-thirds of the Executive

⁶² GAO, *High-Risk Series: Progress in Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (February 2017), 61.

⁶³ GAO, *High-Risk Series: Progress in Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (February 2017), 61.

⁶⁴ Office of Personnel Management, [Fact Sheet: Lump Sum Payment for Annual Leave](#).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

Management employees (66 percent) were eligible to retire within 5 years, and another 57 percent of FDIC Corporate Managers are eligible in that same timeframe. Without proper succession planning strategies, these retirements can result in further leadership gaps.

Retirement Eligibility – Impact on Divisions (Headquarters and Regions)

Between 34 and 63 percent of employees in the following FDIC driver and primary support Divisions were eligible to retire within 5 years (as of July 31, 2018):

- 63 percent of employees within the Division of Resolutions and Receiverships (243 employees);
- 59 percent of employees within the Legal Division (268 employees);
- 57 percent of employees within the Division of Administration (201 employees);
- 45 percent of employees within the Division of Information Technology (133 employees);
- 38 percent of employees within the Division of Risk Management Supervision (929 employees); and
- 34 percent of employees within the Division of Depositor and Consumer Protection (276 employees).

While employees do not always retire when first eligible,⁶⁵ there is a risk that a wave of retirements could lead to gaps in leadership positions and skillsets at the FDIC. Leadership gaps can result in delayed decision-making, reduced program oversight, and failure to achieve goals and agency missions when positions are unfilled or leaders remain in acting status. Skillset gaps can undermine the ability of the FDIC to achieve its goals and missions.

In addition, in 2017, the Division of Insurance and Research (DIR) experienced higher than normal attrition rates of 13 percent. Over this period of time, 27 individuals (out of 208 in DIR) departed DIR, 74 percent of whom were specialized economists with advanced degrees. These unique skillsets may be more difficult to replace in an expanding economy.

Retirement Eligibility – Impact on Regional Offices

In the six FDIC Regional Offices, more than one-third of employees are eligible to retire within the next 5 years. Those retirements are predominantly for examination staff. Between 34 and 53 percent of employees in the FDIC Regional Offices were eligible to retire within this timeframe (as of July 31, 2018):

- 53 percent of employees within the FDIC Dallas Regional Office (413 employees);
- 38 percent of employees within the FDIC Atlanta Regional Office (176 employees);
- 37 percent of employees within the FDIC San Francisco Regional Office (164 employees);
- 34 percent of employees within the Chicago Regional Office (172 employees);

⁶⁵ Our analysis shows that employees tend to remain with the FDIC for approximately 8 years after their retirement eligibility date.

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

- 34 percent of employees within the Kansas City Regional Office (169 employees); and
- 34 percent of employees within the New York Regional Office (195 employees).

The FDIC is working to hire and train new examiners to address the retirement shortfall, but it takes approximately 4 years from the time an employee is hired until that employee earns an examination commission. Such commissioning requires that employees meet benchmarks, training, and other technical requirements, including passing a Technical Examination.

In its review of the financial crisis of 2008-2011, the FDIC stated that one of its strengths was “a core of seasoned examiners and supervisors.”⁶⁶ These experienced employees were crucial in tailoring “informal and formal enforcement actions that helped make it possible for many banks to return to health.” As noted by the FDIC in its review, the crisis experience highlighted the importance of a steady flow of new examiners who can benefit from the knowledge and experience of seasoned examiners. The FDIC may be challenged to build on innovative strategies used in prior crises for any future banking crisis without these experienced examiners and supervisors or the transfer of their knowledge to newer examiners.

Even with additional hires, Regional Offices may not have sufficient experience among their examiners. As a result, senior examiners may be required to travel more frequently in order to supervise less experienced staff and sign reports of examination (since pre-commissioned examiners cannot sign those reports). In addition, experienced examiners may be required to travel more often, in order to fill staffing needs where there have been significant retirements. This increase in travel requirements could be costly and may affect the morale of examiners, since it has been cited as the top reason for voluntary attrition by examiners.

RMS also identified a need to build out skill sets. In 2012, RMS initiated a multi-year Subject Matter Expert Project to build out workforce capacity and focus on developing advanced skills in the areas of accounting, capital markets, information technology, and anti-money laundering compliance. The FDIC also recently updated employees about a Field Office Modernization initiative, aimed, in part, to maintain a reasonable work/life balance for field examiners.

In 2013, the FDIC established a Workforce Development Initiative (WDI) to address succession planning and other workforce development challenges and opportunities. Five years after its establishment, however, the FDIC noted, in its 2018 Annual Performance Plan, that the WDI is “in the early stages of a multi-year effort to identify future workforce and leadership requirements, assess current workforce capabilities, support employees who aspire to leadership and management roles, and develop and source the talent to meet emerging workforce needs.”

The management of human capital is critical to the FDIC’s achieving its mission. To meet its goals and objectives, the FDIC must continue to focus on managing the life cycle of human

⁶⁶ *Crisis and Response, An FDIC History, 2008-2013* (November 30, 2017), 143-144.

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

capital activities – planning, recruitment, on-boarding, compensation, engagement, succession planning, and retirement programs.

8 | ADMINISTERING THE ACQUISITIONS PROCESS

The FDIC relies heavily on contractors for support of its mission, especially for IT and administrative support services. The average annual expenditure by the FDIC for contractor services over the past 5 years has been approximately \$587 million. The FDIC should maintain effective controls to ensure proper oversight and management of such contracts and should conduct regular reviews of contractors. In addition, the FDIC should also perform due diligence to mitigate security risks associated with supply chains for goods and services.

According to GAO's *Framework for Assessing the Acquisition Function at Federal Agencies*, agencies should effectively manage their acquisitions process in order to ensure that contract requirements are defined clearly and all aspects of contracts are fulfilled.⁶⁷ Agencies must properly oversee contractor performance and identify any deficiencies.

In 2018, the Administration recognized the importance of improving Federal Government acquisitions in finding that such acquisitions “often fail to achieve their goals because many Federal managers lack the program management and acquisition skills to successfully manage and integrate large and complex acquisitions into their projects.”⁶⁸ In 2018, GAO reported that agencies continue to award contracts warranting increased management attention.⁶⁹ In addition, GAO found that government contracting officials were carrying heavier workloads, and thus, it was more difficult for these officials to oversee complex contracts and ensure that contractors adhered to contract terms. Further, in the *Framework for Assessing the Acquisition Function at Federal Agencies*, GAO noted the importance of agencies defining their contracting needs and identifying, selecting, and managing providers of goods and services.

Federal Government agencies also should conduct due diligence to recognize potential threats in supply chains for products and services. When an organization hires contractors who, in turn, may sub-contract services to third-parties, the organization is likely to have reduced visibility, understanding, and control of the underlying relationships, as illustrated in Figure 7.

⁶⁷ GAO, *Framework for Assessing the Acquisition Function at Federal Agencies*, GAO-05-218G (September 2005).

⁶⁸ The President's Management Agenda: Modernizing Government for the 21st Century, 12.

⁶⁹ GAO, *Federal Acquisitions: Congress and the Executive Branch have Taken Steps to Address Key Issues, but Challenges Endure*, GAO-18-627 (September 2018).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

If not managed properly, organizations may face supply chain risks, including installation of malicious or counterfeit hardware or software, disruption of critical production, and reliance on nefarious or unqualified service providers.⁷⁰ Government agencies may not discover the consequences of these risks until much later, after the fraud or compromise

Contract Oversight

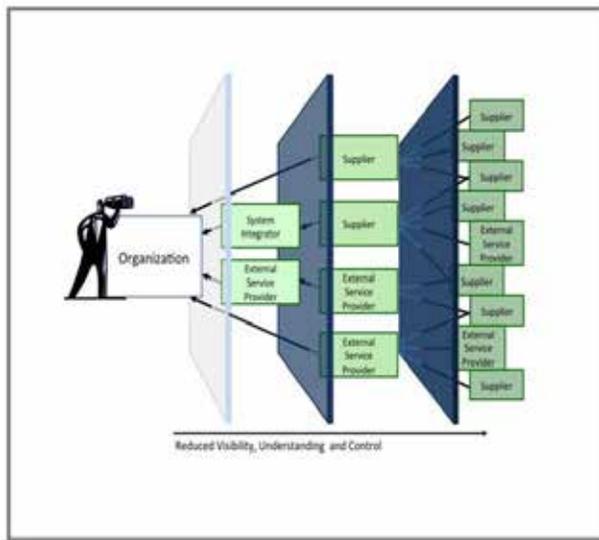
The FDIC awarded \$2.3 billion in contracts from January 2015 through September 2018. For the first 7 months of 2018, the FDIC issued 372 contract awards for a total of \$383 million. In addition, the FDIC budget for 2019 includes more than \$420 million in contracting expenses for outside services.

Between January 2015 and September 2018, the Divisions of Administration (DOA), Information Technology (DIT), and Resolutions and Receiverships (DRR) accounted for 96 percent (\$1.38 billion) of all contract awards through the Acquisition Services Branch. Contracting Officers are responsible for ensuring the performance of all actions necessary for efficient and effective contracting, compliance with contract terms, and protection of the FDIC's interests in all of its contractual relationships. In addition, FDIC program offices develop contract requirements, and Oversight Managers and Technical Monitors oversee the contractor's performance and technical work.

Our OIG analysis indicates that there has been an increase in the average dollar amount per contract awarded by the FDIC from 2016 to 2017. The average contract size has increased 18 percent during this time. Over the past 2 years, DRR and DIT oversaw 127 contracts valued at \$1 million or more each. Many of these contracts are for computer-related and administrative services that range in value from \$1 million to \$98 million. According to GAO, these types of contracts require increased oversight and management attention due to the risk that contractors may perform tasks reserved for the Government.⁷¹

Our work has identified a number of issues related to the FDIC's contract administration. In our OIG report, [The FDIC's Failed Bank Data Services Project](#) (March 2017), we reviewed transition costs (\$24.4 million) of a 10-year project to change information systems on failed financial institutions. We found that the FDIC faced challenges related to defining contract requirements, coordinating contracting and program office personnel, and establishing

Figure 7: Supply Chain Risk View



Source: NIST Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

⁷⁰ GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies*, GAO-18-667T (July 12, 2018), 7-8.

⁷¹ GAO, *Federal Acquisitions: Congress and the Executive Branch have Taken Steps to Address Key Issues, but Challenges Endure*, GAO-18-627 (September 2018).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

implementation milestones. We reported that FDIC personnel did not fully understand the requirements for transitioning failed financial institution data and services to a new contractor, or communicate these requirements to bidders in a comprehensive transition plan as part of the solicitation. Further, the FDIC did not establish clear expectations in the contract documents and did not implement a project management framework and plans.

In addition, our OIG report on the [Follow-on Audit of the FDIC's Identity, Credential, and Access Management Program](#) (June 2017) found that the FDIC did not maintain current, accurate, and complete contractor personnel data needed to manage Personal Identity Verification (PIV) cards, and management had not finalized and approved a plan for retiring the FDIC's legacy PIV card system.

In our OIG Memorandum, [Infrastructure Support Contract 3 \(ISC-3\) with CSRA, Inc.](#) (July 2018), we concluded that based on limited testing, while we did not see instances of inaccurate or unsupported invoices, there was an increased risk that both errors and fraudulent activity would go undetected due to the complexity of CSRA's accounting entries for contractor and subcontractor billing. Of the seven DIT individuals overseeing the contract, two individuals never took the required training on contract oversight, and the training certificates for two other individuals had already expired in 2008.

In addition, in our OIG report, [Payments to Pragmatics, Inc.](#) (December 2018), we determined that about 10 percent (\$47,489) of the labor charges we reviewed were not adequately supported or allowable under the contract and related task orders. The unsupported labor charges were for hours billed by two subcontractor employees who did not access the FDIC's network or facilities on the days they charged the hours. In addition, we identified unallowable labor charges for work performed offsite, away from FDIC facilities.

We currently have an ongoing evaluation to assess the FDIC's contract management oversight process. The evaluation objective includes assessing the monitoring of contracts; capacity of oversight managers to oversee assigned contracts; oversight managers' experience and qualifications; and security risks posed by contractors and their personnel.

Security and Supply Chain Risk

The FDIC also must continue to ensure that its contractors and contracting personnel meet security and suitability standards for employment and access to sensitive information. In addition, contractors must meet criteria for integrity and fitness, including the elimination of conflicts of interest, adherence to ethics obligations, and security of confidential information.⁷²

These protections are important since the contractors often have access to FDIC space and information and use FDIC equipment, including sensitive information related to bank closings, as well as PII for bankers, bank customers, and FDIC employees. The FDIC's DOA (Security

⁷² 12 C.F.R. Part 366.

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

and Emergency Preparedness Section) is responsible for establishing and implementing the security policy for contractor personnel. DOA reviews include background investigations, evaluation of any derogatory information, adjudication, and approvals and clearances.⁷³

In addition, NIST identified the best practices for organizations to manage security risks associated with supply chains of goods and services; these standards require the integration of risk management throughout an organization.⁷⁴ Currently, the FDIC does not have policy guidance with respect to these supply chain risks. In addition, the duty of managing supply chain risk is a collateral responsibility for the FDIC's Insider Threat Program Manager.

The FDIC also faces challenges to mitigate supply chain risk if threats are reported through highly sensitive security information. Currently, DOA acquisition staff does not have authorized access to highly sensitive security information. Therefore, if the FDIC learns of or identifies a threat to its supply chain through the receipt of such information, the FDIC would not have contracting personnel to respond to the threat, as the current staff is not authorized to access the underlying threat information.

The FDIC depends on contracts and contractors for its mission-critical systems and operations, especially in times of crisis. The FDIC should maintain strong contracting oversight and effective controls over its contractors. In addition, the FDIC should protect against supply chain and other risks posed by goods and services procured through third-party contractors and vendors.

9 | IMPROVING MEASUREMENT OF REGULATORY COSTS AND BENEFITS

Before issuing a rule, the FDIC should ensure that the benefits accrued from a regulation justify the costs imposed. The FDIC should establish a sound mechanism to measure both costs and benefits at the time of promulgation, and it should continue to evaluate the costs and benefits of a regulation on a regular basis, even after it has been issued.

In a report issued in February 2018, GAO noted that “representatives of community banks and credit unions expressed concerns about the burden that additional regulations create for them,” such as increasing their overall compliance burden and adversely affecting lending.⁷⁵ In April 2018, the FDIC updated its *Statement of Policy on the Development and Review of Regulations and Policies*, and the revised policy states that once the FDIC has found the need for a regulation, “the FDIC evaluates benefits and costs, based on available information, and

⁷³ FDIC, Circular 1610.2, *Personnel Security Policy and Procedures for FDIC Contractors* (January 2010).

⁷⁴ NIST Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, 7.

⁷⁵ GAO, *Community Banks and Credit Unions: Regulators Could Take Additional Steps to Address Compliance Burdens*, GAO-18-213 (February 2018), 1-2.

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

considers reasonable and possible alternatives.” While some regulations implement a statutory requirement, the FDIC should develop and maintain strong processes to measure both costs and benefits.

Analysis of Costs and Benefits

The difficulties of cost-benefit analysis lie in the uncertainty over how to measure and calculate regulatory costs.⁷⁶ For example, the FDIC experienced challenges in quantifying the costs and benefits of a proposed rule on *Recordkeeping for Timely Deposit Insurance Determination*. The FDIC engaged a contractor that initially estimated the costs of this rule at \$328 million, to be incurred by 36 financial institutions (80 cents per deposit account). However, the FDIC encountered difficulties in determining the benefits of the rule, explaining that “[b]ecause there is no market in which the value of these public benefits can be determined, it is not possible to monetize these benefits.” Based upon the comments received on the proposed rule, the FDIC revised the total cost in the final rule to \$478 million (an increase of \$150 million). The estimated cost would be allocated to covered institutions at \$386 million, while the remaining costs of \$92 million were to be borne by bank customers (depositors) and the FDIC.

In 2018, GAO reviewed regulatory procedures for the financial regulators and found several weaknesses with analyses done by six financial regulators, including the FDIC.⁷⁷ In particular, the regulators did not account for the burden that certain rules would have on small entities. The Regulatory Flexibility Act (RFA) requires that Federal agencies, including the financial regulators, analyze the impact of proposed regulations on small entities and consider alternatives that could lessen the regulatory burden. Alternatively, the head of the agency may certify that the rule would not pose a significant impact on a substantial number of small entities.

The then-FDIC Chairman certified that a rule would not pose a significant impact on a substantial number of small entities for over 75 percent of the rules issued by the FDIC between 2010 and 2016 that were subject to RFA requirements.⁷⁸ GAO concluded that for two of the three rules it sampled, the FDIC did not provide any supporting information for the certifications. For example, GAO found that the FDIC did not include any of the Office of Advocacy’s⁷⁹ suggested components: (i) a description of the number of affected entities; (ii) the size of the economic impacts; or (iii) the justification for the certification.⁸⁰

⁷⁶ Yale Law Journal, *Cost-Benefit and Other Analysis Requirements in the Rulemaking Process*, Congressional Research Service (2014); *Cost-Benefit Analysis of Financial Regulations Case Studies and Implications* (2015).

⁷⁷ GAO, *Financial Services Regulations: Procedures for Reviews under Regulatory Flexibility Act Need to Be Enhanced*, GAO-18-256 (January 2018).

⁷⁸ GAO focused only on the RFA sections and not the other regulatory analysis in the Federal Register notice, despite agencies being allowed by statute to combine analysis to avoid duplication.

⁷⁹ The Office of Advocacy is a component of the Small Business Administration and serves as a watchdog for the RFA.

⁸⁰ GAO, *Financial Services Regulations: Procedures for Reviews under Regulatory Flexibility Act Need to Be Enhanced*, GAO-18-256 (January 2018).

OFFICE OF INSPECTOR GENERAL'S ASSESSMENT (continued)

For the rules for which the FDIC did perform a regulatory flexibility analysis,⁸¹ GAO reported that while the FDIC's analyses described and quantified the rules compliance costs, they did not include descriptions or assessments of regulatory alternatives, issues raised in public comments, or steps to minimize effects on small entities.⁸² GAO recommended that the FDIC adopt policies and procedures to comply with RFA requirements and key aspects of Office of Advocacy and OMB guidance in order to improve consistency. The FDIC adopted additional policies and procedures in 2018; however, the GAO recommendation remains unimplemented.

In a subsequent report issued the following month, GAO found that there were additional inadequacies in the financial regulators' consideration of regulatory burden on small institutions – particularly with respect to the quantification of data and cumulative effects of regulations.⁸³ The Economic Growth and Regulatory Paperwork Reduction Act of 1996 (EGRPRA) requires that at least every 10 years, the FDIC must review its rules and regulations to determine if any are outdated, unnecessary, or unduly burdensome. However, GAO found that the regulators, including the FDIC, did not conduct or report on quantitative analyses as part of their EGRPRA review process. Instead, as GAO noted, “regulators generally only provided their arguments against taking actions and did not cite analysis or data to support their narrative.” GAO further found that “regulators ha[d] not assessed the ways that the cumulative burden of the regulations they administer may have created overlapping or duplicative requirements.” According to GAO, Congress specifically intended for EGRPRA to require regulators to measure the cumulative effect of regulations.

In August 2018, the FDIC Chairman stated that a top priority for the agency was to examine the regulatory burden on small banks. The following month, in September 2018, the FDIC issued a proposal to retire 374 of 664 Financial Institution Letters (FIL) related to risk-management supervision. These FILs contained outdated information or guidance that was available elsewhere from the FDIC. In announcing this proposal, the FDIC committed to a review of the remaining 290 FILs.⁸⁴ We are currently conducting an evaluation to determine the effectiveness of the FDIC's cost-benefit analysis process for ensuring that rules are efficient and appropriately tailored.

Financial regulations significantly affect financial institutions and bank customers, and before imposing costs on such entities, the FDIC should ensure that the benefits of the rule justify the costs associated with its implementation. To do so, the FDIC should obtain concrete, valid, and reliable data, and analyze the information, so that it can accurately measure the costs and benefits of a regulation.

⁸¹ For three of the four regulatory flexibility analyses it performed, the FDIC indicated that the rules were not subject to the requirements of the RFA.

⁸² GAO, *Financial Services Regulations: Procedures for Reviews under Regulatory Flexibility Act Need to Be Enhanced*, GAO-18-256 (January 2018).

⁸³ GAO, *Community Banks and Credit Unions: Regulators Could Take Additional Steps to Address Compliance Burdens*, GAO-18-213 (February 2018).

⁸⁴ Financial Institution Letter 46-2018, *FDIC Seeks Comment on Proposed Retirement of Certain Financial Institution Letters* (September 10, 2018).

D. ACRONYMS AND INITIALISMS

AEI	Alliance for Economic Inclusion	CMG	Crisis Management Group
AFS	Available-For-Sale	CMP	Civil Money Penalty
AIG	American International Group, Inc.	ComE-IN	Advisory Committee on Economic Inclusion
AML	Anti-Money Laundering	CPI-U	Consumer Price Index for All Urban Consumers
AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism	CRA	Community Reinvestment Act
ASBA	Association of Supervisors of Banks of the Americas	CRE	Commercial Real Estate
ASC	Accounting Standards Codification	CSIRT	Computer Security Incident Response Team
ASU	Accounting Standards Update	CSF	Cybersecurity Framework
BCBS	Basel Committee on Banking Supervision	CSBS	Conference of State Bank Supervisors
BDC	Backup data center	CSRS	Civil Service Retirement System
BoA	Bank of America	DCP	Division of Depositor and Consumer Protection
BSA	Bank Secrecy Act	DFA	Dodd-Frank Act
Call Report	Consolidated Reports of Condition and Income	DIF	Deposit Insurance Fund
CAMELS rating scale	Capital adequacy; Asset quality; Management quality; Earnings; Liquidity; Sensitivity to market risks	DIMIA	Depository Institution Management Interlocks Act
CAT	Cybersecurity Assessment Tool	DIR	Division of Insurance and Research
CBAC	Advisory Committee on Community Banking	DIT	Division of Information Technology
CCP	Central Counterparties	DLP	Data Loss Prevention
CDFI	Community Development Financial Institution	DOA	Division of Administration
CECL	Current Expected Credit Losses	DRR	Designated Reserve Ratio
CEO	Chief Executive Officer	DRR (FDIC)	Division of Resolutions and Receiverships
CEP	Corporate Employee Program	EC	European Commission
CFI	Complex Financial Institution	EDIE	Electronic Deposit Insurance Estimator
CFO Act	Chief Financial Officers' Act	EGRPRA	Economic Growth and Regulatory Paperwork Reduction Act of 1996
CFPB	Consumer Financial Protection Bureau	EGRRCPA	Economic Growth, Regulatory Relief, and Consumer Protection Act
CFR	Center for Financial Research	EU	European Union
CFTC	Commodity Futures Trading Commission	ERM	Enterprise Risk Management
CIO	Chief Information Officer	FAQ	Frequently Asked Questions
CIOO	Chief Information Officer Organization	FASB	Financial Accounting Standards Board
		FBIIC	Financial and Banking Information Infrastructure Committee
		FBO	Foreign Bank Organization

FDI Act	Federal Deposit Insurance Act	GECC	General Electric Capital Corporation, Inc.
FDIC	Federal Deposit Insurance Corporation	GPRA	Government Performance and Results Act
FEHB	Federal Employees Health Benefits	G-SIBs	Global Systemically Important Banks
FERS	Federal Employees Retirement System	G-SIFI	Global SIFIs
FFB	Federal Financing Bank	HMDA	Home Mortgage Disclosure Act
FFIEC	Federal Financial Institutions Examination Council	HQLA	High quality liquid asset
FFMIA	Federal Financial Management Improvement Act	IADI	International Association of Deposit Insurers
FHLB	Federal Home Loan Banks	ICIPC	Intelligence and Critical Infrastructure Protection Committee
FICO	Financing Corporation	IDI	Insured Depository Institution
FIL	Financial Institution Letter	IMF	International Monetary Fund
FinCEN	Financial Crimes Enforcement Network	IMFB	IndyMac Federal Bank
FinTech	Financial Technology	InTREx	Information Technology Risk Examination Program
FIRREA	Financial Institutions Reform, Recovery and Enforcement Act	ISM	Information Security Manager
FIs	Financial Institutions	IT	Information Technology
FIS	Financial Institution Specialists	ITCIP	Insider Threat and Counterintelligence Program
FISMA	Federal Information Security Modernization Act of 2014	ITSP	Information Technology Strategic Plan
FLEC	Federal Financial Literacy and Education Commission	LCR	Liquidity coverage ratio
FMFIA	Federal Managers' Financial Integrity Act	LIBOR	London Inter-bank Offered Rate
FMSP	Financial Management Scholars Program	LIDI	Large Insured Depository Institution
FRB	Board of Governors of the Federal Reserve System	LLC	Limited Liability Company
FRF	FSLIC Resolution Fund	MDI	Minority Depository Institutions
FSB	Financial Stability Board	MOL	Maximum Obligation Limitation
FS-ISAC	Financial Services Information Sharing and Analysis Center	MOU	Memoranda of Understanding
FSLIC	Federal Savings and Loan Insurance Corporation	MRM	Model Risk Management
FSOC	Financial Stability Oversight Council	MRBA	Matters Requiring Board Attention
FTE	Full-Time Employee	MWOB	Minority- and Women-Owned Business
GAAP	Generally Accepted Accounting Principles	MWOLF	Minority- and Women-Owned Law Firms
GAO	U.S. Government Accountability Office	NCATS	National Cybersecurity and Technical Services
GDP	Gross Domestic Product	NCUA	National Credit Union Administration

NITTF	National Insider Threat Task Force	SBA	Small Business Administration
NPR	Notice of Proposed Rulemaking	SCRA	Servicemembers Civil Relief Act
NSFR	Net Stable Funding Ratio	SEATAB	Security and Enterprise Architecture Technical Advisory Board
OCC	Office of the Comptroller of the Currency	SEC	Securities and Exchange Commission
OCFI	Office of Complex Financial Institutions	SIFI	Systemically Important Financial Institution
OIG	Office of Inspector General	SLA	Shared-Loss Agreement
OJT	On-the-Job Training	SME	Subject Matter Expert
OLA	Orderly Liquidation Authority	SMS	Systemic Monitoring System
OLF	Orderly Liquidation Fund	SNC	Shared National Credit Program
OMB	U.S. Office of Management and Budget	SRAC	Systemic Resolution Advisory Committee
OMWI	Office of Minority and Women Inclusion	SRR	SIFI Risk Report
OO	Office of the Ombudsmen	SRB	Single Resolution Board
OPM	Office of Personnel Management	SSGN	Structured Sale of Guaranteed Note
ORE	Owned Real Estate	TILA	Truth in Lending Act
OTS	Office of Thrift Supervision	TIPS	Treasury Inflation-Protected Securities
P&A	Purchase and Assumption	TSP	Federal Thrift Savings Plan
PIV	Personal Identity Verification	TSP (IT-related)	Technology Service Providers
Q&A	Question and Answer	UBPR	Uniform Bank Performance Report
QBP	Quarterly Banking Profile	UFIRS	Uniform Financial Institutions Rating System
QFC	Qualified Financial Contracts	UK	United Kingdom
REMA	Reasonably Expected Market Area	URSIT	Uniform Rating System for Information Technology
ReSG	FSB's Resolution Steering Group	VIEs	Variable Interest Entities
RESPA	Real Estate Settlement Procedures Act	WE	Workplace Excellence
RMIC	Risk Management and Internal Controls	WIOA	Workforce Investment Opportunity Act
RMS	Division of Risk Management Supervision	YSP	Youth Savings Program
RTC	Resolution Trust Corporation		