

1 STATE OF OKLAHOMA

2 1st Session of the 57th Legislature (2019)

3 COMMITTEE SUBSTITUTE  
4 FOR

5 SENATE BILL 584

6 By: Stanislawski

7 COMMITTEE SUBSTITUTE

8 An Act relating to public finance; amending 62 O.S.  
9 2011, Section 34.32, as last amended by Section 1,  
10 Chapter 285, O.S.L. 2014 (62 O.S. Supp. 2018, Section  
11 34.32), which relates to Security Risk Assessments;  
12 eliminating certain exception; establishing  
13 requirement for information security audit conducted  
14 by certain firm under certain basis; requiring  
15 submission of information security audit findings;  
16 modifying requirement for submission of findings  
17 within certain time; requiring submission of a list  
18 of remedies and a timeline for the repair of any  
19 deficiencies within certain time; requiring the  
20 Information Services Division to assist in repairing  
21 vulnerabilities; modifying reporting requirements;  
22 requiring technology system consolidation under  
23 certain circumstance; and providing an effective  
24 date.

BE IT ENACTED BY THE PEOPLE OF THE STATE OF OKLAHOMA:

SECTION 1. AMENDATORY 62 O.S. 2011, Section 34.32, as  
last amended by Section 1, Chapter 285, O.S.L. 2014 (62 O.S. Supp.  
2018, Section 34.32), is amended to read as follows:

Section 34.32. A. The Information Services Division of the  
Office of Management and Enterprise Services shall create a standard

1 security risk assessment for state agency information technology  
2 systems that complies with the International Organization for  
3 Standardization (ISO) and the International Electrotechnical  
4 Commission (IEC) Information Technology - Code of Practice for  
5 Security Management (ISO/IEC 27002).

6 B. Each state agency that has an information technology system  
7 shall obtain an information security risk assessment to identify  
8 vulnerabilities associated with the information system. ~~Unless a~~  
9 ~~state agency has internal expertise to conduct the risk assessment~~  
10 ~~and can submit certification of such expertise along with the annual~~  
11 ~~information security risk assessment, the risk assessment shall be~~  
12 ~~conducted by a third party.~~ The Information Services Division of  
13 the Office of Management and Enterprise Services shall approve not  
14 less than two firms which state agencies may choose from to conduct  
15 the information security risk assessment. A state agency with an  
16 information technology system that is not consolidated under the  
17 Information Technology Consolidation and Coordination Act or that is  
18 otherwise retained by the agency shall additionally be required to  
19 have an information security audit conducted by a firm approved by  
20 the Information Services Division that is based upon the most  
21 current version of the NIST Cyber-Security Framework, and shall  
22 submit a final report of the information security risk assessment  
23 and information security audit findings to the Information Services  
24 Division ~~by the first day of December of each year.~~ Agencies shall

1 also submit a list of remedies and a timeline for the repair of any  
2 deficiencies to the Information Services Division within ten (10)  
3 days of the completion of the audit. The final information security  
4 risk assessment report shall identify, prioritize, and document  
5 information security vulnerabilities for each of the state agencies  
6 assessed. The Information Services Division shall assist agencies  
7 in repairing any vulnerabilities to ensure compliance in a timely  
8 manner.

9 C. The Subject to the provisions of subsection C of Section  
10 34.12 of this title, the Information Services Division shall report  
11 the results of the state agency assessments and information security  
12 audit findings required pursuant to this section to the Governor,  
13 the Speaker of the House of Representatives, and the President Pro  
14 Tempore of the Senate by the first day of January of each year. Any  
15 state agency with an information technology system that is not  
16 consolidated under the Information Technology Consolidation and  
17 Coordination Act that cannot comply with the provisions of this  
18 section shall consolidate under the Information Technology  
19 Consolidation and Coordination Act.

20 SECTION 2. This act shall become effective November 1, 2019.

21

22 57-1-1931 MG 2/21/2019 2:03:03 PM

23

24