

## Exhibit 17

### Action Item

#### Consideration of the Internal Audit Plan and Risk Assessment for the 2014-15 and 2015-16 Fiscal Years

---

The mission of the Internal Audits Unit within the Legal & Audit Services Division is to assist the Commission in the discharge of its oversight, management and operating responsibilities for the state and federal financial aid programs it administers. By conducting internal audits of its processes, the Commission can improve its control, risk management and governance practices.

For a variety of reasons, including the departure of the previous internal auditor and other considerations, it has been several years since the Commission adopted a comprehensive internal audit plan. Even without a specific plan, the Commission has still been able to evaluate some aspects of its internal processes through both its institutional program compliance reviews and other mandatory state reporting. For example, when conducting program compliance reviews, the program compliance auditors are able to assess how different aspects of applicant eligibility, institutional reporting and payments are handled by the Commission's systems and whether these processes function in accordance with statutory requirements and operational expectations.

In addition, as a state body, the Commission must complete the reporting required by the Financial Integrity and State Manager's Accountability (FISMA) Act of 1983. FISMA was enacted to reduce the waste of resources and strengthen accounting and administrative control. FISMA requires each state agency head to maintain effective systems of internal accounting and administrative control, to evaluate the effectiveness of these controls on an ongoing basis, and to biennially review and prepare a report on the adequacy of the agency's systems of internal accounting and administrative control. Through the FISMA, the Commission performs a risk assessment and develops a corrective action plan to address the identified risks. The Commission's most recent FISMA reporting was done in December 2013. The Commission continues to work on its corrective actions in response to the identified risks.

The Commission is also required to submit a management representation letter (MRL) as part of State's overall response to the Single Audit. The Single Audit Act and Office of Management and Budget (OMB) Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations*, requires non-federal entities that expend equal to or in excess of \$500,000 in federal awards within a fiscal year to have an audit performed in accordance with the Single Audit Act. The MRL is signed by the Commission's Executive Director and Chief of Administration and External Affairs. The most recent MRL was submitted in April 2014.

Recognizing the importance of having a dedicated internal auditor, the Commission recently shifted one of its experienced program compliance auditors to the internal auditor position to formally reestablish that function within the Commission. Staff is now seeking the adoption of a two-year internal audit plan to direct the activities of the internal auditor.

## California Student Aid Commission

The proposed Internal Audit Plan and Risk Assessment for the 2014-15 and 2015-16 Fiscal Years, Exhibit 17.1, is based upon the results of the FISMA and the application of five additional risk factors that rank internal operations based upon a scoring system that assigns a point value for each risk factor and calculates an overall risk score. These risk factors include:

- Business Mandates
- Transaction volumes
- Dollar value of transactions
- Previous audit findings
- Potential impact on the Commission's reputation

These point rankings were then incorporated into the proposed plan and a proposed audit plan was drafted that focuses on the highest risk areas as identified in the risk assessment. The proposed internal audits are as follows:

- Personally Identifiable Information (PII) Protection (Information Security)

This audit would seek to determine the adequacy of the Commission's internal controls to protect the confidentiality and integrity of the PII in its possession; including a review of the policies, practices and security controls related to the protection of sensitive financial and borrower information used in day-to-day operations.

- Information Technology Modernization

This audit would seek to determine the adequacy of the Commission internal controls to ensure that its information technology systems meet the Commission's current and future business needs.

- Cal Grant Program – Selection and Notification

This audit would seek to determine the adequacy of the Commission's internal controls in awarding applicants and ensuring compliance with the Education Code as it relates to Cal Grant eligibility for entitlement and competitive students, as well as, notification processes for both student and institutions.

- Cal Grant Program - Dream Act New Applicant Eligibility

This audit would seek to determine the adequacy of the Commission's internal controls in collecting applicant data, awarding applicants and ensuring compliance with the Education Code as its relates to Cal Grant eligibility for Dream Act students.

- Departmental Succession Planning

This audit would seek to ensure the sustainability of critical business process and systems through appropriate documentation of policies, procedures and functions. This audit would evaluate the extent to which the Commission suffers from key-person dependency in mission-critical areas and the actions being taken to address succession planning.

- Network Security

## California Student Aid Commission

This audit would seek to determine the adequacy of internal controls to protect the integrity of the Commission's information technology system including a review of the system configuration documentation, network settings, use of guest or generic accounts, physical connections and traffic load.

**Recommended Action:** Staff recommends that the Internal Audit Plan and Risk Assessment for the 2014-15 and 2015-16 Fiscal Years be adopted.

**Responsible Person(s):** Keri Faseler Tippins  
General Counsel and Chief  
Legal & Audit Services Division



# **Internal Audit Plan and Risk Assessment**

**FYs 2014 – 2015 and 2015 – 2016**



## Table of Contents

	Page
I. AUDIT PLAN	
A. Executive Summary .....	2
B. Planned Internal Audits for October 1, 2014 through June 30, 2016 .....	3
C. Allocation of Audit Resources .....	5
II. RISK ASSESSMENT	
A. Risk Assessment Process .....	6
B. Comprehensive Assessment .....	7
C. Risk Assessment Factors .....	8



---

## Executive Summary

---

The Financial Integrity and State Manager's Accountability Act (FISMA) of 1983 requires each state agency to maintain effective systems of internal accounting and administrative control, to evaluate the effectiveness of these controls on an ongoing basis, and report on adequacy of these controls every two years. State entities are required to submit a certification letter on the adequacy of their internal and administrative controls by December 31 of each odd-numbered year. The next certification is due December 31, 2015.

The California Department of Finance Office of State Audits and Evaluations (OSAE) developed an audit guide for the evaluation of accounting and administrative controls to fulfill FISMA requirements. The guide indicates that a risk-based approach is the best method to use in determining audit focus. It further states that, because each entity's processes are unique, the guide may be modified based upon the results of the risk assessment.

The Audit Plan was created based on the annual needs of the Commission as well as the 2013 risk assessment. The risk assessment process involved meeting with management staff to discuss risks. They were required to fill out questionnaires and a spreadsheet stating their business functions, risks associated with those and controls in place to mitigate any risk. Based on the written and oral statements certain areas were selected for further audit and review. Some audits mentioned on the plan did not come from the risk assessment but from outside input regarding certain control concerns.

The Audit Plan provided in this document has been developed using a risk-based approach specific to CSAC operations. This plan provides for audits of high risk areas and a limited amount of special audit related projects for the Commission. The Commission Internal Audit Unit includes one staff auditor position. Actual scheduling may be affected by personnel turnover or unforeseen circumstances in a scheduled audit. The audits included in this plan are those that can be covered with existing CSAC internal audit resources.

The Internal Audit Unit is implementing this plan for the 2014- 2015 and 2015-16 fiscal years. The plan is a living document which allows for shifting priorities as they arrive.

## Planned Audits and Projects by Year

The chart below identifies the high risk areas that will be audited during each year of the two year audit cycle ending June 30, 2016. A brief description of each audit is set forth below.

<b>High Risk Audits</b>	<b>2014-15</b>	<b>2015-16</b>
Personally Identifiable Information Protection	X	
Departmental Succession Planning	X	
Information Technology Modernization	X	
Cal Grant Program - Dream Act New Applicant Eligibility		X
Cal Grant Program - Selection and Notification		X
Information Security Program		X
Network Security		X
<b>Required Audits &amp; Activities</b>		
FISMA	X	X
Single Audit	X	X

- Personally Identifiable Information (PII) Protection (Information Security)** – This audit will review the established controls in place to safeguard PII. It would seek to determine the adequacy of the Commission’s internal controls to protect the confidentiality and integrity of the PII in its possession; including a review of the policies, practices and security controls related to the protection of sensitive financial and borrower information used in day-to-day operations.
- Departmental Succession Planning** –This audit will seek to ensure the sustainability of the Commission’s critical business processes and systems through appropriate documentation of policies, procedures and functions. This audit would evaluate the extent to which the Commission suffers from key-person dependency in mission-critical areas and the actions being taken to address succession planning.
- Information Technology Modernization** – A review of the current technology (GDS) challenges. This audit would seek to determine the adequacy of the Commission internal controls to ensure that its information technology systems meet the Commission’s current and future business needs.
- Cal Grant Program – Dream Act New Applicant Eligibility**– This audit would seek to determine the adequacy of the Commission’s internal controls in collecting applicant data, awarding applicants and ensuring compliance with the Education Code as its relates to Cal Grant eligibility for Dream Act students.



- 
- **Cal Grant Program – Selection and Notification** – This audit would seek to determine the adequacy of the Commission’s internal controls in awarding applicants and ensuring compliance with the Education Code as it relates to Cal Grant eligibility for entitlement and competitive students, as well as, notification processes for both student and institutions.
  - **Information Security Program (300 hours)** – This audit would seek to determine the adequacy of internal controls to protect the integrity of the Commission’s information technology system including a review of the system configuration documentation, network settings, use of guest or generic accounts, physical connections and traffic load.
  - **Network Security** – This audit would seek to determine the adequacy of internal controls to protect the integrity of the Commission’s information technology system including a review of the system configuration documentation, network settings, use of guest or generic accounts, physical connections and traffic load.

---

## Allocation of Audit Resources

---

The approach to developing an annual audit plan recognizes that resources of personnel and dollars are limited which prohibits one hundred percent audit coverage each year. This limiting factor is inherent in the concept of utilizing a risk assessment to help prioritize audits.

The estimated number of available staff hours to conduct internal audits during the period October 1, 2014 through June 30, 2016 is presented below.

### Internal Audits

High Risk	2424
Required Audits	200
Follow-up Activities	100
Special Projects	<u>200</u>
Total Audit Hours	2,924

### Available Audit Hours (October 2014 – June 2016)

Total Hours (21 months * 168 hours)	3528
Continuing Education / Training	-104
Leave (personal time and holidays)	-300
Staff/Commission Meetings and other	
Administrative Responsibilities	<u>-200</u>
Audit Hours Subtotal	2924

**Note:** The duration of each audit is an estimate which may vary due to the scope and objectives of the audit determined during the initial planning process and unanticipated issues that may arise during the audit. Special requests from the Executive Director and/or Audit Committee considered a priority may also alter the completion of the Audit Plan as scheduled. However, an additional 200 hours has been included in the Audit Plan to more readily allow all audits to in the plan to be completed even in the event an additional audit is assigned.



---

## Risk Assessment Process

---

The risk assessment process is an integral part of developing an audit plan. The objective of the assessment is to identify and prioritize potential audits which pose the greatest risk and liability to the Commission.

The process begins by identifying the total population of potential audits. Internal Audit accomplished this by conducting interviews with Commission managers and staff, reviews of Commission prepared documentation, and Internal Audit staff's knowledge about the Commission's operations.

Once the potential audit universe had been determined, each auditable unit was evaluated against the following five risk factors:

- Business mandates
- Transaction volumes
- Dollar value of transactions
- Previous external audit findings
- Potential Impact on the Commission's reputation

Internal Audits evaluated each auditable unit and assigned three possible risk levels for each risk factor. The risk impacts are identified as High, Medium, and Low. Level high represents high impact; level medium indicates moderate impact; and level low signifies minimal impact.

The risk assessment process is an ongoing effort. Internal and external risks constantly develop, presenting new concerns for the Commission. Change itself is a risk and the Commission must continually adapt its policies, procedures, and business practices to manage operations to an acceptable risk level.

The risk factors and scoring process will be periodically evaluated and modified, as necessary, in order to continually improve the audit plan



---

## Comprehensive Assessment

---

The comprehensive risk assessment is presented in matrix format on the next several pages. The matrix was developed as part of the 2013 Department Wide Risk Assessment for FISMA. Additionally, the matrix was developed as part of the 2005 audit plan. The business processes and audit risks have not changed significantly over time. Internal Audit recognizes that it may be necessary to re-evaluate the plan at the end of the current fiscal year as significant changes in policies, procedures and/or business activities occur and modify the plan as needed.

		Business Mandates	Transaction Volume	Dollar Value of Transactions	Previous External Audit Findings	Potential Impact on the Commission's Reputation
<b>A. GRANTS AND PROGRAMS</b>						
1	Cal Grant Institution participation	5	1	N/A	N/A	2
	<ul style="list-style-type: none"> <li>Mailing and receipt of new and renewal Institution Participation Agreements (IPAs)</li> <li>Eligibility determination activities for new IPAs</li> <li>Renewal process (every four years)</li> <li>Data entry of school information</li> </ul>	California Education Code (CEC) section 69432.7(l); Institution Participation Agreement; California Code of Regulations (CCR); Cal Grant Manual.	In 2012-13 there were 302 eligible Cal Grant Institutions. An additional 154 were determined to be ineligible, but may have had renewal students.		Process subject to State audit/oversight; however, no recent audits conducted.	
2	Cal Grant new applicant eligibility	5	5	N/A	N/A	2
	<ul style="list-style-type: none"> <li>Data collection activities - Institutional Student Information Record (ISIR)</li> <li>Applicant record maintenance activities</li> <li>Eligibility determination in line with statutory requirements and other awarding criteria</li> </ul>	CEC 69430; CCR 30000; Cal Grant Manual.	Approximately 1.3 million applications received from new applicants for FY 2012-13.		Process subject to State audit/oversight; however, no recent audits conducted.	
3	Cal Grant selection and notification	5	5	5	N/A	2
	<ul style="list-style-type: none"> <li>Entitlement scoring, selection and approval activities</li> <li>Competitive scoring, selection and approval activities</li> <li>Notification of awards</li> <li>Notification of non-eligibility/disqualification</li> <li>Tracking activities</li> </ul>	Highly regulated; CEC 69430.	For FY 2012-2013: approximately 120,000 new entitlement notifications	For FY 2012-2013: Approximately \$357 million in entitlement awards, \$121 million in competitive awards, and \$102 million in existing awards.	Process subject to State audit/oversight; however, no recent audits conducted.	
4	Cal Grant corrections and appeals	5	4	N/A	N/A	1
	<ul style="list-style-type: none"> <li>Appeal review activities</li> <li>Entitlement application correction processing</li> <li>Notification to applicants</li> <li>Overpayments</li> </ul>	G-11(4/04)-Appeal Information for Entitlement Applicant Cal Grant Program; CEC 66021.2 and 69530-69547; CCR 3000-30904.	Approximately 4,500 appeals received in 2013.		Process subject to State audit/oversight; however, no recent audits conducted.	

		<b>Business Mandates</b>	<b>Transaction Volume</b>	<b>Dollar Value of Transactions</b>	<b>Previous External Audit Findings</b>	<b>Potential Impact on the Commission's Reputation</b>
5	Cal Grant disbursements	5	4	5	N/A	5
	<ul style="list-style-type: none"> <li>• Advancement calculations</li> <li>• Advancement payments - claim schedule preparation and submission to SCO</li> <li>• Authorizations</li> <li>• Data collections of payment transactions reported by schools</li> <li>• Reconciliation of payments to school outstanding balances</li> <li>• Supplemental payments - claim schedule preparation and submission to SCO</li> <li>• Overpayments</li> <li>• Refunds</li> </ul>	CEC 69432.8; Cal Grant Manual; Operations Memos.	Approximately 302 schools receive funds through 12,000 Disbursements annually.	Approximately \$1.3 billion disbursed to schools FY 2012-13.	Process subject to State audit/oversight; however, no recent audits conducted.	
6	Cal-SOAP - contracting, funding and oversight other than Program Compliance Review	5	1	3	N/A	3
	<ul style="list-style-type: none"> <li>• Awarding of block grants</li> <li>• Disbursement of funds</li> <li>• Oversight of contracts with consortia</li> </ul>	Cal-SOAP Policies and Procedures Reference Manual; CEC 69560; Standard Contract; DGS regulations as it relates to the contracting process.	There are 15 consortia serving 27 counties.	Approximately \$7.2 million.	CSAC's Program Compliance Branch performs fiscal audits at the consortia level and has issued findings. The Internal Audit focus would be on activities performed by CSAC in contracting, funding and oversight.	
7	Chafee Grant Program	5	2	3	N/A	2
	<ul style="list-style-type: none"> <li>• Application</li> <li>• Notification to schools to perform a need analysis</li> <li>• Award processing (including notification)</li> <li>• Payment processing</li> <li>• Renewal</li> <li>• Data submission to Department of Social Services</li> <li>• Compliance with the interagency agreement</li> </ul>	Interagency agreement between CSAC and Department of Social Services; Social Security Act (sections 474, 477).	3570 awards issued in FY 2012-13.  1,500 new awards annually.	Approximately \$11.3 million in funds disbursed for FY 2012-13.	Process subject to Federal or State audit/oversight; however, no recent audits conducted.	

		Business Mandates	Transaction Volume	Dollar Value of Transactions	Previous External Audit Findings	Potential Impact on the Commission's Reputation
8	Assumption Program of Loans for Education (APLE)	5	3	5	N/A	2
	<ul style="list-style-type: none"> <li>• Application</li> <li>• Notification of award</li> <li>• Renewal</li> <li>• Tracking</li> <li>• Payment processing</li> <li>• Preparation and submission of Annual Legislative Report</li> <li>• Interactions with the County Office of Education</li> </ul>	California Education Code (sections 69612–69615.6); Title 5. Education Division 4. Chapter 1. Article 14. 30701.	Program is being phased out.	\$19.8 million in grant awards for FY 20012-13.	Process subject to State audit/oversight; however, no recent audits conducted.	
9	Law Enforcement Personnel Dependents Grant	5	1	1	N/A	1
	<ul style="list-style-type: none"> <li>• Application</li> <li>• Renewal</li> <li>• Payment processing</li> </ul>	Labor Code (sections 4709 a– h); California Education Code (sections 69535 k –69535.1 a-c); SB 730.	7 recipients in FY2012-2013.	\$45,000 in grant awards for FY 2003-2012-13.	Process subject to State audit/oversight; however, no recent audits conducted.	
10	Child Development Teacher and Supervisor Grant Program	5	1	1	N/A	2
	<ul style="list-style-type: none"> <li>• Application</li> <li>• Notification of award</li> <li>• Renewal</li> <li>• Tracking</li> <li>• Payment processing</li> <li>• Reimbursement processing (from California Department of Education)</li> <li>• Compliance with interagency agreement</li> <li>• Preparation and submission of annual legislative report</li> </ul>	Interagency agreement between CSAC and California Department of Education; California Education Code (sections 69620 – 69629).	Between 500-600 applicants.  Up to 100 new grants awarded each fiscal year.	\$136,500 annually.	Process subject to Federal or State audit/oversight; however, no recent audits conducted.	

**B. GRANT AND PROGRAM OPERATIONAL SUPPORT**

11	Communications and Publications	5	1	N/A	N/A	1
	<ul style="list-style-type: none"> <li>• Approval of press releases, publications and graphic designs</li> <li>• Responding to media inquiries</li> </ul>	CEC; CCR.	Approximately 225 media contacts and 275 other communications annually.			
12	Outreach/Public Awareness Activities	5	1	4	N/A	1
	<ul style="list-style-type: none"> <li>• Procurement of outreach and Publications materials</li> <li>• Disbursement of funds</li> <li>• Appropriateness of expenditures</li> </ul>	Internal Policies		Approximately \$125,000 on communications and publications		

		Business Mandates	Transaction Volume	Dollar Value of Transactions	Previous External Audit Findings	Potential Impact on the Commission's Reputation
13	Cal Grant projections/baseline	5	1	N/A	N/A	2
<ul style="list-style-type: none"> <li>Forecasting disbursements</li> </ul> <p>Note: Internal Audit would not re-perform the calculations for projections. Internal Audit will review the projection methodology and approval process.</p>		Projections are required by DOF and LAO.	Ongoing, monitored at least monthly.		Process subject to State audit/oversight; however, no recent audits conducted.	
14	Program compliance	5	1	N/A	N/A	1
<ul style="list-style-type: none"> <li>Selection of institutions based on regulatory criteria</li> <li>Scope of reviews encompass institutions adherence with regulatory requirements</li> <li>Oversight of reviews</li> <li>Completeness of reports</li> <li>Implementation of report action items</li> </ul>		Review is based on all applicable regulations; 34 CFR 600: Institution Eligibility; 34 CFR 668: Student Eligibility; CEC 69510: Student Aid Commission; Cal Grant Manual; Institution Participation Agreement.	Approximately 33 performance reviews are conducted annually.		Process subject to State audit/oversight; however, no recent audits conducted.	

**C. FINANCIAL MANAGEMENT**

15	Budget development and management (revenue and expenditures)	5	1	5	N/A	3
<ul style="list-style-type: none"> <li>Annual budget development methodology and management sign-off</li> <li>Ongoing budget variance monitoring</li> <li>Budget revisions, including approvals</li> </ul>		SAM (sections 20050, 8300-8382, and 6400) and legislative/governor's processes.	Activity performed once annually with a few revisions and analysis during the year. Monitored monthly.	Approximately \$1.9 billion in grant disbursements and \$12.4 million in operating expenses.	Process subject to State audit/oversight; however, no recent audits conducted.	
16	Procurements - general operations (including computer hardware, software and technology consulting)	5	1	2	N/A	3
<ul style="list-style-type: none"> <li>Third-party contract and/or purchase order development, including approvals</li> <li>Development of interagency agreements, including approvals</li> <li>Purchasing practices, including vendor and product selection</li> <li>Contract/purchase order management</li> <li>Encumbering funds</li> <li>Contract/purchase order/interagency adjustments</li> </ul>		SAM (sections 1200, 20050, 8340, 8422.1, 8602, 8630 and 3500), California Administrative Code (Title 2, Division 2, Section 677) and State Procurement and Contracting Manuals.	Less than 300 purchase orders/ contracts on an annual basis.	Approximately \$1 million annually.	Process subject to State audit/oversight; however, no recent audits conducted.	

		Business Mandates	Transaction Volume	Dollar Value of Transactions	Previous External Audit Findings	Potential Impact on the Commission's Reputation
17	Accounts payable and disbursements - general operations (i.e. other than grants and Cal-SOAP disbursements)	5	2	5	N/A	3
	<ul style="list-style-type: none"> <li>• Payment approval activities</li> <li>• Budget availability determination</li> <li>• Management of payment timing (late- payment penalty avoidance, early-payment discount advantages, just-in-time payment to avoid loss of interest earnings, etc.)</li> <li>• Preparation of claims schedules for submission to SCO</li> <li>• Payment transaction recording in financial system</li> </ul>	SAM (sections 20050, 8000+ and 7908).	Less than 5,000 transactions annually.	Approximately \$2 million in annual CSAC expenditures.	Process subject to State audit/oversight; however, no recent audits conducted.	
18	Reconciliations - SCO and bank	5	1	5	N/A	5
	<ul style="list-style-type: none"> <li>• Identification and documentation of reconciling items</li> <li>• Resolution of reconciling items</li> </ul>	SAM (section 7900).	Performed monthly.	Significant amount of money moving in and out of accounts.	Process subject to State audit/oversight; however, no recent audits conducted.	
19	Fixed assets management	4	2	3	N/A	2
	<ul style="list-style-type: none"> <li>• Receipt of physical assets</li> <li>• Physical tracking</li> <li>• Warranties and insurance on fixed assets</li> <li>• Capitalization and depreciation</li> <li>• Disposal process</li> <li>• Recording transactions in asset management and financial systems</li> </ul>	SAM (sections 20050, 3520.2, 8600, 7977-7978, 1335.1, and 7800) along with DGS requirements involving accounting for surplus and write-offs.	Approximately 3,000 fixed assets tracked for CSAC.	Approximately \$9.2 million in fixed assets are tracked.	Process subject to State audit/oversight; however, no recent audits conducted.	
20	Revolving Fund	4	1	1	N/A	3
	<ul style="list-style-type: none"> <li>• Travel expense claims</li> <li>• Allowable advances</li> <li>• Approvals</li> <li>• Replenishment</li> </ul>	DPA Regulations, SAM (sections 8100 and 20050), and bargaining union contracts.	300 – 400 transactions annually.	Approximately \$100,000 annually.	Process subject to State audit/oversight; however, no recent audits conducted.	
21	Manual journal entries	1	1	5	N/A	2
	<ul style="list-style-type: none"> <li>• Documentation maintained to support journal entries</li> <li>• Journal entry review and approvals</li> <li>• Data entry of transactions to financial system</li> </ul>	Low - no specific regulatory requirements addressing this area other than requirement to maintain proper accounting.	650 manual journal entries annually	Including General Fund, Student Loan Operating Fund, Cash for College Fund and Federal Fund	Process subject to State audit/oversight; however, no recent audits conducted.	

		Business Mandates	Transaction Volume	Dollar Value of Transactions	Previous External Audit Findings	Potential Impact on the Commission's Reputation
22	Financial reporting	5	1	N/A	N/A	2
<ul style="list-style-type: none"> <li>Source data</li> <li>Report submission/distribution</li> <li>Adjustments to data previously reported</li> </ul>		SAM (sections 7900 and 10608).	Approximately 40 reports generated at year end.		Process subject to State audit/oversight; however, no recent audits conducted.	
23	Cashiering	5	1	5	N/A	3
<ul style="list-style-type: none"> <li>Delivery of physical checks to CSAC</li> <li>Wire transfers to STO and/or bank for CSAC</li> <li>Transaction postings to all systems</li> <li>Remittance preparation to claim funds</li> <li>Reconciliation activities, including handling and resolution of unidentified payments</li> <li>Bank deposit preparation</li> <li>Delivery of deposit to bank</li> </ul>		SAM 8000.	630 deposits annually.		Process subject to State audit/oversight; however, no recent audits conducted.	

**D. HUMAN RESOURCES AND PAYROLL**

24	Payroll processing	5	2	3	N/A	2
<ul style="list-style-type: none"> <li>Maintenance and control of employee information (salary, deductions, elections, social security number, home address, etc.)</li> <li>Data exchanged between CSAC, SCO,</li> <li>DPA and other State agencies/departments Reporting to regulatory bodies</li> <li>Handling and distribution of physical checks, electronic payments, and pay stubs</li> <li>Salary adjustments</li> <li>Termination payments and removal from payroll</li> </ul>		Family Medical Leave Act, Union Contracts, DPA, Executive Orders.	Approximately 108 CSAC staff paid monthly, additional overtime payments as required.	Approximately \$10 million in salaries and benefits paid annually.	Process subject to State audit/oversight; however, no recent audits conducted.	
25	Hiring, retirement, transfers, and termination processes	5	1	N/A	N/A	3
<ul style="list-style-type: none"> <li>Entrance/Exit procedures and checklists</li> <li>Retirement processing</li> <li>Transfer processing</li> <li>ID badges, keys collected and locks changed</li> <li>Final salary payments</li> <li>Exit interview</li> <li>Access changed for transfers</li> </ul>		Internal procedures and CalHR.			Process subject to State audit/oversight; however, no recent audits conducted.	

		Business Mandates	Transaction Volume	Dollar Value of Transactions	Previous External Audit Findings	Potential Impact on the Commission's Reputation
26	Employee performance assessment	3	1	N/A	N/A	1
	<ul style="list-style-type: none"> <li>Performance expectation setting</li> <li>Performance tracking and evaluation</li> </ul>	Union contract and DPA rules and regulations.	Approximately 108 civil service staff receive annual performance assessments, merits adjustment evaluations, etc. Probation reports completed for new hires and promotions.		Process subject to State audit/oversight; however, no recent audits conducted.	
27	Employee training	5	1	1	N/A	1
	<ul style="list-style-type: none"> <li>Enforcement of CSAC core training requirements</li> </ul>	Union Contract, DPA, and SAM.	Number of classes attended is low.	Small training budget.	Process subject to State audit/oversight; however, no recent audits conducted.	
28	Exam process	5	1	N/A	N/A	1
	<ul style="list-style-type: none"> <li>Preparation</li> <li>Scoring</li> <li>Minimum qualifications</li> <li>Lateral transfers</li> <li>Scores based on application/resume only</li> </ul>	SAM, Bargaining Union Contract, DPA.	Less than 5 exams conducted annually.		Process subject to State audit/oversight; however, no recent audits conducted.	
29	Conflicts of interest/Statement of Economic Interest, Gifts	5	1	N/A	N/A	4
	<ul style="list-style-type: none"> <li>Identification</li> <li>Investigation</li> <li>Resolution</li> <li>Reporting</li> </ul>	Form 700, Government Code 81000-91015.	About 30 CSAC staff, and 15 Commissioners complete Statement of Economic Interest annually and when leaving a reportable position.		Process subject to State audit/oversight; however, no recent audits conducted.	
30	Personnel records management	5	1	N/A	N/A	1
	<ul style="list-style-type: none"> <li>Employee personal information security</li> <li>Records retention</li> </ul>	Highly regulated.	Low volume – less than 350 files maintained.		Process subject to State audit/oversight; however, no recent audits conducted.	

		<b>Business Mandates</b>	<b>Transaction Volume</b>	<b>Dollar Value of Transaction</b>	<b>Previous External Audit</b>	<b>Potential Impact on the Commission's Reputation</b>
<b>E. TECHNOLOGY MANAGEMENT</b>						
31	Software and hardware management	4	2	1	N/A	2
	<ul style="list-style-type: none"> <li>Maintenance of software licensing agreements, including license renewals</li> <li>Software tracking</li> <li>Sanitizing hardware for disposal or re-use</li> <li>Unauthorized software on desktops or networks</li> <li>Payment of license fees for software no longer in use</li> </ul>	SAM 4846 - Software Management Policy; SAM 4903, 4989 Workgroup Computing Policy-purchasing of IT equipment.	Approximately 2,500 software licenses. Approximately 165 dispositions.	Approximately \$200,000 in software licensing costs FY 2003-2004.	Process subject to State audit/oversight; however, no recent audits conducted.	
32	Change management (for Grant Delivery System-GDS)	4	1	N/A	N/A	2
	<ul style="list-style-type: none"> <li>Implementing changes to production</li> <li>User acceptance testing</li> <li>Sign-offs and approvals</li> <li>Code repository maintained to roll back to previous revisions if problems encountered in production after implementation</li> </ul>	Internal policies requiring sign-offs and approvals for implementing program changes. Implemented applicable industry standards and best business practices.			Process subject to State audit/oversight; however, no recent audits conducted.	
33	External user access to GDS and other CSAC applications	5	5	5	N/A	3
	<ul style="list-style-type: none"> <li>Establishing or changing user access</li> <li>User access appropriateness</li> <li>Removal of access for terminated users</li> </ul>	SAM 4840 Security and Risk Management. CSAC is required to ensure that grant and student information is adequately secured. Internal policies and procedures govern user access.	Approximately 1,200 external users performing thousands of transactions.	External users potentially affecting millions of dollars of transactions.	Process subject to State audit/oversight; however, no recent audits conducted.	
37	Establishing and maintaining internal user access to system hardware and software	5	5	5	N/A	4
	<ul style="list-style-type: none"> <li>Establishing or changing user access, including employees that transfer to a different department</li> <li>User access appropriateness</li> <li>Removal of access for terminated employees</li> </ul>	SAM 4840 Security and Risk Management. CSAC is required to ensure that grant and student information is adequately secured. Internal policies and procedures govern user access.	Approximately 100 users performing thousands of transactions.	Internal users potentially affecting millions of dollars of transactions.	Process subject to State audit/oversight; however, no recent audits conducted.	

		<b>Business Mandates</b>	<b>Transaction Volume</b>	<b>Dollar Value of Transactions</b>	<b>Previous External Audit Findings</b>	<b>Potential Impact on the Commission's Reputation</b>
35	Employee remote access	<b>3</b>	<b>1</b>	<b>1</b>	<b>N/A</b>	<b>2</b>
	<ul style="list-style-type: none"> <li>Remote access users</li> <li>Security over access, including authentication and encryption of data</li> <li>Unauthorized user access</li> </ul>	Senate Bill 1386-encryption of data. Proper set-up of users to ensure proper security of information.	Low number of employees with remote access.	Low dollars associated with remote access.	Process subject to State audit/oversight; however, no recent audits conducted.	
36	Technology project management control	<b>4</b>	<b>1</b>	<b>1</b>	<b>N/A</b>	<b>4</b>
	<ul style="list-style-type: none"> <li>Project management practices and methodology throughout the system development life cycle, including monitoring progress and costs</li> <li>Quality control process, including approvals and sign-offs at milestones</li> <li>User documentation</li> <li>Post-implementation reviews</li> </ul>	Internal discipline/methodology implemented and followed for projects. SAM 4800-roles and responsibilities governing IT projects; SAM 4920 and 4942-feasibility study report requirements.	Approximately 4 projects performed in FY 2012-2013. Approximately 200 defects and enhancements were completed in 2012-2013.	External contracts for IT services were approximately \$850,000 in 2012-13.	Process subject to State audit/oversight; however, no recent audits conducted.	
37	GDS - Data (record) maintenance	<b>5</b>	<b>5</b>	<b>5</b>	<b>N/A</b>	<b>3</b>
	<ul style="list-style-type: none"> <li>Data maintenance changes</li> <li>Review and approval of changes</li> <li>User access</li> </ul>	CSAC is required to maintain accurate grant and student information.	Approximately 6,000 system jobs per year to update information; however, users with data maintenance access could potentially perform changes to any grant or student information.	The majority of data maintenance changes are made to student information and not grant amounts. However, users with this access could potentially affect any information associated with any grant.	Process subject to State audit/oversight; however, no recent audits conducted.	
38	Table maintenance	<b>5</b>	<b>5</b>	<b>5</b>	<b>N/A</b>	<b>1</b>
	<ul style="list-style-type: none"> <li>Additions, changes and deletions made to tables</li> <li>User access to tables</li> <li>Review and approval of changes</li> </ul>	CSAC is required to maintain accurate grant and student information.	Table maintenance updates could potentially impact the total grant portfolio.	Table maintenance updates could potentially impact the total grant portfolio.	Process subject to State audit/oversight; however, no recent audits conducted.	
39	Disaster recovery and business resumption	<b>5</b>	<b>5</b>	<b>5</b>	<b>N/A</b>	<b>3</b>
	<ul style="list-style-type: none"> <li>Plan documentation and testing, including classification of critical applications</li> <li>Application backups</li> <li>Off-site data storage</li> <li>Hot-sites for disaster recovery</li> </ul>	SAM 4843 Recovery Plan; SAM 4903 and 4989 Workgroup Computing Policy-local backup and recovery procedures	Potentially a significant impact on transaction volume should there be a disaster.	Potentially a significant impact on dollar volume of transactions should there be disaster.	Process subject to State audit/oversight; however, no recent audits conducted.	

**Exhibit 17.1**

		<b>Business Mandates</b>	<b>Transaction Volume</b>	<b>Dollar Value of Transactions</b>	<b>Previous External Audit Findings</b>	<b>Potential Impact on the Commission's Reputation</b>
40	Network security	<b>5</b>	<b>5</b>	<b>5</b>	<b>N/A</b>	<b>5</b>
	<ul style="list-style-type: none"> <li>Prevention and detection of viruses or other security threats/vulnerabilities</li> <li>Encryption of network traffic</li> <li>System configuration documentation</li> <li>Network settings and use of guest or generic accounts</li> <li>Physical connections and traffic load</li> <li>Administrator permissions</li> </ul>	Requirements necessary to secure and manage the network and CSAC data. Internal policies pertain to information security; IS 93-05, IS 92-01. SAM 4903 and 4989 Workgroup Computing Policy-password controls.	Extremely large volume of transactions run through the network.	Extremely high dollar volume of transactions run through the network.	Process subject to State audit/oversight; however, no recent audits conducted.	
41	Operating system	<b>3</b>	<b>5</b>	<b>N/A</b>	<b>N/A</b>	<b>4</b>
	<ul style="list-style-type: none"> <li>Maintenance of the operating system, including system patches</li> <li>System audit logs, including security incidents or events, frequency of reviews and policy settings (e.g. logon/logoff- should record failed logon attempts, user/group management-should record additions, deletions or changes to users or group accounts)</li> <li>Trusted domains</li> <li>Security permissions for system directories</li> <li>System programs, commands, utilities and services</li> </ul>	Standard requirements to ensure functionality of the system.	Operating system performs services for application programs.	Operating system handles communication requests from the application and services; dollar value is not applicable.	Process subject to State audit/oversight; however, no recent audits conducted.	
42	Internet access and usage	<b>2</b>	<b>5</b>	<b>N/A</b>	<b>N/A</b>	<b>3</b>
	<ul style="list-style-type: none"> <li>Internet usage policy</li> <li>Monitoring staff internet activity</li> <li>Denial of access to inappropriate sites</li> <li>Downloading of software</li> </ul>	Employees may access inappropriate web sites; potential concerns over downloading software; impact to other CSAC policies; S-001 Internet Access and Use.	Extremely large volume of internet activity.	No dollars associated with internet activity.	Process subject to State audit/oversight; however, no recent audits conducted.	
43	Firewall	<b>5</b>	<b>5</b>	<b>5</b>	<b>N/A</b>	<b>5</b>
	<ul style="list-style-type: none"> <li>Firewall in place between network and external connections</li> <li>Firewall configuration to secure incoming and outgoing traffic and logging of activity</li> <li>Updates and maintenance, including security over accessing the firewall</li> </ul>	Internal business requirements dictate how the firewall should be established.	All activity runs through the firewall- extremely large volume.	All activity runs through the firewall- extremely large dollar volume.	Process subject to State audit/oversight; however, no recent audits conducted.	

		Business Mandates	Transaction Volume	Dollar Value of Transactions	Previous External Audit Findings	Potential Impact on the Commission's Reputation
44	Help desk	1	4	N/A	N/A	2
	<ul style="list-style-type: none"> <li>• Call tracking, handling and resolution, including prioritization and escalation procedures</li> <li>• Technical expertise and on-going training</li> <li>• Internal service level requirements</li> <li>• Help desk software</li> </ul>	Internal process to manage calls.	Approximately 200 calls per week; 10,000 per year.	Dollar value not applicable-offer aid and assistance to users.		
45	Information security program	5	5	5	N/A	5
	<ul style="list-style-type: none"> <li>• Information security awareness</li> <li>• Activities for managing risk, developing security policies, and assigning responsibilities</li> <li>• Monitoring CSAC's computer-related controls</li> </ul>	A significant volume of PII exists on CSAC systems. IS 93-05 and IS 92-01 - Information Security Policies.	Large volume of system activity governed by Information Security policies.	Information security program could potentially impact the grant and specialized program portfolios (over millions of dollars).	Process subject to State audit/oversight; however, no recent audits conducted.	
46	Web services	4	5	2	N/A	4
	<ul style="list-style-type: none"> <li>• Web site security</li> <li>• Defined responsibilities over managing and operating the web site</li> <li>• Approval of changes and updates</li> <li>• Oversight of third party contract</li> </ul>	Business dictates the requirements to ensure functionality of the system.	Large volume of access to the home page and intranet.	Approximately \$200 per month for hosting services with a third party; \$2,400 on an annual basis.	Process subject to State audit/oversight; however, no recent audits conducted.	

**F. Other Areas**

47	Bagley-Keene Open Meeting Act	5	1	N/A	N/A	5
	<ul style="list-style-type: none"> <li>• Includes teleconference meetings and all committee meetings</li> <li>• Proper notice</li> <li>• Proper voting</li> <li>• Sufficient quorum</li> <li>• Closed sessions</li> <li>• Records access</li> <li>• Public participation</li> </ul>	Government Code 6250 et seq.	Approximately 25-30 meetings annually.		Process subject to State audit/oversight; however, no recent audits conducted.	
48	Records management - including retention	4	5	N/A	N/A	2
	<ul style="list-style-type: none"> <li>• Record storage and retrieval</li> <li>• Management of offsite disaster documentation</li> <li>• Approved document retention schedules</li> <li>• Retrieval of documentation stored offsite</li> <li>• Confidential document destruction</li> </ul>	SAM 1600; California Records 14740-14774; Public Records Act 6254.	Thousands of records will be received and generated during the current fiscal year.		Process subject to State audit/oversight; however, no recent audits conducted.	

## Risk Assessment Factors

<b>Factor</b>	<b>Definition</b>	<b>Values</b>
Business Mandates	Consider any regulations, policies or contractual agreements applicable to the department or process under review. The regulatory environment can include State, Federal, and local requirements. Consider the significance of business practices and operations pertaining to the area. Additionally, consider the impact and relative importance of industry standards relative to this area. The greater the number of regulations, policies and/or contractual agreements or the greater the relative importance, the higher the risk ranking.	1 = Low - no regulatory or policies 2 = Medium Low 3 = Medium – small number of regulations and policies 4 = Medium High 5 = High - highly regulated or significant policies and significant impact for non-compliance
Transaction Volume	The average transaction level within the area per year. Evaluate the transaction volume involved. Consider how long it would take before department personnel were overwhelmed by transaction volume if the current processing environment (including systems) failed. Generally, the user should select a higher risk ranking for larger volumes of transactions.	1 = less than 1,000 2 = 1,000 – 5,000 3 = 5,000 – 10,000 4 = 10,000 – 25,000 5 = Over 25,000
Dollar Value of Transactions	If the area/risk involves dollars, typically select the range that most closely represents the average dollar amount of transactions per year. Consider what effect the transaction has on the organization's overall business operations. The greater the effect, the higher the risk rating.	1 = less than \$1 million 2 = \$1 – \$5 million 3 = \$5 – 10 million 4 = \$10 – \$25 million 5 = over \$ 25 million
Previous External Audit Findings	Review the previous external audit report findings and recommendations. Significant control issues or recurring findings should yield high risk rankings. Conversely, less significant report issues should result in a lower risk ranking. If no previous audit has been performed, the risk factor is not applicable.	1 = Low - no control issues or findings 2 = Medium Low 3 = Medium 4 = Medium High 5 = High – significant control issues or recurring findings
Potential Impact on the Commission's Reputation	Consideration of the significance an area of risk poses to public perception of the Commission, how it administers its programs, its financial controls and its compliance with state laws, processes and negative publicity	1 = Low – not likely to cause significant negative publicity or reputational harm should a risk be actualized in the area. 2 = Medium Low 3 = Medium 4 = Medium High 5 = High – significant negative publicity or reputational harm could occur from risks in the area.