

## PCI Survey Results

### Process/Operational – General

#### 1. Who manages your university's relationship with its merchant bank/processor?

Accounting/Controller	14	12.84%
Bursar/Cashier/Student Services	10	9.17%
Finance/Treasury	76	69.72%
Other	9	8.26%
Administrative Specialist	1	0.92%
Director	2	1.83%
Manager	2	1.83%
Manager, Card Services	1	0.92%
Merchant Card Coordinator (MCC)	1	0.92%
Two positions	1	0.92%
UT System	1	0.92%
Total:	109	

#### 2. Who is your merchant bank/processor?

Bancorp	1	1.82%
Bank of America	4	7.27%
Chase Paymentech Solutions	13	23.64%
Citizen's Bank	1	1.82%
Fifth Third Bank	2	3.64%
First Data	2	3.64%
First Horizon Merchant Services	2	3.64%
Global Payments	7	12.73%
Moneris Solutions	1	1.82%
National City	1	1.82%
NOVA	5	9.09%

NPC Merchant Services	2	3.64%
PennSecurity	1	1.82%
SunTrust Merchant Services	1	1.82%
TIB-The Independent Bankers Bank	1	1.82%
USBank	1	1.82%
Wells Fargo Merchant Services	3	5.45%
More than one	7	12.73%
Total:	55	

**3. Who buying/leasing decisions regarding payment systems? Please specify Title and Department.**

Accounting/Controller	10	6.41%
Bursar/Cashier/Student Services	21	13.46%
Ecommerce	8	5.13%
Finance/Treasury	50	32.05%
Other	64	42.95%
Area purchasing sys	1	0.64%
Asst VC for Business Services	2	1.28%
Business Mgr, Athletics, Theatre	1	0.64%
Centralized	3	1.92%
Department	50	32.05%
Department and Treasury	3	1.92%
Determined by the functional needs	1	0.64%
Director - Intercollegiate Athletics	1	0.64%
Director, Athletic Ticket Office	1	0.64%
Wells Fargo/Individual Depts.	1	0.64%
Total:	153	

**4. How are new merchant accounts established?**

Other	2	3.51%
Primarily centralized, but larger auxiliary units have their own agreements with processors. All merchants established through central office, all ecommerce through central service.	1	1.75%
The business office of each university is responsible for establishing merchant accounts.	1	1.75%
Through a central process with central oversight of account management.	30	52.63%
Through a central process with departmental oversight of account management	20	35.06%
Through a distributed process (departments acquire and manage merchant accounts independently)	3	5.26%
Total:	57	

**Compliance**

**5. Do you require departments to submit a business plan or business case before setting up a new account?**

No	35	68.63%
Yes	16	31.37%
Total:	51	

**6. Do you require each department that processes credit cards sign an internal agreement outlining their responsibilities in regard to card processing?**

No	37	72.55%
Yes	14	27.45%
Total:	51	

**7. Does your school process cards on behalf of professional organizations with which faculty/staff have affiliations?**

No	41	82.00%
Yes	9	18.00%
Total:	50	

**8. Is anyone at your institution designated to conduct annual cost/benefit analyses for card processing on individual merchant accounts?**

Accounting/Controller	1	1.61%
Finance/Treasury	10	16.13%
Other	51	82.26%
No	40	64.52%
Yes	11	17.74%
Total:	62	

**9. If you answered 'Yes' to number 8, does that provoke discussions around continued card acceptance for a particular merchant account or department?**

No	5	41.67%
Yes	7	58.33%
Total:	12	

**10. Does an approval process exist for establishing new merchant accounts?**

No	10	19.23%
Yes, for all new accounts	37	71.15%
Yes, for e-commerce accounts only	5	9.62%
Total:	52	

**11. Who gathers/presents information for approvals of new merchant accounts?**

Accounting/Controller	11	13.41%
Bursar/Cashier/Student Services	8	9.76%
E-Commerce	2	2.44%
Finance/Treasury	44	53.66%
Other	17	20.73%
Asst Vice Chancellor	1	1.22%
Budget/business office	1	1.22%
Business Operations	1	1.22%
Business Services	1	1.22%
Coordinator III	1	1.22%
Dept requesting merchant a/c	6	7.32%
Director	1	1.22%
Manager	2	2.44%
Manager, Card Services	1	1.22%
Various Department members	2	2.44%
Total:	82	

**12. What committee or person approves requests for new merchant accounts?**

Accounting/Controller	13	13.13%
Bursar/Cashier/Student Services	9	9.09%
E-Commerce	6	6.06%
Finance/Treasury	49	49.49%
Other	20	22.22%
Advisory Council	1	1.01%
Assistant VP for Business Affairs	1	1.01%
Asst Vice Chancellor	1	1.01%
Coordinator III	1	1.01%
Director	1	1.01%
Directors, Assoc Directors, AVP's	1	1.01%
Manager	1	1.01%
N/A	10	10.10%
General Counsel, Financial	1	1.01%
Various (general counsel, tax, licensing, etc)	1	1.01%
Vice President for Business Affairs	1	1.01%
Total:	97	

**Process/Operational – Training and Support****13. How many FTE's does your school have dedicated to operational support for merchant card processing?**

>4	2	4.55%
0	13	29.55%
0.5	8	18.18%
1	5	11.36%
1.5	3	6.82%
2	8	18.18%
2.5	2	4.55%
3	1	2.27%
3.5	2	4.55%
Total:	44	

**14. Who is responsible for end-user training (equipment, reconciliation, data protection) and/or support?**

Accounting/Controller	15	9.93%
Bursar/Cashier/Student Services	21	13.25%
E-Commerce	8	5.30%
Finance/Treasury	69	45.70%
Other	38	25.83%
Administrative Specialist	1	0.66%
Analysis & Information	1	0.66%
Asst Vice Chancellor	1	0.66%
Central Administration	1	0.66%
Coordinator III	2	1.32%
Credit Card Processor	11	7.28%
Department	4	2.65%
Director	2	1.32%
General Account provides Reconciliation	1	0.66%

Info Tech Services	4	2.65%
LAN Support Specialist	1	0.66%
Manager	4	2.65%
Manager, Card Services	2	1.32%
PCIDSS Compliance Officer (PCIDSS	1	0.66%
Specialist	1	0.66%
Supervisor	1	0.66%

Total: 151

**15. Please describe the accounting controls around card processing at your school? (e.g. How do you ensure reconciliation, appropriate handling etc.?)**

The University provides merchant processors with formal 'Guidelines for Transacting Credit Card Payments'. This document outlines reconciliation, the journal entry process, and security and record retention policies.

Responsibility lies with individual departments who accept credit cards.

Departments oversee and reconcile their individual accounts. Treasurer's office provides assistance if there are discrepancies on the accounts.

Depts reconcile

Management oversight, subject to audit

We are centralized with our Bank Function. Bank Supervision Depts are notified of any problems

We are in the process of instituting updated University wide policies and procedures that address PCISS security requirements. Departments accepting cc's will be required to read, understand and adhere to those policies to insure safe handling of card info.

Each merchant unit is responsible for reconciling its merchant activity (statement) to the general ledger. Each campus bursar office reconciles the bank account to the posted General Ledger transactions, or items are posted directly from a general settle

Transactions balanced daily. Bank statement reconciled timely. Cash Handling policy strictly enforced.

Almost Non-existent. Reconciliation does not even take place at most units at this time. Projects are in place to develop a new central payment server with a consolidated merchant account and daily transaction reporting to units.

Card processing controls are somewhat defined for e-commerce. Other controls exist at the departmental level, but central oversight of controls is being developed.

Written policy Centralized deposits Internal controls self assessment PCI compliant

Accounting for monthly transactions occurs in a central department. Financial Reporting receives a download from the bank of all transactions and electronically posts to the general ledger. Departments are responsible for reconciling the monthly merchant

Cash management collects reconciliations for all credit card merchant accounts. Each department is responsible for the appropriate handling of credit cards.

Each department is responsible for reconciliation and compliance with internal control processes.

Daily settlement receipts from merchant terminals are processed same as cash & check. Majority are sent through two cashier locations that prepare and enter data for upload to ledgers. Bank reconciliation is monthly which includes bank data and ledger data

The cashiers book the entry either beforehand from the bank stats and match backup the next day or from the backup and match to the banking detail. Weekly recons are done on the Bank account setup for merchant processing. Appropriate handling is rev

Departments are required to allocate the appropriate funds to their account. At the end of the month, accounting makes sure everything is reconciled. If something is not right, accounting must do further research to get it balanced.

Reconciliation data is fed to our ERP system and compared against bank reports. Individual units are responsible for proper handling of daily batch reports and can pull reports from the ERP system for any further reconciliation

Written procedures and training provided to new merchants. Merchant deposits are centrally reconciled by treasury staff.

All credit card transactions are processed into the GL by our Treasury Workstation.

Cashier and accountant reconcile

Financial Management Operations centralizes the reconciliations of the credit card 'bank accounts' to ensure that what the department claims to have received is what truly has been received at the bank. The University has rules and regulations that dicta

Daily monitoring of merchant deposit at bank for collection report from department. Periodic review of processes.

We balance the Bank Statement each day with the paperwork each individual merchants presents.

Bank Account reconciled monthly in General Accounting; balanced daily by Manager, Cashier's Office.

We have a separate zero-balance account that we process credit card through. At the end of each day transactions from that account are deposited into our Concentration Account. This account is reconciled by employees from Treasury Management.

Reconciliation is done by General Accounting for campus wide accounts, by SFS Accounting for Internet and Main Cashier accounts (processes we own). We require a User's Agreement, a terminal PCI compliance and review of the UCLA User's Guide for Credit Car

All credit card deposits must be deposited with the Bursar's Office within 24 hours of receipt. Failure to do so will result in a policy compliance memo being sent to the depositor, his/her supervisor and Internal Audit. Unidentified credit card settlement.

We receive a raw data file from the bank and that is uploaded to our general ledger. We also have a service level agreement with each merchant outlining their duties and responsibilities for credit card handling.

Reconciliation handled by individual depts. Business manager or dept head required to sign Terms of Use agreement prior to opening the merchant account, this describes their responsibility for accounting controls and processing rules.

Departments are responsible for reconciling transactions and submitting entries to the Financial System. The Treasury Management Department reviews and posts all processing fees to department accounts (fees are passed through to department.)

Training provided by Treasury Operations to campus credit card merchants. Internal Audit recommendations. Segregation of duties: Departments record revenue to g/l and Accounting Dept reconciles g/l to bank Separate bank account for credit card se

All merchant accounts reconciled to bank statement centrally in Financial Reporting department. Financial Officers in units have oversight of cash handling for any departments in their areas using credit card processing.

reconcile receipts to merchant statements and general ledger activity

Reconciliation of bank accounts is done in a timely manner.

One office is responsible for reconciliation that is monitored monthly

A control account is established as part of the merchant application process. Credit card sales are recorded in our e-deposit system with two entries, a positive entry to the departmental revenue account, and a negative entry to the control account.

**Process/Operational – Fee Assessment**

**16. Merchant card processing fees (e.g. interchange per item and authorization fees) are:**

Charged to each merchant account by	16	29.63%
Charged to each merchant account by	28	51.85%
Funded centrally	4	7.41%
Majority funded centrally, ecom loc fund	1	1.85%
Other (please specify):	2	5.56%
Processor charges Treasury Ops	1	1.85%
Some are centrally funded, some are re-charged		
by University personnel	1	1.85%
Total:	53	

**17. How does your school fund overhead costs related to merchant card processing and compliance (salaries, infrastructure, compliance related fees such as scans, etc.)? Check all that apply.**

1% is charged to marginally fund	1	1.72%
Bursar	2	3.45%
Controller's Office	1	1.72%
Overhead costs are funded centrally	42	72.41%
Processor assesses a fee to departments and remits back to the university	2	3.45%
Student Financial Services	1	1.72%
Treasury	1	1.72%
University assesses a fee and credits a central fund	7	12.07%
Varies across campuses	1	1.72%
Total:	58	

**Compliance – Oversight**

***Leadership***

**18. What is the one department primarily responsible for overseeing achievement of PCI compliance? (CAUTION: Only use the text box if you choose 'Other' from the menu below.)**

Accounting/Controller	8	13.11%
Bursar/Cashier/Student Services	4	6.56%
Ecommerce	1	1.64%
Finance/Treasury	21	34.43%
Other	27	44.26%
Compliance Office	1	1.64%
Information Security	2	3.28%
Information Technology	3	4.92%
Joint Effort	1	1.64%
Joint effort - Controller, ITS, Compliance,	1	1.64%

None	5	8.20%
Other (please specify)	13	21.31%
To Be Determined	1	1.64%
Total:	61	

**19. Please indicate the Title of your PCI Compliance lead and outline the reporting structure for that function. (e.g. Compliance Officer > Controller > VP Finance > Executive VP > President)**

Accounting/Controller	6	15.79%
Bursar/Cashier/Student Services	2	5.26%
Ecommerce	3	7.89%
Finance/Treasury	20	52.63%
Other	7	18.42%
Director of Business Systems Analysis	1	2.63%
No formal structure	1	2.63%
Not applicable	1	2.63%
Program Lead --> Oversight Committee	1	2.63%
To Be Determined	2	5.26%
University Chief Security Officer	1	2.63%
Total:	38	

**Governance**

**20. Steering Committee (highest level of governance)**

We do not currently have a formal steering committee in place

---

Project owners 3 people vp it vp finance vp general council

---

Assistant Treasurer and Treasury Management Officer - 2 members. Information Security - 2 members.

---

Vice Chancellors (3)

---

5 members - Officers/VP's - Business Operations (1), Finance (1), General Counsel (1), Information Technology (1), Provost (1), meet quarterly.

---

Controller's Office (4), Internal Audit (2), General Counsel (1), Finance (2), Information Technology (2)

---

Vice Provost of Libraries, Computing and Technology (1) Asst VP/CFO/Controller (1)

This has not been established yet but will be shortly. Right now it is a team of audit, IS and Treasurer's Office and the executive management is aware of some of the issues.

Steering committee - 2 Members - VPs - VP Financial Services and Reporting (1), VP Finance and Administrative Services (1), meet monthly.

Director, Student Financial Services - 1 person, occasionally meet with Director, Administrative Information Services and Risk Management Director

None

## 21. Oversight Committee (intermediate level governance)

Our core team meets weekly and drives the project. 7 members from general council, IT, finance, audit and information security

IT Directors Council (5)

Internal Audit

Controller and Director of Disbursement Services

6 members - Directors, AVP's - Business Operations (1), Cash Manager (1), Controller (1), General Counsel (1), Information Security (1), meet twice a month.

Controller's Office (1), Internal Audit (1), Information Security (1), General Counsel (1)

Oversite committee - 2 members - Asst. Controller Financial Services (1), Asst Coordinator Payroll/Travel (1), meet bi-weekly.

CyberPay Support Team - 5 members - Manager, Supervisor, three AA III, meet as needed. Terminal Support Team - 4 members - Manager, two Accountants, 1 AA III, meet as needed.

Compliance Office - office responsible for overseeing and coordinating all compliance issues.

Treasury Operations

None

## 22. Working Group (program leadership and individual contributors)

Manager of Cash Receipts & Disbursements, Bursar, & Controller

Members of schools and centers that own merchant accounts. 30 members. meets monthly. Responsible for self assessment

IT, Treasury, Finance

Treasury (1)

Controller's Office, Office of Information Technology

PCIDSS Compliance Officer and Business Analyst/External Sales

3 members - Information Security (1), Controller's Group (1), e-Commerce service (1)

PCI Committee, 10 members, Controllers Office(4), ITS Security(1), ITS(5)

Meet weekly

Internal Audit (1), Information Security (1), Controller's Office (2)

1 from Controller's Office 4 from Administrative Information Services (IT) 2 from Network Security 1 from Internal Audit Meet weekly

Working Group - 2-3 members - Asst Coordinator Payroll/Travel (1), accepting departments (1-2), meet when needed.

---

Treasury Officer Department liaison (technical staff)

---

In process - trying to get about 5 members from Risk and Compliance, Computing and Information Services, Financial Management Operations, and System Treasury Operations

---

One internal auditor working with Cash Manager to create

---

Manager, Accounting Info Services - Lead Director - Computing and Info Services Assistant Controller - University Financial Services

---

Senior Associate Controller Assistant Controller (2 of these) Coordinator of Computer Services University Web Administrator

---

Treasurer's Office (3); Information Technology Security Services (1); Information Technology Central Services (3)

---

Director of Treasury Management is primarily responsible for PCI Compliance. Works with Compliance Office.

---

VISA CISP Working Group - meet monthly - 12 members Controller's Office (2), Privacy Office (1), Internal Audit (1), eCommerce Services (1), Security Office (1), Info Tech Services (3), Merchant Representatives (4)

---

None

**23. Do you have written policies on PCI Compliance?**

In Process	22	46.81%
No	13	27.66%
Yes	12	25.53%

Total: 47

**24. Do you have each department processing credit cards sign a contract outlining their responsibilities in regard to PCI compliance?**

No	34	75.56%
Yes	11	24.44%

Total: 45

*Staffing*

**25. How many FTE's does your school have staff dedicated to PCI Compliance?**

>4	2	4.76%
0	19	45.24%
0.5	4	9.52%
1	6	14.29%
1.5	4	9.52%
2	3	7.14%
2.5	3	7.14%
3.5	1	2.38%
Total:	42	

**26. To what area(s) do these personnel report? (e.g. Information Security Central E-commerce Service, Controller, Treasury, etc.)**

Accounting/Controller	8	24.24%
Bursar/Cashier/Student Services	3	9.09%
Ecommerce/IT	2	6.06%
Finance/Treasury	13	39.39%
Other	7	21.21%
Info security-Provost Treasury & Controller CFO	1	3.03%
Information Security, Treasurer	2	6.06%
Internal Audit Treasury	1	3.03%
N/A	3	9.09%
Total:	33	

**27. Do they have other responsibilities (e.g. Accounting, Treasury, Audit, etc)? If so please list.**

Yes

---

Cash Management

---

None of the people currently working on the PCI compliance issue are dedicated to only that--we all have full time duties in our positions---everyone who is working on PCI compliance is currently doing that on top of their regular duties--we are working w

---

Treasury

---

Accounting Audit

---

N/A

---

Audit has additional technology audit duties, InfoSec resources include: Program InfoSec Lead (.5 PCI, .5 other initiatives); infosec analyst (1) = fully dedicated; .5 IDS analyst (.5 PCI, .5 other IDS duties)

---

Business Analyst

---

Ongoing eCommerce

---

University Security Officer - IT All aspects of e-commerce - TCM

---

1 from Controller's Office 4 from Administrative Information Services (IT) 2 from Network Security 1 from Internal Audit

---

Treasury. Yes, Cash Operations for University. Some risk management as it relates to Treasury, cashflow forecast, etc.

---

Payroll, Travel, Credit Card Services

---

E-Commerce

---

Treasury responsibilities

---

Accounting - PCI has been another project added to this area in addition to their regular responsibilities

---

internal audit, treasury

---

yes, LAN Support Specialist

---

Accounting

---

Accounting and reconciliation, Armored courier scheduling and credit card oversight, Customer Service and Support, Internet merchant assistance

---

Accounting, Banking

---

Yes, E-Commerce, IT Security

---

PCI DSS and credit card acceptance program historically has been a minor additional duty for the Bursar and Assistant Treasurer. A reorganization in 2003 expanded the Assistant Treasurer's responsibilities (and renamed the position to Director

---

Management of University ID Card Services.

**PCI Compliance – Technical**

**28. Who conducts compliance testing? Please specify internal vendor name or none. Please provide cost estimates/ranges if available.**

External	37	36.27%
In Process	10	9.80%
Internal	36	35.29%
None	19	18.63%
Total:	102	

**PCI Compliance – Monitoring**

**29. Once compliance is achieved what is the one department primarily responsible for overseeing and monitoring ongoing PCI compliance?**

Accounting/Controller	7	15.56%
Bursar/Cashier/Student Services	4	8.89%
Ecommerce	1	2.22%
Finance/Treasury	18	40.00%
Other	15	33.33%
Audit	1	2.22%
Information Security	3	6.67%
Information Technology	1	2.22%
None	2	4.44%
Other	8	17.78%
Total:	45	

**30. How do you detect unauthorized merchant accounts or payment services? Specifically who is responsible and how is the issue detected?**

Accounting/Controller	8	10.26%
Bursar/Cashier/Student Services	7	8.97%
Finance/Treasury	37	47.44%
Other	26	33.33%
Audit Department	1	1.28%
Auditing accounts	1	1.28%
By accident	1	1.28%
Central authorization for new accounts;	1	1.28%
Chargeback	1	1.28%
Contacting merchant processor	1	1.28%
Director	2	2.56%
Exceptions to the monthly processing	1	1.28%
Google	1	1.28%
Inquiry to banks, bank reconciliation	1	1.28%
Looking at revenue, looking at websites.	1	1.28%
Manager	1	1.28%
None	2	2.56%
PCIDSS Compliance Officer/OIT Security	1	1.28%
Reporting from other departments	1	1.28%
Reports from financial institutions	2	2.56%
Request report on new merchant	1	1.28%
School Web Sites, IT, Registration Forms	1	1.28%
Semi annual online search	1	1.28%
Sr. Auditor	1	1.28%
Survey of local banks	1	1.28%
Varies by Campus	1	1.28%
Vendor notification	1	1.28%
Total:	78	

### 31. What steps are taken when an unauthorized merchant account or credit card activity is identified?

1. Contact with department using the unauthorized account. 2. Termination of unauthorized merchant number and associated bank account 3. Allow department to conduct credit card transactions through the University's approved card processors.

Work on a policy not adhering - leads to termination

We are creating a new policy that stipulates that unauthorized credit card/e-commerce acceptance will not be tolerated. Departments will be required to use the one University designated payment gateway for all their internet processing.

Appropriate campus officials contacted to put immediate stop to all unauthorized activity; new account set up under University umbrella

1. Contact Controller 2. Contact Internal Audit 3. Contact credit card provider (if applicable) 4. Contact department

OIT Security contacts account holder to shut down payment service. They can shut down IP address if non-compliant.

Account is closed and, possibly, moved to approved merchant bank.

Contact department Obtain explanation Correct situation

Financial Reporting notifies the Cash Manager who contacts the bank

If it is a new bank account, we close the bank account. If it is an unauthorized merchant account with our bank, we contact the department to determine what has happened and inform the bank to only set up merchant accounts through our central process.

Account is shut down but can be reopened under the university merchant chain.

Unauthorized credit card activity is brought to attention of Asst Treasurer who forwards to security and/or bank for assistance in next steps

Research their method to find out the process and if they are compliant with regulations. If they are not, initiate a plan to make them compliant.

Account is deactivated and unit is set up with an account through Treasury Operations

Merchant must be able to justify credit card acceptance. Must provide specific statute that permits collection of revenue.

The departmental merchant account and Treasury work with the credit card process to reconcile.

N/A

We would work through our Card Processor for guidance.

Director of SFS meets with merchant to discuss, evaluates compliance needs and outstanding issues. Merchant is either terminated, compliance proven, or variances are obtained from Director SFS and UCOP for continuing process.

Notify Associate VP for Finance

University department responsible for this merchant account would be notified and account would be closed immediately.

We either shut them down or have them convert to authorized use

Given the non-existence of a formal detection/monitoring program, any discovery of an unauthorized merchant account or credit card activity would be by sheer luck. Should an event be identified the Director of Treasury Management would most likely be res

---

No unauthorized activity has been identified; however, if we discover a rogue merchant, we would close the account and open a new merchant account under the central supervision of Treasury Operations.

---

All unusual activity is reviewed

**PCI Compliance – Incident Response**

**32. Do you currently have an incident response policy?**

In Process	12	27.27%
No	20	45.45%
Yes	12	27.27%
Total:	44	

**33. Have you had a security incident involving cardholder data?**

No	35	81.40%
Yes, and we may be fined	1	2.33%
Yes, and we were not fined	4	9.30%
Yes, and we were/are being fined	3	6.98%
Total:	43	

**34. If your institution were to be fined how would the fine be assessed?**

Charge the merchant account(s) or departments involved	15	34.09%
Don't know at this time	27	61.36%
Payment with central funds	2	4.55%
Total:	44	

**35. How do you communicate with the card associations (VISA, MC, etc.)?**

Directly	3	7.14%
No communication	8	19.05%
Through our merchant bank	31	73.81%
Total:	42	

**36. Who within your organization is responsible for incident response roles listed below?**

Accounting/Controller	2	3.03%
Bursar/Cashier/Student Services	3	4.55%
Ecommerce/IT	30	45.45%
Finance/Treasury	13	19.70%
NA	1	1.52%
Other	17	25.76%
Asst VC for Business Services	1	1.52%
Audit Department	1	1.52%
General Counsel	1	1.52%
N/A	12	18.24%
Unknown	2	3.03%
Total:	66	