
PROPOSED AUDIT PLAN CHANGE

TO: KEVIN TWOMEY, TOM SERWATKA
FROM: ROBERT BERRY
SUBJECT: PROPOSED AUDIT PLAN CHANGE REVISED
DATE: DECEMBER 6, 2007
CC: SHARI SHUMAN, JOHN DELANEY

INTRODUCTION

It is The Office of Internal Auditing's (OIA) responsibility to review process, policies and procedures based on the potential risk to university assets. In doing this, we must continuously reevaluate our audit plan to ensure we address relevant areas. As a result, we propose the following adjustments to our audit schedule:

Remove	Purchasing Card (P-Card) Process Audit
Replace With	Management Advisory Service – Assist Management with Payment Card Industry Data Security Standards (PCI – DSS) Review
Rationale	The Auditor General recently completed a review of the UNF PCard process. Performing another review of this area does not constitute the best use of university resources. Management is currently considering contracting with a third party to perform a PCI – DSS assessment. As a service to management, the OIA is suggesting our inclusion in the process as an advisory function.

BACKGROUND

The Payment Card Industry (PCI) Security Standards Council was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International. The Council's mission is to enhance payment account data security wherever it resides (i.e. databases, hardcopy, electronic transmission, etc) by fostering broad adoption of the PCI Data Security Standards (DSS).

The PCI DSS is made up of a set of twelve general compliance requirements organized around six primary goals that add up to a comprehensive information security program, centered around technology and operational practices, for protecting credit card numbers and other sensitive cardholder data from loss or compromise.

WHO MUST COMPLY

All merchants and service providers who store, process, or transmit credit card account numbers must comply with the standards. Additionally, the program applies to all payment channels, including card present, mail/telephone orders, and e-commerce transactions.

HOW TO COMPLY

The most comprehensive requirements (Visa and MasterCard) include three levels of validation including:

- an on-site security audit,
- a self-assessment questionnaire and
- a network scan.

The level of validation required and the frequency of validation efforts depend upon the rating assigned to the merchant or service provider under PCI Ratings (see below)

Merchant Level & Description		Validation Actions			Enforcement Dates
		On Site Audit	Self Assessment Questionnaire	Network Scan	
1	Any merchant processing over 6 million transactions per year.	Required Annually		Required Quarterly	9.30.2007
2	Any merchant processing 1 to 6 million transactions per year.		Required Annually	Required Quarterly	9.30.2007
3	Any merchant processing 20,000 to 1 million e-commerce transactions per year.		Required Annually	Required Quarterly	?
4	Any merchant less than 20,000 e-commerce transactions per year and all other merchants processing up 1 million transactions per year.		Required Annually	Required Quarterly	7.30.2007

FINES & PENALTIES

There are potential fines and penalties for non-compliance ranging from the following:

- Up to \$100,000 per month a merchant is not compliant
- Fines up to \$500,000 per incident of data compromise
- Possible refusal to process credit card transactions

To illustrate the point, on December 3rd TJ Maxx agreed to pay VISA \$40.9 million as a result of a data breach in January 2007. Additional settlements are anticipated with the other major credit card processors.

BREACH NOTIFICATION

Most credit card processors require merchants to provide notification of security breaches. For example, Visa members who fail to "immediately notify" Visa of a suspected or known loss or theft of transaction data may be fined \$100,000 per incident, plus extra fines if a PCI violation presents "immediate and substantial risks" to Visa and its members.