Mission Statement
The Payment Card Industry Team PCIT serves as a formal advisory group to the Vice President for Finance and Administration and Chief Financial Officer (VPFA/CFO). VPFA/CFO has authority to make decisions regarding the program. The PCI program coordinator will report university compliance status and remediation recommendations annually to VPFA/CFO and to the Strategic Enterprise Risk Management and Compliance (SERMC) committee.

The mission of the PCIT is to reduce the risk of card data breach and maintain compliance with Payment Card Industry data security standards.

To fulfill this mission the PCIT will maintain UO Payment Card Acceptance Policy and Procedures, oversee an annual PCI risk assessment process, engage a Qualified Security Assessor (QSA), partner with campus merchants, and business, IT, and procurement professionals, and oversee the activities of the PCI program coordinator.

Responsibilities of the team
- Meet semi-annually;
- Review and update the UO Payment Card Acceptance Policy as needed;
- Review the annual report prepared by the program coordinator revealing the compliance status of campus merchants and remediation plans for areas of non compliance;
- A subcommittee of PCIT will validate a sample of merchant attestations
- Monitor new merchant activity, the scope of the card data environment, payment card processes, and vendor relationships (service providers and QSA).
- Prioritize identified risks, perform cost benefit analysis, and recommend remediation options.
- Oversee the campus PCI compliance training program
- Plan and prioritize risk reduction and compliance remediation activities;
- Identify resources for PCI compliance initiatives.
- Provide PCI assessment for cyber insurance

Membership
The PCIT includes senior leadership representatives from units across the university with expertise in PCI compliance, information technology, information security, risk assessment, business, and card operations.

Program Coordinator and Team Lead:
Director, BAO Information Systems

Members
Chief Information Security Officer, Information Services
Chief Auditor, Internal Audit
Chief Procurement Officer, Purchasing and Contracting
Alignment and connection to other campus teams
The PCIT is connected to other important response and prevention teams on campus through liaison connections and joint membership. These teams include but are not limited to the following:

- The Strategic Enterprise Risk Management and Compliance (SERMC) committee use two approaches to address current or emerging risks that do not have a clearly defined university risk owner.
  - Standing committees and teams to monitor, mitigate, and respond to risk and vulnerabilities, and
  - Workgroups with specially charged workgroups

The PCI program coordinator will present the campus report on compliance annually to SERMC each spring.

- UO Incident Management Team (IMT) – Provides the command and control infrastructure that is required to manage the logistical, fiscal, planning, operation, safety and campus issues related to any and all incidents/emergencies.

- Campus Vulnerability Assessment Team (CVAT) – A collaborative interdisciplinary effort that conducts site specific assessments to identify the vulnerability of people, property, operations and environment.

- Data Security Incident Response Team (DSIRT) – Responsible for reducing the risk associated with data security issues and overseeing the response to data security incidents.

- Information Security and Policy Governance Committee (ISP GC) – Represents subsets of business, research, and teaching technologies, takes recommendations and advice from service advisory boards, and addresses questions about security and information assurance. The UO Chief Information Security Officer is a member of the PCIT providing linkage to the ISP GC.