The following is an example of a completed assessment survey, from OIRT:

Gramm Leach Bliley Security Program

Office of Information Resources Technology

Standards for Safeguarding Customer Information

(a) Designate an employee or employees to assist the CIO in the coordination of the Program.

In addition to the CISO, the Director of Systems and the Director of Networking are the designated employees for the Office of Information Resources Technology

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

- Unauthorized disclosure of sensitive information by employees through intentional or unintentional methods.
- Unauthorized access, disclosure, misuse, alteration or destruction of information on hosts.
- Detection and prevention of attacks on the systems.
- Unsecured transmission of data.
- Physical security of computer systems, network equipment, backups and paper materials.
- Managing data integrity and system failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

1) Unauthorized disclosure of sensitive information by employees through intentional or unintentional methods:

   - Employees go through mandatory Written Information Security Program (WISP) Training
   - Prior to any IT requests, User Information Is checked against WISP to ensure they are current with training
   - Employees are provided training and are closely observed by managers before being given access to sensitive information. Training includes password policy and management, physical security of

cabinets, storage, and equipment rooms, and recognizing fraudulent attempts to obtain sensitive information.

    - Policy, social engineering, keystrokes loggers, etc.

- All employees must sign and accept the University's "Acceptable Use Policy" and the "Confidentiality Agreement" if applicable.
- Requests for sensitive information are directed to individuals with proper training and authority to review the request.
- Potential employees are subjected to a background check before being hired by the University.
- Updated IT Informational website that includes documentation of all policies and procedures specific to securing data.
- Use of Data Loss Prevention tool to proactively monitor and correct non-compliance issues
- Access to information is granted only to the extent required for the employee to perform their job functions.

2) Unauthorized access, disclosure, misuse, alteration or destruction of information on hosts:

- Passwords are required for access to any system with sensitive information.
- Strong password policies are in place where possible.
- Multi-factor authentication to access sensitive systems for all faculty, adjuncts, staff and students.
- Multi-factor authentication for all admin accounts.
- Auditing systems (e.g. Change Management Process, Netwrix, Microsoft ATP) are used to track and report on changes to critical files.
- Notifications of employee terminations are received prior to or on date of termination. Immediate notification is received when circumstances warrant instant suspension of access to systems.

3) Detection and prevention of attacks on the systems:

- Auditing systems (e.g., Netwrix) are used to detect attempts to breach systems or alter system configurations.
- System logs are reviewed daily for evidence of attacks.
- Policies are in place to regularly apply patches to systems.
- A firewall is in place for perimeter protection.
- Obsolete systems are being replaced by newer systems that are better supported by hardware and software vendors. Most systems include host-based firewalls.
- The wired portion of the university network is entirely switched to minimize the possibility of packet sniffing and other similar attacks.
- WPA2 Enterprise is deployed and available for wireless accessible locations.
- Endpoint protection software is in place, which automatically updates servers & clients.

4) Unsecured transmission of data:

- Connections to all systems are using modern cryptographic techniques.
- University standard practice is to use HTTPS for web services; all publicly accessible web traffic is proxied through load balancers.
- SFTP is used to transmit data to various vendors securely.
- EFax services deployed, ensuring fax transmissions are encrypted both in transit and at rest.
- Virtru software for encrypted email communication of sensitive and Personally Identifiable Information
- 7-Zip is used to encrypt files being sent to and from vendors.

5) Physical security of computer systems, network equipment, backups and paper materials:

- All computer systems and core network equipment are physically secured in locked rooms or cabinets.
- Essential services are monitored for availability and alerts are sent when a system or service becomes unavailable.
- Printed material with personal information is shredded when no longer needed.
- The main data centers and several ancillary MDF's have heat and humidity detection systems as well as a fire suppression system.
- Alarms with motion detectors are in place in all data centers. The university department of Public Safety monitors the alarms.
- Security cameras are set and on 24-hour recording on both main data centers
- A card access system controls access to the data centers and IT administrative offices.

6) Managing data integrity and system failures:

- Daily backups of host systems are performed.
- Network hardware configurations are backed up weekly.
- Out of band capabilities exist to support network management and large-scale outages.
- Continual off-site backup of all FDU-owned workstations.
- Mirroring of networked file services across campuses is occurring.
- UPS systems provide backup power to central data centers.
- Extending backup capabilities to include off-site backup of all University systems
- A backup generator is in place for the main data centers.
- A disaster recovery plan has been developed.

(d) Oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring FDU's service providers by contract to implement and maintain such safeguards.

Contracts require appropriate safeguarding measures be taken by the vendor. Third-Party Assessment evaluation using Industry best practice tools prior to executing contracts.

(e) Evaluate and adjust FDU's information security program in light of the results of the testing and monitoring required by this Policy; any material changes to FDU's operations or business arrangements; or any other circumstances that are known or have reason to be known as having a material impact on FDU's information security program.

OIRT continually performs extensive reviews of applicable written policies and has a continuous program in place to review applicable policies and procedures.

OIRT periodically (generally annually) performs an email Phishing test to all full-time faculty and staff. FDU uses a third party as the tool for performing the test. Individuals who fail the Phishing test are required to complete remedial training with a passing score. Supervisors are made aware of those who fail the test and are encouraged to speak with their employees.

OIRT conducts comprehensive vulnerability assessments aligned to the NIST Risk Management Framework (RMF) that included external vulnerability scanning, penetration testing, netflow analysis of our IP ranges, review of IT and cybersecurity-specific and FDU-wide documentation, and dark web footprinting.

OIRT takes action to increase the cadence of monitoring and reacting to server, desktop and mobile device alerts, ensure compliance of website configurations and deploy security measures to ensure security of email system and reduce spoofing of emails.