Information Owner Training

IT Shared Services

Training@security.untsystem.edu

Why me?

The Texas Administrative Code 202 requires the institution to identify information owners and document their responsibilities.

Your position was identified as an information owner

Additional Information for Information Owners can be found:

- All information in this presentation can also be found in more detail in the Information Ownership Guide

- Additional resources are located on the Information Owners Website

Information owners can help prevent data loss

Data breaches at UNT would most likely occur through inadvertent exposure.

Georgia Tech exposed 1.3 million identities in 2019

In 2017, a permission error exposed the information of 10,000 Stanford University employees

Oregon State University potentially exposed student and family records by a phishing attack in 2019

Security Roles

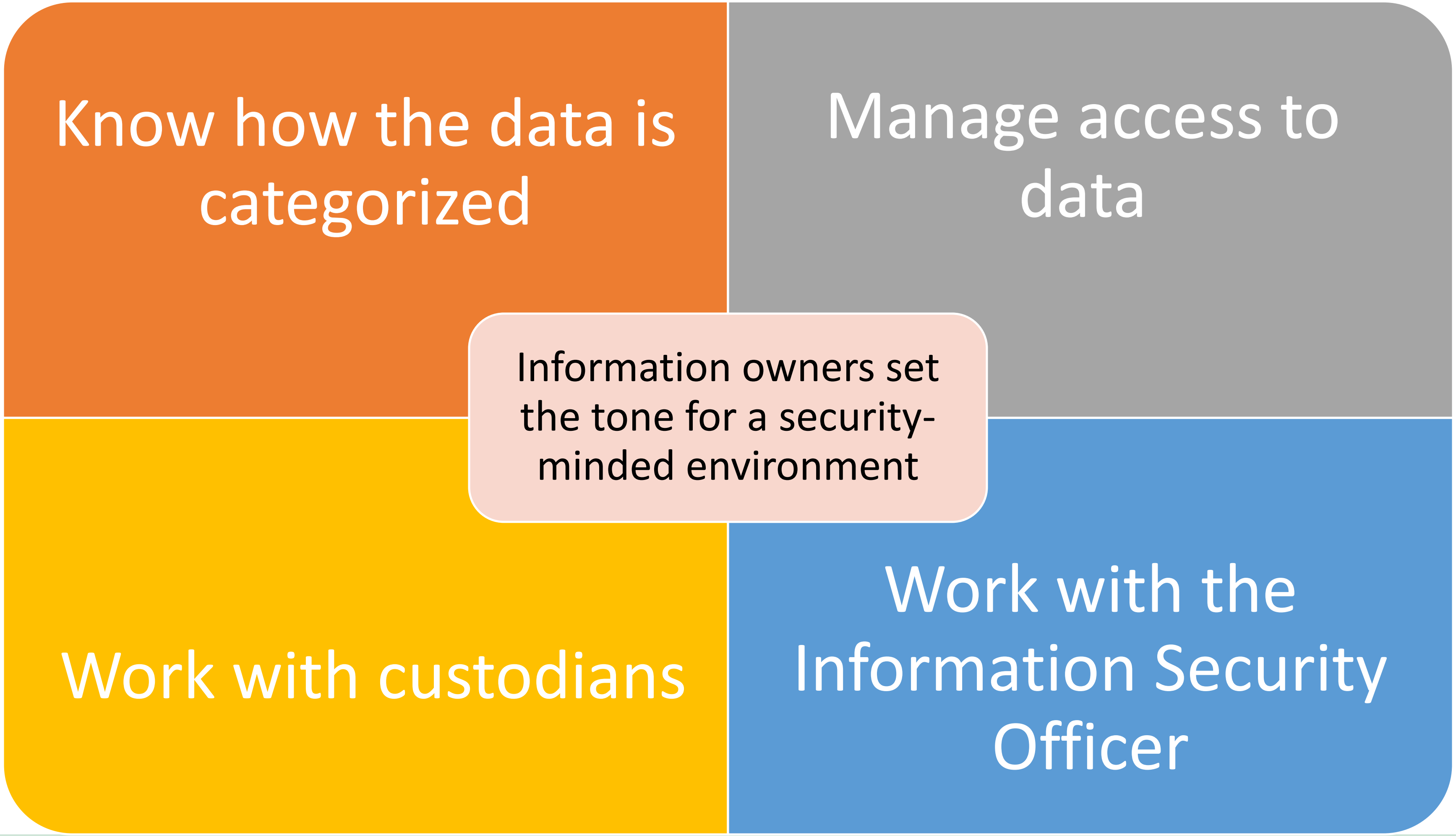
Information Owners - are individuals with operational authority for specified information and who are responsible for authorizing the controls for the generation, collection, processing, access, dissemination, and disposal of that information

Custodians – are responsible for the operation of an information resource. Individuals who obtain, access, or use information provided by information owners for performing tasks also act as custodians of the information and are responsible for maintaining the security of the information.

Users - are an individual or automated application authorized to access an information resource in accordance with the information owner-defined controls and access rules.

Information Security Officer - provides guidance and assistance to information owners and others concerning security roles and responsibilities. The Information Security Officer is appointed by the head of each institution and is responsible for developing and administering the operation of an information security program.

Information Owners’ Areas of Responsibility



Know how the data is categorized

Manage access to data

Information owners set the tone for a security-minded environment

Work with custodians

Work with the Information Security Officer

Responsibility 1:

Know How Data is Categorized

Categories of Information

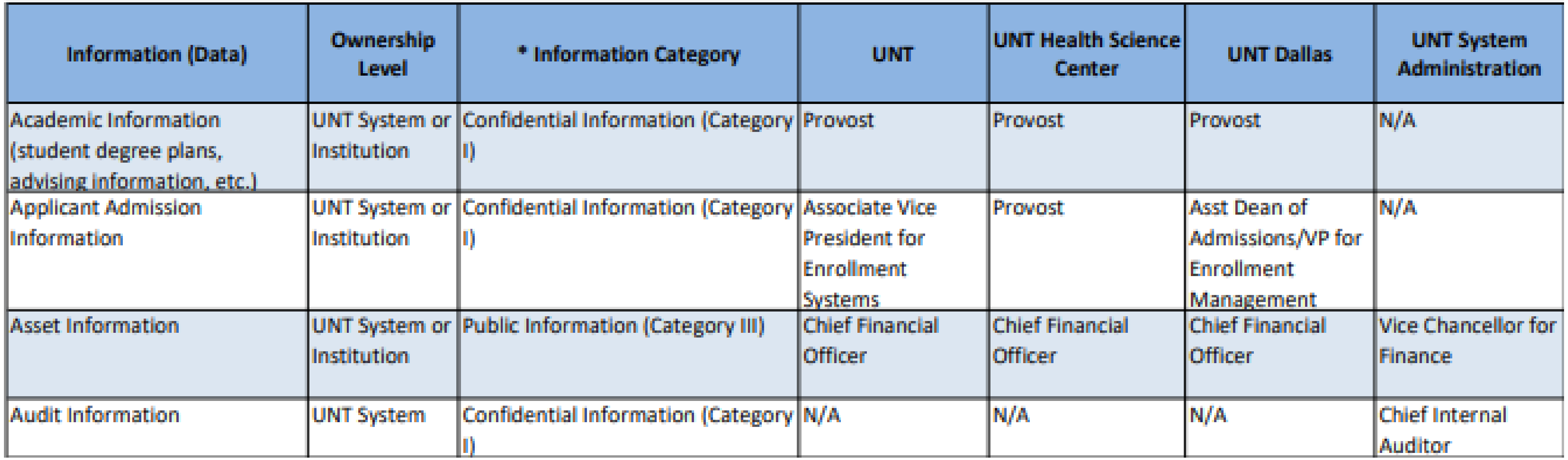
Category I: Confidential – Protected information: E.g. financial aid, health and medical information, social security numbers, computer account information.

Category II: Proprietary – Should be controlled before release: E.g. grant, donor, and patron information, some payroll information

Category III: Public – Public information available for release.

Categories of Information

- All information has been categorized.
- Categorization and ownership documentation is posted on the UNT System Information Ownership website.



Information (Data)	Ownership Level	* Information Category	UNT	UNT Health Science Center	UNT Dallas	UNT System Administration
Academic Information (student degree plans, advising information, etc.)	UNT System or Institution	Confidential Information (Category I)	Provost	Provost	Provost	N/A
Applicant Admission Information	UNT System or Institution	Confidential Information (Category I)	Associate Vice President for Enrollment Systems	Provost	Asst Dean of Admissions/VP for Enrollment Management	N/A
Asset Information	UNT System or Institution	Public Information (Category III)	Chief Financial Officer	Chief Financial Officer	Chief Financial Officer	Vice Chancellor for Finance
Audit Information	UNT System	Confidential Information (Category I)	N/A	N/A	N/A	Chief Internal Auditor

Chart is sample data only

Responsibility 2:

Manage Access to Data

Manage Access to Data

Grant approval authority to individuals designated to act on your behalf (e.g. ACEs)

Document your approval and the type of access granted to designated representative(s) and other individuals that you authorize to use information.

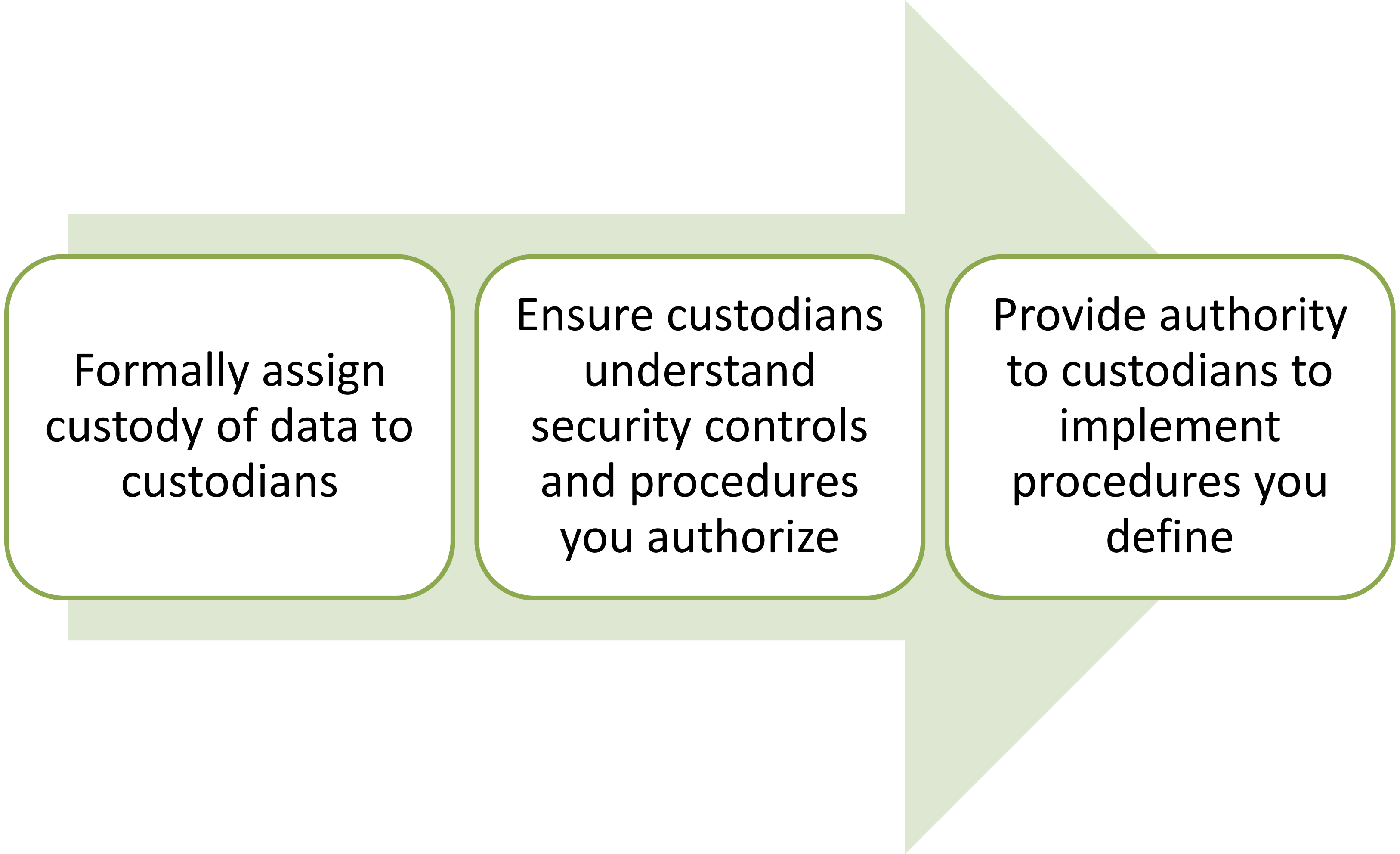
Review and revise access lists periodically

- *Reviews should be conducted at least annually*
- *Reviews should occur more frequently depending on the importance of the data*
- *Reviews should consider changes in employment*

Responsibility 3:

Work With Custodians

Work with Custodians

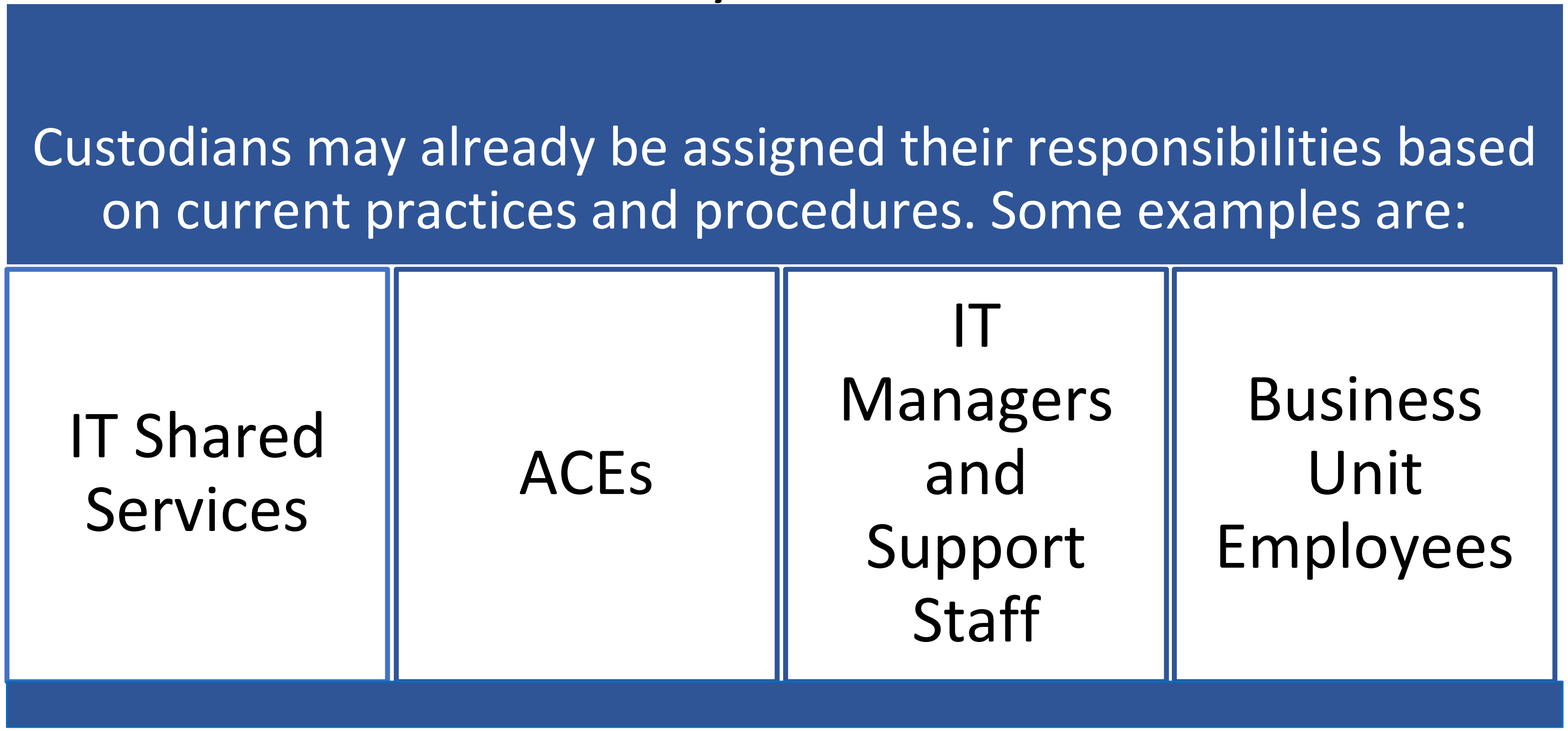


Formally assign custody of data to custodians

Ensure custodians understand security controls and procedures you authorize

Provide authority to custodians to implement procedures you define

Work with Custodians-Formally Assign Custody of Data



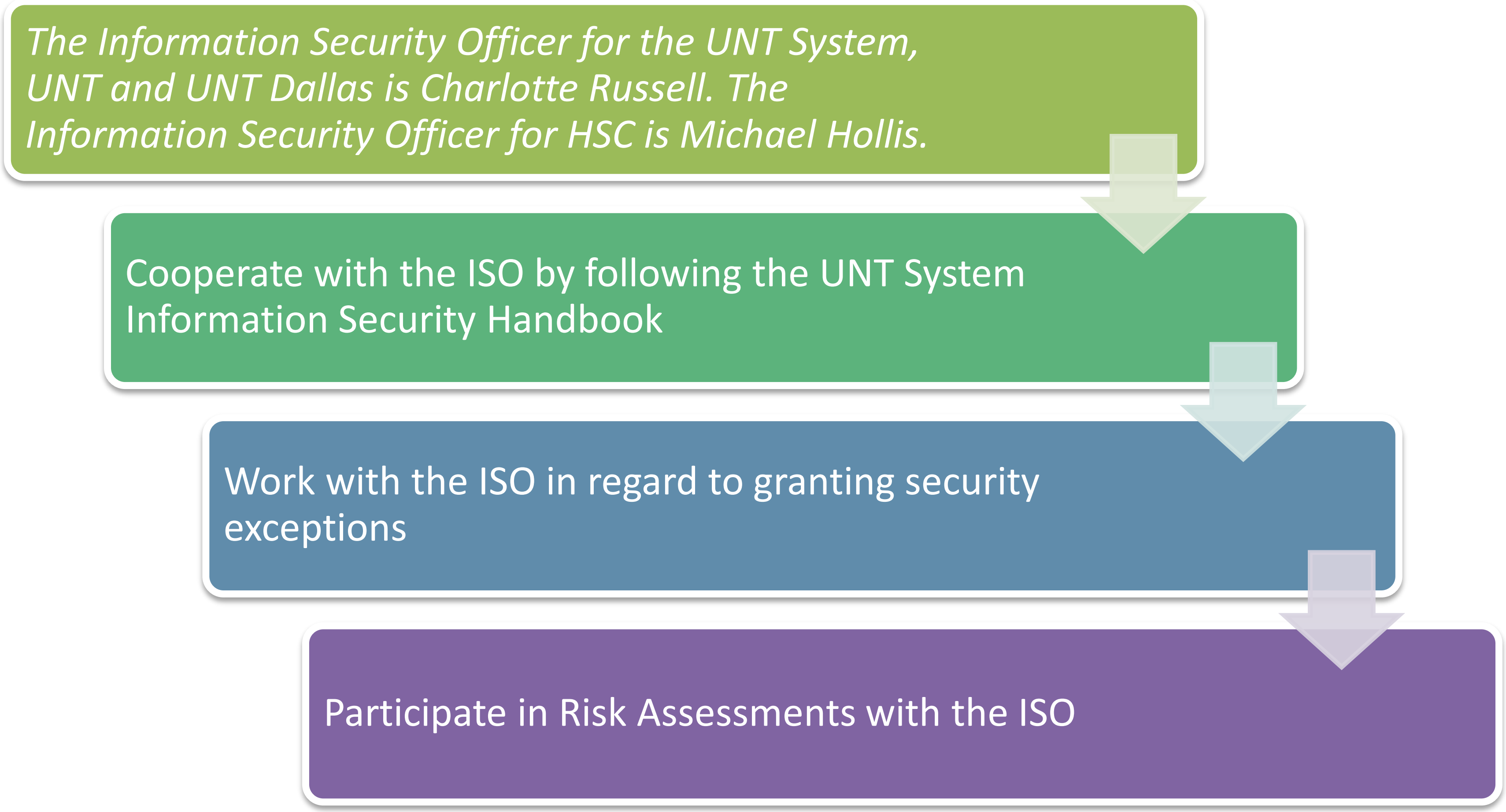
Custodians may already be assigned their responsibilities based on current practices and procedures. Some examples are:

- IT Shared Services
- ACEs
- IT Managers and Support Staff
- Business Unit Employees

Responsibility 4:

Partner with the Information Security Officer

Work with the Information Security Officer (ISO)



The Information Security Officer for the UNT System, UNT and UNT Dallas is Charlotte Russell. The Information Security Officer for HSC is Michael Hollis.

Cooperate with the ISO by following the UNT System Information Security Handbook

Work with the ISO in regard to granting security exceptions

Participate in Risk Assessments with the ISO

What do I need to do?

- ✓Read the Information Ownership Guide
- ✓Read the UNT System Information Security Handbook
- ✓Establish procedures for documenting and reviewing custodianship
- ✓Work with the Information Security Officer to complete risk assessments and when requesting security exceptions
- ✓Ensure data security requirements are met through people, processes, and technology
- ✓Convey that security is everyone’s job

Resources

- UNT System Information Ownership Guide
- UNT System Information Ownership Website
- UNT System Information Security Handbook
- UNT System Information Security Regulation
- Texas Administrative Code, Section 202

For additional assistance, e-mail:

training@security.untsystem.edu