For purposes of this reporting period, the following key compliance risk areas will be assessed.

Compliance Risk Areas	Related Governing Laws, Rules, Regulations, or University Policies
Using IT resources as authorized Protecting University-assigned accounts and authentication Abiding by security controls Downloading or installing software that interferes/disrupts service or does not have a clear business/academic use Inappropriate use: actions that violate state of federal laws, regulations or polices; harassment; dissemination of unsolicited and unauthorized electronic communications Excessive use of system information technology (i.e. Network capacity)	BOR Code of Conduct BOR Acceptable Use of Information Technology Resources Policy Internal Access to and Sharing University Information

Cost of Compliance Measurement Questions

1. How many full-time employees (FTEs) are dedicated to compliance-related activities in this area?

2. What is spent annually, on average, to perform the compliance-related activities conducted by this unit? Please include only those items that require the purchase or goods or services from an outside entity such as outside consulting services, equipment purchases, non-routine supplies, or fees.

3. Please list all training required to maintain University compliance in this subject area.

4. For each training requirement:
    a. Identify category (ies) of employees (e.g., faculty, P&A, etc.) required to take the training.

    b. Estimate the number of employees in each category required to take the training.

    c. Identify the frequency (e.g., quarterly, annually) and the length of the training (e.g., 1.5 hours).

    d. Estimate the number of employees system-wide who are subject to the compliance requirements in this area.

5. Excluding time required to meet training requirements addressed in Question 3 above, please estimate the time required annually for these employees to comply with other compliance requirements (e.g., record keeping, monitoring, testing, reporting).

General compliance question(s)

1. How is compliance with the policy monitored?
2. What is the frequency of the monitoring?
3. What are the typical noncompliance issues found and how are they corrected?
4. Are there any recent (within 3 years) internal audit and/or external audit findings? If yes, how were the findings addressed?
5. Provide an overview (purpose, operations, incident management process) of the incident management system at the University. And, share reports from the last two years that summarize the number and findings of Reportable Acceptable Use Violations to include: Inappropriate Disclosure, Unauthorized Access, Malicious Code, and Copyright and Licensing Violation.
6. How (and by whom) are information security threats and weaknesses assessed and mitigated?

Ensuring Appropriate Use of Information Security Assets

1. What assurance exists that users are protecting their university assigned accounts and authentications? What actions (communication, training) are taken for this assurance?
2. How are security controls identified, managed and updated/maintained in order to protect information technology resources and data?
    a. How are those controls communicated and managed?
3. What controls have been put in place to protect IS assets, for employees working remotely?
4. What vulnerabilities exist related to employees using their own devices for university-related work? How are those managed?
5. Are there any risks that you'd like to add to this Compliance Risk Review? If so, please include those here.