TEXAS HIGHER EDUCATION
COORDINATING BOARD
P. O. Box 12788 Austin, Texas 78711

February 1, 2021

Dr. Harrison Keller
Commissioner of Higher Education
1200 E. Anderson Lane
Austin, TX 78752

Dear Dr. Keller,

The July 2020 status report provided by management to the Agency Operations Committee was accurate regarding actions taken to implement the recommendations in the NTT Texas Cyber Security Assessment Report at the Texas Higher Education Coordinating Board, issued June 2017, and AT&T Texas Cyber Security Assessment Report at the Texas Higher Education Coordinating Board, issued August 2019. (see Appendix 1).

Both reports included a security program maturity assessment following control objectives based on the Texas Cybersecurity Framework (TCF) and the DIR (Department of Information Resources) Security Control Standards Catalog.

Our review focused on:

1. assessing the accuracy of management's most recent report of corrective action status, dated August 2020.
2. consideration of actions taken between our first assessment conducted in Fiscal Year 2018, and our second assessment for Fiscal Year 2020.
3. assessing compliance with select provisions of agency information security policy, such as, implementing data classification, integrating data classification with data loss prevention (DLP), and establishing a program to monitor security control compliance by external service providers on an ongoing basis.

Our status assessment provides an outside evaluation of the agency's information security program as required on a biennial basis by Texas Administrative Code Chapter 202 Information Security. We reviewed both NTT and AT&T assessments and obtained a status update with relevant documentation to determine the implementation status.

We conducted this review in conformance with the *International Standards for the Professional Practice of Internal Auditing.* Additionally, we conducted this review in accordance with *Generally Accepted Government Auditing Standards*. Those standards require that we plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives. We further acknowledge that, as internal auditors, we are independent according to the requirements specified in Government Auditing Standards. Our consideration of internal control was for the compliance purposes described in the objective/scope section and was not designed to identify all deficiencies in internal control.

The NTT and AT&T assessments provided 73 recommendations divided into five categories. The most significant recommendations related to areas where the "**maturity**" of a scored element was at level two, on a scale of zero to level five. NTT initially scored 34 of 73 of its recommendations as level two maturity. Later assessment by AT&T resulted as level three maturity to all 73 recommendations. Maturity levels zero to five are defined in Appendix 2.

Details	# of Recommendations
Recommendations Reported by NTT Data at Level 2	34
Areas Remaining at Level 2, Verified by Internal Audit	0
Recommendations Reported by AT&T Data at Level 2	0
Recommendations Reported by AT&T Data at Level 3	73

Status of Recommendations	# of Recommendations	Management's Comment
Completed	31	On Going Monitoring
In Progress	42	Future actions pending upon availability of resources.

To comply with security policy as identified in DIR security control standards, ISS:

- Implemented the processes for identifying and classifying data to provide consistency across the enterprise. All the Microsoft Applications now have a default setting, 'sensitive'. Users as well as data owners can change the default setting as appropriate.
- Implemented technical controls that integrate data classification with Data Loss Prevention (DLP) in order to enforce data protection policies. This includes preventing sensitive data from being transmitted over public networks or copied to portable devices without encryption.
- Implemented House Bill (HB) 3834 by working with General Counsel to ensure external service providers such as contractors, complete agency Cybersecurity Awareness Training as a condition to gaining network access.

If you have any questions or comments, please let me know.

Sincerely,

Mark A. Poehl

Mark A. Poehl, CPA, CIA, CISA, CFE
Assistant Commissioner, Internal Audit and Compliance

PERFORMED BY:

Mr. Aporajita Ahmed, CPA, CFE, CITP, CGMA, CICA, Certified Cybersecurity Professional, Internal Audit lead

cc:

THECB

Board Members

Commissioner's Office

Mr. Rey Rodriguez, Deputy Commissioner and Chief of Staff
Ms. Nicole Bunker-Henderson, General Counsel
Ms. Zhenzhen Sun, Assistant Commissioner for Information Solutions and Services

STATUTORY DISTRIBUTION REQUIREMENT

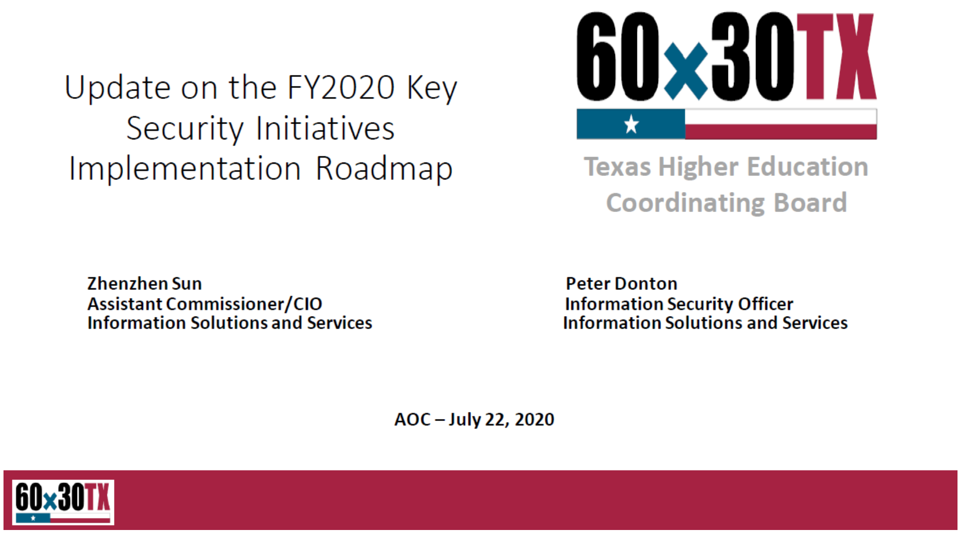
Governor's Office - Budget and Policy Division
Ms. Sarah Hicks, Director

State Auditor's Office
Internal Audit Coordinator

Legislative Budget Board
Mr. Christopher Mattson, Manager

Sunset Advisory Commission
Ms. Jennifer Jones, Executive Director

Appendix 1



Update on the FY2020 Key Security Initiatives Implementation Roadmap

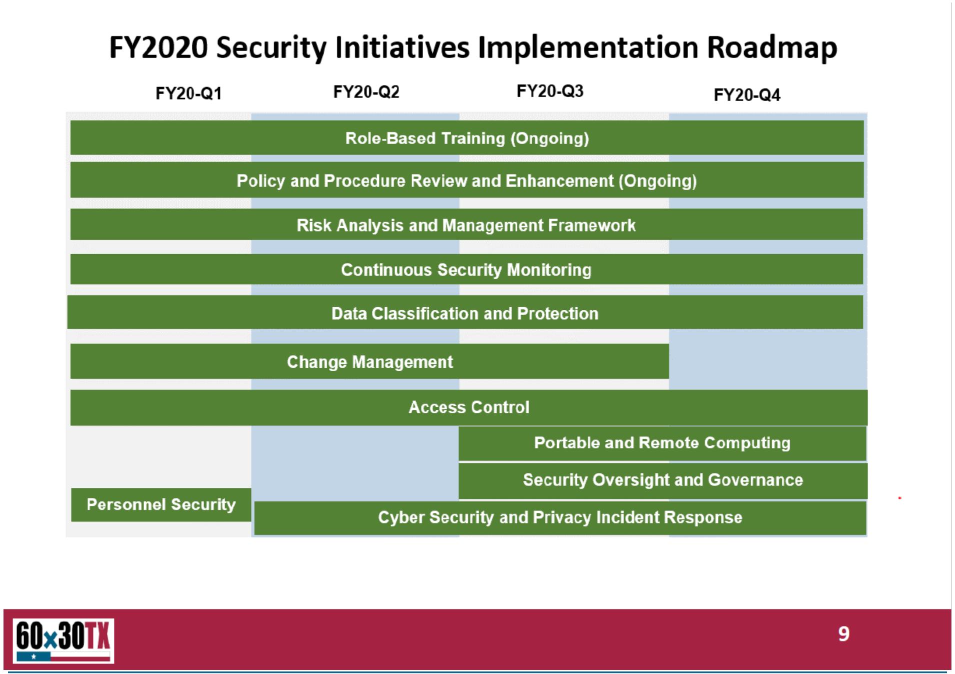
60x30TX

Texas Higher Education Coordinating Board

Zenzhen Sun
Assistant Commissioner/CIO
Information Solutions and Services

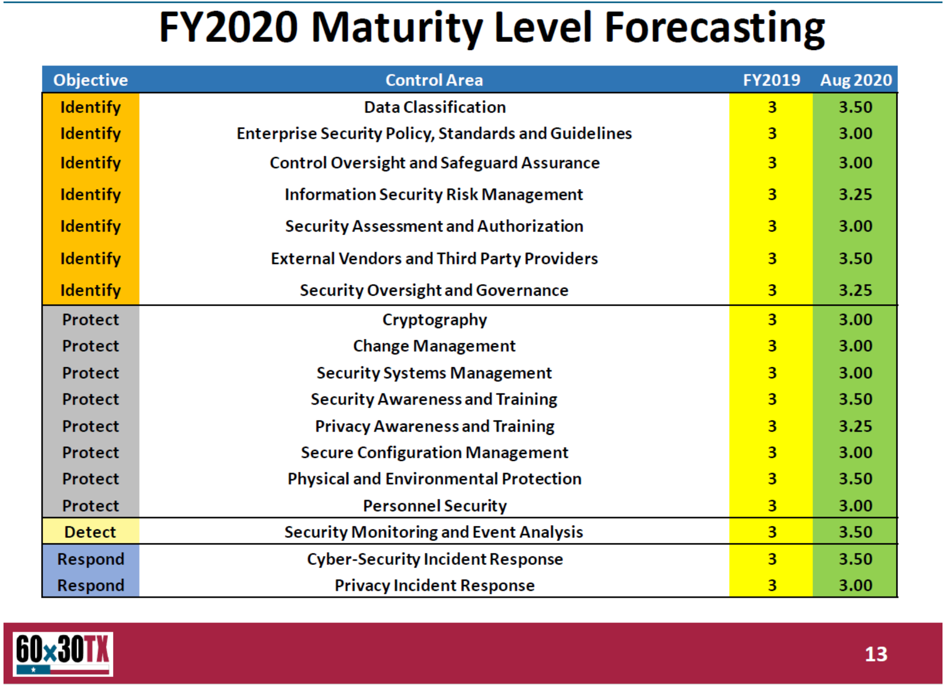
Peter Donton
Information Security Officer
Information Solutions and Services

AOC – July 22, 2020



FY2020 Security Initiatives Implementation Roadmap

FY20-Q1
FY20-Q2
FY20-Q3
FY20-Q4
Role-Based Training (Ongoing)
Policy and Procedure Review and Enhancement (Ongoing)
Risk Analysis and Management Framework
Continuous Security Monitoring
Data Classification and Protection
Change Management
Access Control
Portable and Remote Computing
Security Oversight and Governance
Personnel Security
Cyber Security and Privacy Incident Response
60x30TX
9

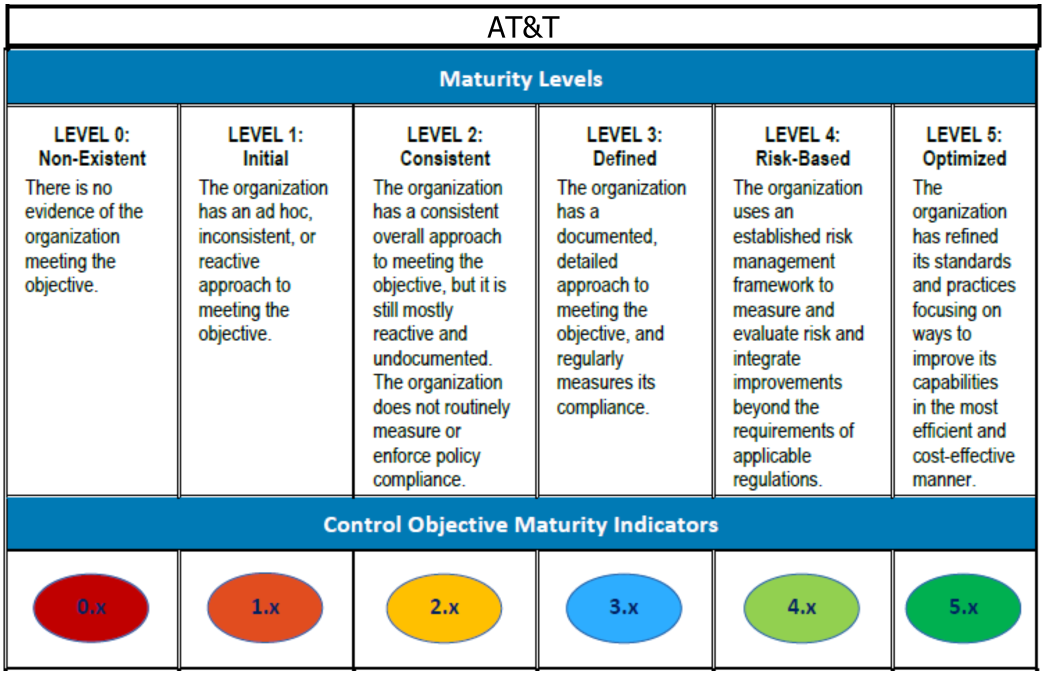


FY2020 Maturity Level Forecasting

Objective	Control Area	FY2019	Aug 2020
Identify	Data Classification	3	3.50
Identify	Enterprise Security Policy, Standards and Guidelines	3	3.00
Identify	Control Oversight and Safeguard Assurance	3	3.00
Identify	Information Security Risk Management	3	3.25
Identify	Security Assessment and Authorization	3	3.00
Identify	External Vendors and Third Party Providers	3	3.50
Identify	Security Oversight and Governance	3	3.25
Protect	Cryptography	3	3.00
Protect	Change Management	3	3.00
Protect	Security Systems Management	3	3.00
Protect	Security Awareness and Training	3	3.50
Protect	Privacy Awareness and Training	3	3.25
Protect	Secure Configuration Management	3	3.00
Protect	Physical and Environmental Protection	3	3.50
Protect	Personnel Security	3	3.00
Detect	Security Monitoring and Event Analysis	3	3.50
Respond	Cyber-Security Incident Response	3	3.50
Respond	Privacy Incident Response	3	3.00

Appendix 2

NTT Maturity Levels					
LEVEL 0: Non-Existent. There is no evidence of the organization meeting objective	**LEVEL 1: Initial.** The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.	**LEVEL 2: Repeatable.** The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.	**LEVEL 3: Defined.** The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.	**LEVEL 4: Managed.** The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.	**LEVEL 5: Non-Existent.** The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.
Control Objective Maturity Indicators					
0	1	2	3	4	5



AT&T					
Maturity Levels					
LEVEL 0: Non-Existent There is no evidence of the organization meeting the objective.	**LEVEL 1: Initial** The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.	**LEVEL 2: Consistent** The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.	**LEVEL 3: Defined** The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.	**LEVEL 4: Risk-Based** The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.	**LEVEL 5: Optimized** The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.
Control Objective Maturity Indicators					
0.x	1.x	2.x	3.x	4.x	5.x