FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Audit of the University's IT Network Security Controls

Report No. 17/18-02

November 2, 2017

FIU | FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: November 2, 2017

To: Robert Grillo, Vice President of Information Technology and CIO

From: Allen Vann, Chief Audit Executive Allen Vann

Subject: Audit of the University's IT Network Security Controls
Report No. 17/18-02

Pursuant to our approved annual plan, we have completed a follow-up to our prior audit of the University's Information Technology Network Security Controls issued in September 2015. The primary objectives of our audit were to evaluate the effectiveness of the reported implementation of the prior audit recommendations and assess the maturity level of the University's cybersecurity processes.

Since the prior audit, the Division of Information Technology (IT) has upgraded the University's cybersecurity controls. Security improvements to payment card devices, user access, and increased security awareness have all proved beneficial. Nevertheless, our examination revealed that four of our past recommendations were partially implemented and one was not implemented. While FIU cybersecurity related policies continue to evolve, further efforts are needed in the areas of formal system-wide security risk assessments and critical firewall reviews. In addition, there are areas where FIU credit card data transmissions and wildcard certificates still pose a risk.

The Division of IT agreed to continue to work with the University's Compliance Office, IT Administrators, the Controller's Office, and other stakeholders to complete the implementation of the remaining recommendations with a view towards achieving a safer network infrastructure.

I would like to take this opportunity to express our appreciation to you and your staff for the cooperation and courtesies extended to us during the audit.

Attachment

C: FIU Board of Trustees
Mark B. Rosenberg, University President
Kenneth G. Furton, Provost and Executive Vice President
Kenneth A. Jessell, Chief Financial Officer and Senior Vice President
Javier I. Marques, Chief of Staff, Office of the President

TABLE OF CONTENTS

OBJECTIVES, SCOPE AND METHODOLOGY

Pursuant to our approved annual plan, we have completed an audit of the University's Information Technology Network Security Controls. The primary objectives of our audit were to (1) evaluate the implementation of the prior audit recommendations to protect the confidentiality, integrity, and availability of the University's sensitive and/or critical data in transit; and (2) assess the maturity level of the University's cybersecurity processes.

During the audit, we reviewed current practices and processing techniques, interviewed responsible personnel and analyzed specific areas of the University's cybersecurity controls. Sample sizes selected for examination were determined on a judgmental basis. Audit fieldwork was conducted from February to August 2017.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*. To accomplish specific Information Technology control objectives, we applied a governance, risk and compliance framework, which utilizes the *Control Objectives for Information and related Technology (COBIT) 5.0 Framework, National Institute of Standards and Technology (NIST) Special Publication 800-53A Revision 4 Assessing Security and Privacy Control in Federal Information Systems and Organizations, and the NIST Baldrige Cybersecurity Excellence Builder Draft dated September 2016*. The Draft is a voluntary self-assessment tool that enables organizations to better understand the effectiveness of their cybersecurity risk management efforts.

As part of our audit, we reviewed internal and external audit reports issued during the last three years to determine whether there were prior recommendations related to the scope and objectives of this audit and whether management had effectively addressed prior audit concerns. There were prior internal audit recommendations from the Audit of University's IT Network Security Controls (Report No. 15/16-02, dated September 29, 2015) requiring follow-up. The follow-up on these recommendations are addressed in section 1 of this report.

BACKGROUND

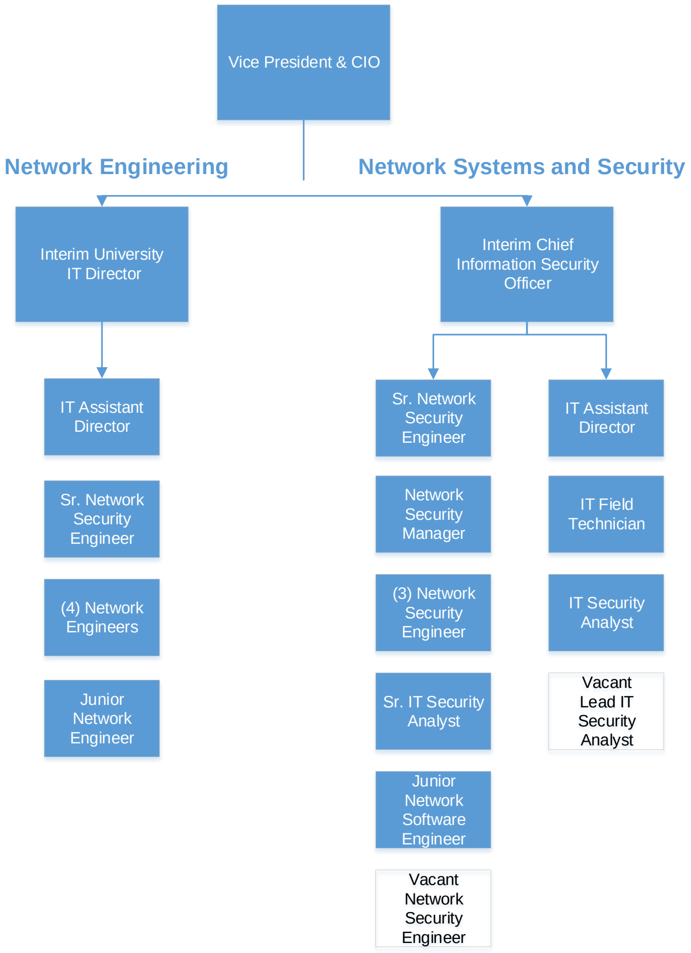
Cybersecurity entails protecting electronically stored and transmitted information by preventing, detecting and responding to attacks. The University's cybersecurity controls cover 165 buildings at the MMC, BBC, Engineering Center, Wolfsonian-FIU, FIU at I-75 and Downtown Brickell campuses.

Since the prior audit, the Division of IT has upgraded the University's cybersecurity controls. As part of the University's ongoing cybersecurity strategy, on March 8, 2016 the Division of IT began implementing two-factor authentication to high risk applications that included VPN, myFIU, and MyAccounts. Two-Factor Authentication increases security measures on user accounts by requiring two steps to log in to their FIU services, which is something they know (password) and something they have (a physical device, like a smartphone). It also offers more account security than a password alone thereby adding an additional security layer of protection.

On March 20, 2017, the Division of IT launched a new Cybersecurity Awareness Training program designed to help users identify and prevent the loss of sensitive data. Since August 13, 2017, all PantherSoft Reporting environments began using Two-Factor Authentication.

Personnel

The Network Engineering and Network Systems and Security Departments are part of the Division of IT and are responsible for maintaining the FIU network security controls. The two departments have maintained their staff sizes in comparison to the prior audit with a total of 8 and 11 employees, respectively. The prior Associate Director of the Network Systems and Security Department is now the interim Chief Information Security Officer. In addition, the Division of IT hosts monthly meetings and sends out email alerts to email groups as a means to communicate directly with the University departments regarding network security controls.


Vice President & CIO
Network Engineering
Network Systems and Security
Interim University IT Director
Interim Chief Information Security Officer
IT Assistant Director
Sr. Network Security Engineer
(4) Network Engineers
Junior Network Engineer
Sr. Network Security Engineer
Network Security Manager
(3) Network Security Engineer
Sr. IT Security Analyst
Junior Network Software Engineer
Vacant Network Security Engineer
IT Assistant Director
IT Field Technician
IT Security Analyst
Vacant Lead IT Security Analyst

Financial Information

According to the Division of IT, during the 2015-16 fiscal year, they spent a total of $2.5 million on cybersecurity related controls as follows.

Division of IT Cybersecurity-related Expenditures by Category	
Category	**Amount**
Security Resources FTE	$501,455
Border Firewalls	454,082
McAfee Endpoint: Antivirus, Threat Intelligence, Data Loss Prevention, Whole Disk Encryption, Host Intrusion Prevention	324,879
McAfee Network IPS	199,981
Security Information and Event Management (SIEM)	185,078
Two Factor	135,000
Vulnerability Management Software	132,800
Backup (Crashplan)	85,391
Data Center Firewalls	57,460
DR Firewalls	41,040
VPN (3-year cost)	85,209
Security Awareness (2-year cost)	83,500
Cybersecurity Insurance	59,422
Lifesafe for Students	50,000
Splunk	47,578
Forensics Tools	6,094
Total	$2,448,969

FINDINGS AND RECOMMENDATIONS

As with the last audit, we identified areas where the Division of IT has opportunities to strengthen network security, particularly in improving the communication with Information Technology Administrators (ITAs) and the creation of key performance indicators to ensure that strategies are accomplished. Our review of the prior audit recommendations revealed that the Division of IT has made improvements in its ability to identity, protect, detect, respond and recover from cybersecuity related incidents. However, 5 of the 13 prior recommendations were not fully completed. Additional efforts are underway in the following areas: policies, system-wide risk assessments, secure transmission of credit card data, firewall rules review, and the use of wildcard certificates. The completion of the prior recommendations will undoubtedly increase the effectiveness of the University's network security controls.

Our overall evaluation of internal controls is summarized in the table below.

INTERNAL CONTROLS RATING			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls		**X**	
Policy & Procedures Compliance		**X**	
Effect		**X**	
Information Technology Risk		**X**	
External Risk		**X**	

INTERNAL CONTROLS LEGEND			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls	**Effective**	**Opportunities exist to improve effectiveness**	**Do not exist or are not reliable**
Policy & Procedures Compliance	**Non-compliance issues are minor**	**Non-compliance Issues may be systemic**	**Non-compliance issues are pervasive, significant, or have severe consequences**
Effect	**Not likely to impact operations or program outcomes**	**Impact on outcomes contained**	**Negative impact on outcomes**
Information Technology Risk	**System controls are effective in mitigating identified data risks**	**System controls are moderately effective in mitigating identified data risks**	**Systems controls are ineffective in mitigating identified data risks**
External Risk	**None or Low**	**Medium**	**High**

1. Implementation of Prior Audit Recommendations

In our prior audit report, issued on September 29, 2015, there were 13 network security related recommendations reported by management as completely implemented. During the audit, we compared their assertions to actual processes, interviewed personnel, and tested selected devices.

Our examination of the thirteen recommendations revealed that eight were fully implemented, four were partially implemented, and one was not implemented. Overall, the University has made control improvements to payment card devices, user access, and increased security awareness. While FIU cybersecurity related policies continue to evolve, further efforts are needed in the areas of formal system-wide security risk assessments, critical firewall reviews, secure transmission of credit card data, and the continued use of wildcard certificates.

The test results for each prior recommendation examined are as follows:

#	Recommendation	Implementation		
		Full	Partial	Not
1. Identify Function				
1.1	Work with the various units to ensure that it receives notification of any changes to device inventories, especially payment card devices.	✓		
1.2	Work with senior management to enhance policies so as to provide for stronger centralized authority over the implementation of security controls and ensure that business units understand their responsibilities.		✓	
1.3	Perform periodic formal system-wide security risk assessments.		✓	
2. Protect Function				
2.1	Review privileged user accounts to ensure terminated account are disabled; senior management administrator access is disabled; and staff access is limited to the least necessary to perform their job duties.	✓		
2.2	Continue to work with senior management to increase participation in security awareness training.	✓		
2.3	Ensure credit card data is transmitted on a secured VLAN.		✓	
2.4	Discontinue the use of unnecessary wildcard certificates.			✓
2.5	Review all critical firewalls and at a minimum disable all non-active rules.		✓	

#	Recommendation	Implementation		
		Full	Partial	Not
3. Detect Function				
3.1	Formally review and approve IPS rules that are made by its Network Systems and Security unit.	✓		
3.2	Work with the business units to increase vulnerability scan participation.	✓		
4. Respond Function				
4.1	Formally track and review network security events identified by the detection controls and perform lessons learned with the affected Information System Administrator.	✓		
5. Recover Function				
5.1	Assess the four remaining critical devices and consider adding similar redundancies or include them separately in the Disaster Recovery Plan.	✓		
6. Implementation of Prior Audit Reports Recommendations				
6.1	Work with the effected business units to help them implement the cited recommendations.	✓		

Recommendation

The Division of Information Technology should:	
1.1	Fully implement all prior audit recommendations.

Listed below are the recommendations determined to be not fully implemented accompanied by the results of our current observations and management action plan with the revised implementation date.

- **Recommendation No. 1.2** - Work with senior management to enhance policies so as to provide for stronger centralized authority over the implementation of security controls and ensure that business units understand their responsibilities.

  Previously Reported Actions: Security policies are continuously being reviewed to provide a stronger centralized authority over implementation of security controls for the whole organization. We recently revised our Incident Response Plan, which has been reviewed and approved by the university. The Incident Response Plan is a plan developed for the whole university to follow. We have plans to continue to share the Incident Response Plan with the university community (Previously Reported Implementation Date: July 31, 2017).

  Current Observation: According to the Chief Information Security Officer, the Incident Response Plan was issued to the FIU Executive Committee on August 17, 2016, Information Technology Administrators from 17 departments, and the Dean's Advisory Committee on October 12, 2016. The plan includes a Local

Responder Roles and Responsibilities section to help ensure that business units understand their responsibilities. We were also informed that the Division of IT is continuing to working with the Compliance Office to enhance cybersecurity related policies.

Management Action Plan: Division of IT will continue to update, review, and create new IT Cyber Security Policies where applicable. This is an ongoing task since policies need to be reviewed annually as part of compliance efforts (Revised Implementation Date: December 31, 2018).

- **Recommendation No. 1.3 -** Perform periodic formal system-wide security risk assessments.

  Previously Reported Actions: The Division of IT will be performing periodic security risk assessments. Risk Assessments will be done first in areas of higher risk (Previously Reported Implementation Date: January 20, 2017).

  Current Observation: According to the Division of IT, four informal risk assessments have been performed by the Network Services Department. A formal risk assessment process would provide a better understanding of the University's data risk profile.

  Management Action Plan: The Division of IT will continue to perform security risk assessments. The Division of IT is currently working with the Office of Compliance to finalize the statement of work for a multi-year HIPAA University Wide Assessment. The Division of IT has been working with the Office of the Controller to perform PCI Risk Assessments. We have hired a vendor, Campus Guard to perform PCI risk assessments for the next two years. The Division of IT has also increased their ability to run vulnerability scans accords the FIU network in order to reduce the risk of compromised systems and vulnerabilities. The Division of IT has contracted an external vendor to run vulnerability scans from outside the FIU network for critical systems (Revised Implementation Date: December 31, 2018).

- **Recommendation No. 2.3 -** Ensure credit card data is transmitted on a secured VLAN.

  Previously Reported Action: Finance now manages PCI compliance at FIU. Many credit card devices have been upgraded by the Controller's Office and there are plans to issue PIN pads to improve security. Division of IT will assist Finance as needed (Previously Reported Implementation Date: May 31, 2016).

  Current Observation: An outside consulting firm hired to review FIU's PCI-DSS security controls found that several areas/departments represented significant risk and liability to the University. The consultant expressed their concerns about the level of FIU's compliance with the Payment Card Industry Data Security Standard. Additionally, 7 of 53 FIU credit card payment devices were found to be a security risk by the FIU PCI Compliance Team.

Management Action Plan: The Division of IT will continue to work with the Controller's Office to meet PCI Compliance requirements. We have hired a consultant, Campus Guard to assist us in this process. We have also signed a master agreement with Bluefin, a validated point-to-point encryption (P2PE) solution vendor in order to migrate all existing point of sale devices to the validated P2PE solution for all FIU merchant accounts. This will place FIU network out of scope for PCI-DSS. Bank of America has issued an extension for PCI-DSS Compliance to FIU with a deadline of June 2019 (Revised Implementation Date: June 1, 2019).

- **Recommendation No. 2.4 -** Discontinue the use of unnecessary wildcard certificates.

  Previously Reported Actions: The Division of IT will discontinue use of wildcard certificates where applicable (Previously Reported Implementation Date: May 31, 2016).

  Current Observation: The Division of IT has discontinued two and also added two departments. Once issued, the Division of IT doesn't track which devices contain the certificate, which may lead to improper usage.

  Management Action Plan: Wildcards are still required and will continue to be used in certain deployments where appropriate. The Division of IT approves the purchase of wildcard certificates and does not issue the same certificate to multiple units. The Division of IT will create a policy for the admins to take accountability when using these wildcard certificates; making them responsible for tracking where the certificates are used (Revised Implementation Date: June 1, 2018).

- **Recommendation No. 2.5** - Review all critical firewalls and at a minimum disable all non-active rules.

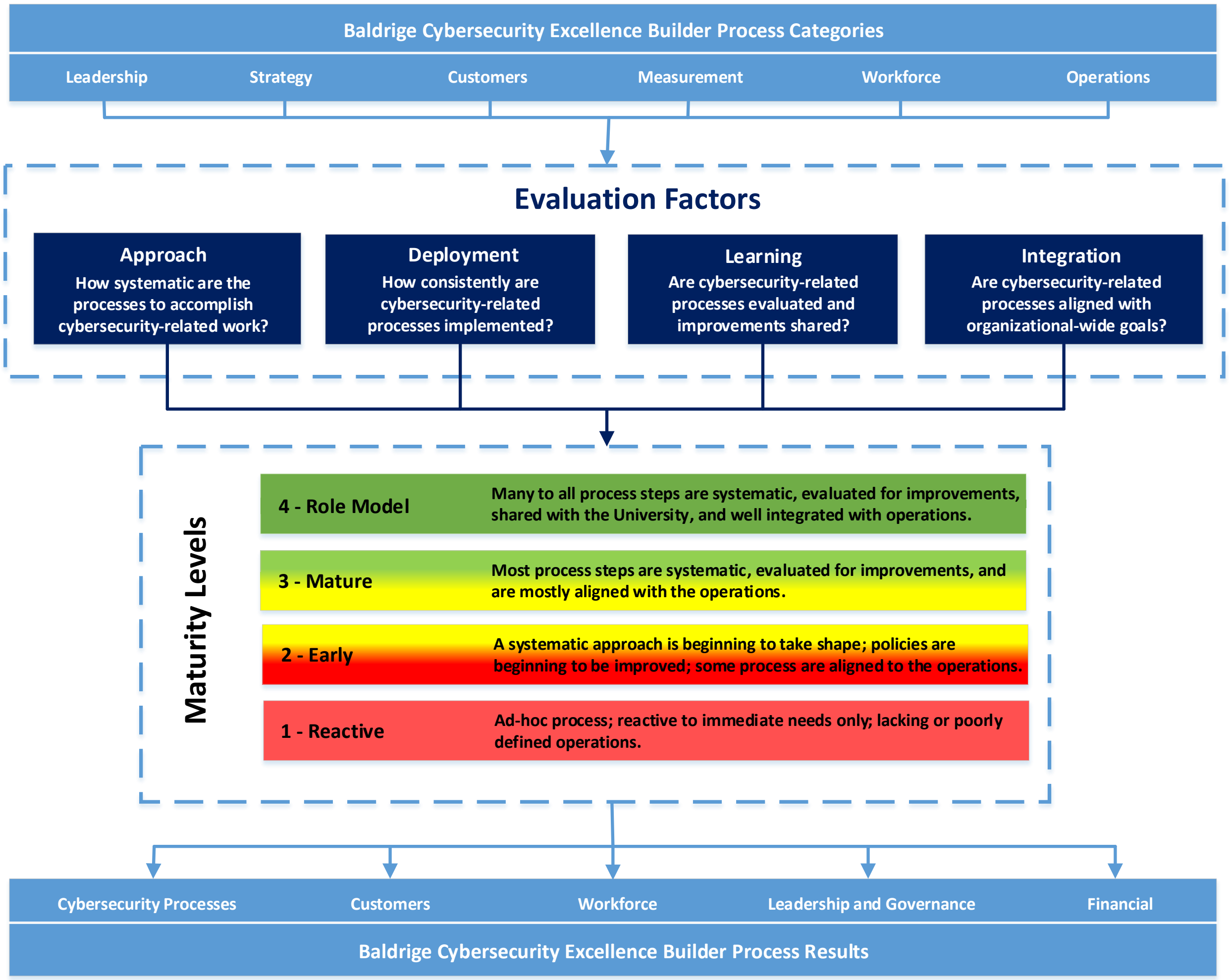
  Previously Reported Actions: The Division of IT will define a process to regularly review and disable firewall rules that have not been used (Previously Reported Implementation Date: May 31, 2016).

  Current Observation: The Division of IT has started reviewing University firewall rules. Documentation provided as evidence showed that the Network Systems and Security Department meets quarterly with the College of Medicine to review rules on selected servers.

  Management Action Plan: The Division of IT does routinely review firewall access lists for various departments such as the Frost Art Museum, One Card, College of Medicine, etc. The Division of IT will continue to improve and develop the processes associated with these tasks (Revised Implementation Date: December 31, 2017).

2. Effectiveness of Cybersecurity Risk Management Efforts

The *National Institute of Standards and Technology (NIST) Baldrige Cybersecurity Excellence Builder* consists of cybersecurity related approaches and results achieved in the areas of leadership, strategy, customers, workforce and operations. It also blends the systems perspective of the Baldrige Excellence Framework with the Cybersecurity Framework as illustrated on the following diagram:



Baldrige Cybersecurity Excellence Builder Process Categories

Leadership | Strategy | Customers | Measurement | Workforce | Operations

Evaluation Factors

Approach How systematic are the processes to accomplish cybersecurity-related work?

Deployment How consistently are cybersecurity-related processes implemented?

Learning Are cybersecurity-related processes evaluated and improvements shared?

Integration Are cybersecurity-related processes aligned with organizational-wide goals?

Maturity Levels

4 - Role Model	Many to all process steps are systematic, evaluated for improvements, shared with the University, and well integrated with operations.
3 - Mature	Most process steps are systematic, evaluated for improvements, and are mostly aligned with the operations.
2 - Early	A systematic approach is beginning to take shape; policies are beginning to be improved; some process are aligned to the operations.
1 - Reactive	Ad-hoc process; reactive to immediate needs only; lacking or poorly defined operations.

Cybersecurity Processes | Customers | Workforce | Leadership and Governance | Financial

Baldrige Cybersecurity Excellence Builder Process Results

A total of 109 Information Technology Administrators (ITAs) were invited to participate in an online questionnaire to solicit their input on the performance of University's cybersecurity controls. As subject matter experts of their departments, we asked them to evaluate each factor from predefined maturity levels. We based our results on the 17 participants who completed the online survey. In addition, we selected 5 out of 17 participants and conducted interviews.

The areas of our observations follow the order of the process categories described above.

a) Leadership

The ITAs were asked to rate leadership's ability to communicate their vision, values and overall mission to key stakeholders. Specifically, how senior and cybersecurity leaders lead cybersecurity policies and operations.

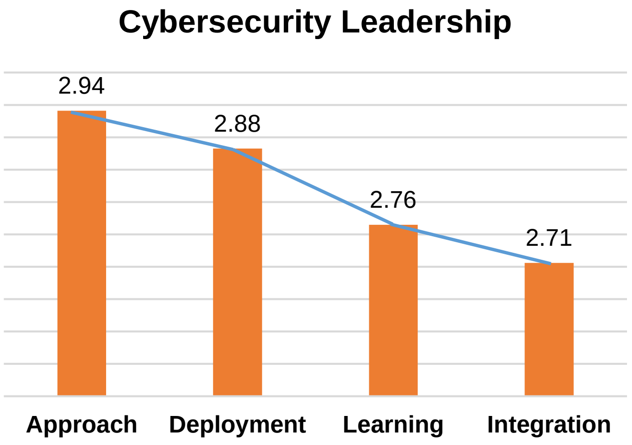


Figure 1

Results from our survey indicate an Early maturity level rating (see Figure 1) and suggest that leadership's effort to get their cybersecurity message to the appropriate units is beginning to take effect. This is also supported by interviews with the ITAs. Their comments included that leadership is committed to cybersecurity and that the CIO has cybersecurity on the top of his agenda. However, the drop between the Approach and Integration factors suggests that Division of IT should assist the ITAs in integrating cybersecurity policies. Currently, the Division of IT is working with the University's Compliance Office to conduct policy reviews. Once finalized, the policies need to be shared with individual departments.

The ITAs were also asked how they govern cybersecurity policies and operations. The ratings in Figure 2 suggest that ITAs are in the Early maturity level of overseeing FIU's strategic vision within their department. This was also supported from ITAs interviews that showed there was no formal guidance on how they ensured the governance of cybersecurity within their department. For example, they indicated that they relied on self-governance of staff or cybersecurity awareness training completion rates.

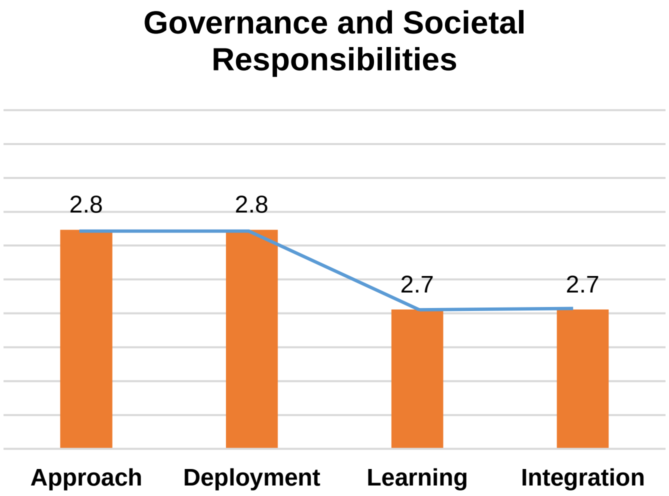


Figure 2

Presently, there is not a consistent measureable method to gauge the effectiveness of the Leadership and Governance controls on operations.

b) Strategy

The Strategy category refers to the department’s approach in preparing for future cybersecurity threats. An approach might include forecasting, scenarios, and/or analysis in order to make strategic decisions and to allocate resources. The ITAs were asked to rate how they develop their cybersecurity strategy.

Based on the ratings in Figure 3, cybersecurity implementation strategies range from Early to Mature levels throughout their department. The feedback from the ITAs showed that they relied on the Division of IT to develop their cybersecurity strategy.

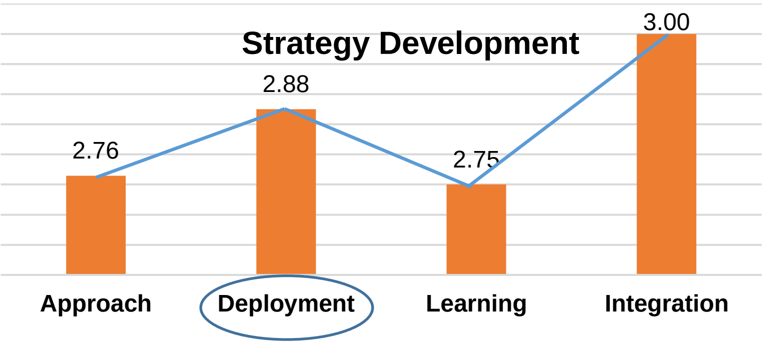


Figure 3

With their reliance on the Division of IT, we found a direct correlation between cybersecurity strategy development and implementation process ratings as highlighted in Figure 4. Since the departments rely on the Division of IT, the ratings suggest that their confidence in how strategies are developed is also carried over to the strategy implementation. The drop in the Deployment rating to 2.71 suggests that ITAs are less sure on how the cybersecurity strategies are applied to their departments. This was supported from the ITAs feedback that included comments such as more communication before implementation would be helpful and that they rated the question conservatively since they do not perform the strategy implementation. Even though the ITAs rely on the Division of IT for their cybersecurity related controls, they should still be included in the strategy development and implementation process to ensure that their department’s needs are adequately addressed.

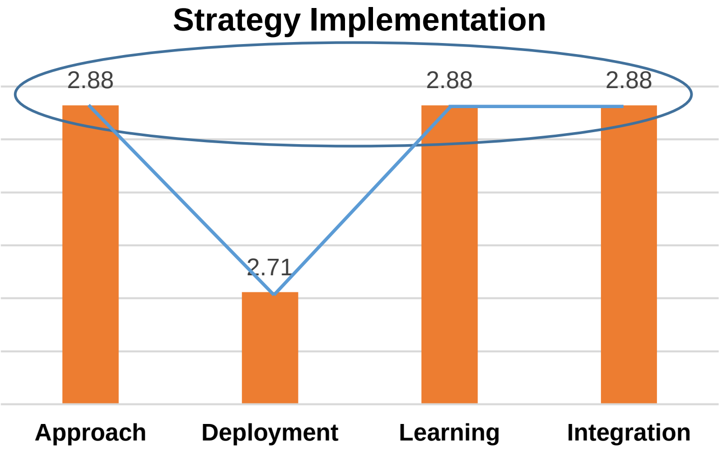


Figure 4

c) Customers

The Customers category refers to the process ITAs use for capturing their user related information. The Mature model ratings in Figure 5 suggest that ITAs have systematic methods when interacting with their users. They then evaluate the information to improve user experiences throughout their department.

Feedback we received from the ITAs on the methods they used to gather user information included informal processes, such as keeping an open communication with their staff, working directly with the students to make them feel more secure, and informing users to contact the ITA directly for assistance.

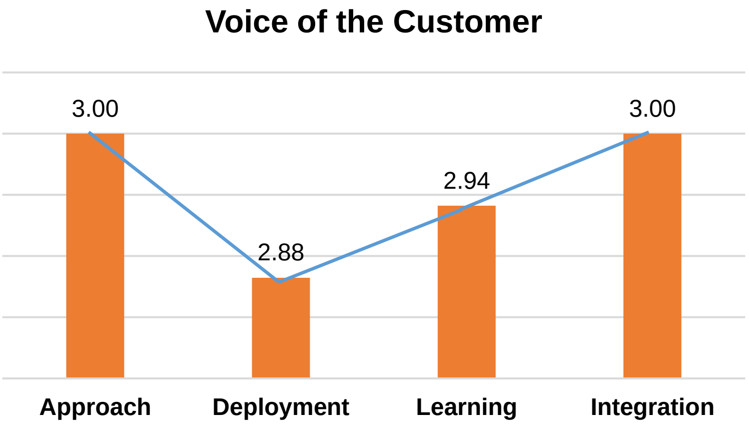


Figure 5

The Deployment factor rating in Figure 5 suggests that the ITAs are slightly less confident that user feedback is directly applied to their cybersecurity controls by the Division of IT.

The ITAs were also asked to rate how they engage their users to better serve their needs and build strong relationships. Specifically, how well they enabled their users to seek information and support related to the department’s cybersecurity operations. Some ITAs indicated that their user complaint process was informal and not tracked, whereas others had a formal process that was periodically reviewed.

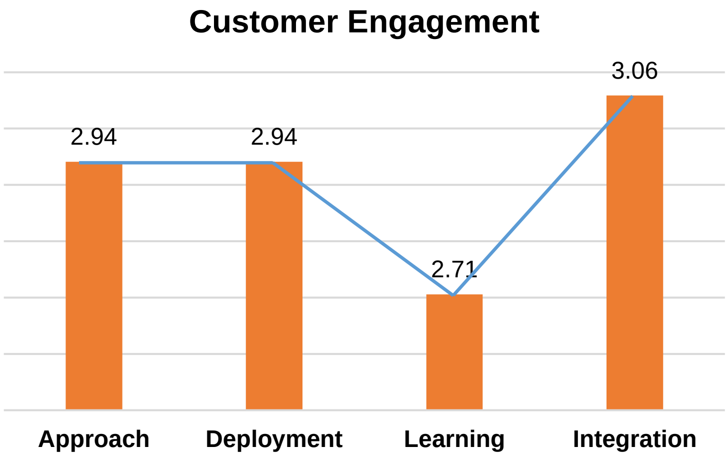


Figure 6

On July 10, 2017, the FIU policies website added a feedback section allowing users to send in their comments regarding a specific policy. The University’s Compliance Office automatically receives the data collected from the feedback section. Once received, the information is disseminated and forwarded to the appropriate policy owner. Additionally, the University’s Compliance Office stated that they will use the feedback for analysis and increase the communication between policy owners and the FIU community.

d) Measurement, Analysis, and Improvement of Performance

The ITAs were asked to rate how they measure, analyze, and use the information to improve the performance of their cybersecurity related controls. The ratings in Figure 7 suggest that ITAs are in the Early level of measuring the effectiveness of their cybersecurity controls. Supported by Early or lower level rating feedback was that an analysis was not performed as the data was not shared by the Division of IT, and another gave a low rating due to a lack of network security reports.

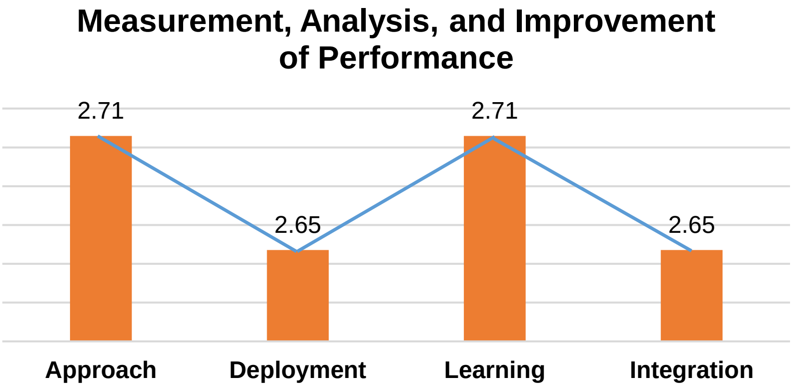


Figure 7

In addition, others rated the Mature or higher level based on either the perception of the Division of IT or specific items such as mandating cybersecurity training, percentage of machines using McAfee product suite, and endpoint devices connected to the crash plan.

The ITAs were also asked to rate how well they managed cybersecurity knowledge and resources into their operations to maintain awareness of a continually changing threat environment. The ITAs interviewed rely on the Division of IT to supply the necessary information systems and financial resources necessary to support cybersecurity controls. Their feedback in Figure 8 reflects the ITAs' lack of familiarity with the management aspects of cybersecurity but that it was appropriately integrated into their processes.

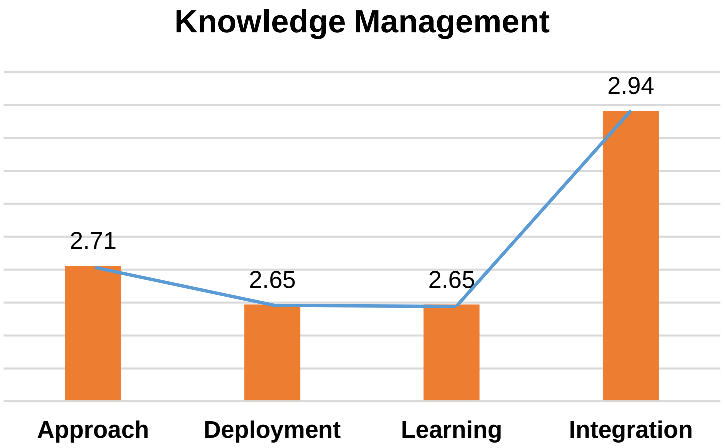


Figure 8

According to the ITAs interviewed up to 5% of their budget was devoted to cybersecurity. There is a cost savings to the departments by having the Division of IT provide cybersecurity controls at no cost to the departments.

e) Workforce

The ITAs were asked to rate how they build an effective and supportive workforce environment to achieve their cybersecurity goals. Specifically, how well they assess and prepare their workforce for changing cybersecurity needs. The IT staff sizes interviewed have 1, 3, and 5 personnel, respectively. Due to the limited staff sizes, the ITAs rely on the Division of IT as their cybersecurity workforce.

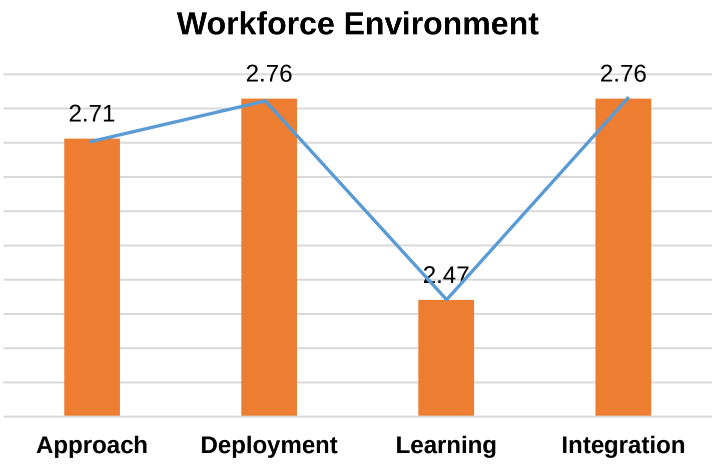


Figure 9

Results from our feedback (see Figure 9) reflect a drop in the Learning factor that suggests that the ITAs were unable to evaluate their Workforce Environment's effectiveness. For example, one of the ITAs indicated that he did not receive antivirus reports for review that contributed to the lower rating.

The ITAs were also asked to rate their department's ability to engage their workforce and achieve a high-performance environment that is in support of their cybersecurity operations. From their feedback, the ITAs use their staff participation rate of the online cybersecurity awareness training as their main method of engaging personnel.

The rating difference between the Learning and Integration factors (see Figure 10) suggests that the ITAs either do not have metrics to appropriately evaluate the effectiveness of cybersecurity awareness training or training was not as helpful as anticipated. Key performance indicators should be developed to ensure that staff skillsets are effectively maintained to handle cybersecurity events.

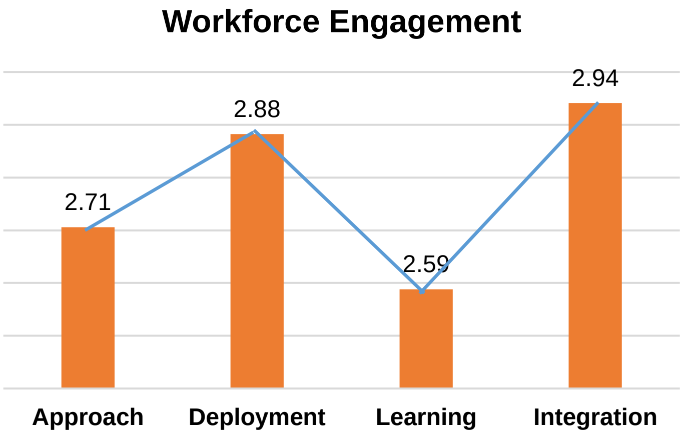


Figure 10

f) Operations

The Operations category is tied to the National Institute of Standards and Technology's Cybersecurity Framework.[1] The ITAs were asked to rate their department's ability to protect, detect, respond and recover form cybersecurity events. Specifically, how well they designed, managed, and improved their key cybersecurity work processes. Results from our survey (see Figure 11) suggest that the departments are in the Early maturity level of applying cybersecurity processes to their operations. Feedback from lower rating respondents included statements that: 1) not all of the personnel in their department were onboard with the cybersecurity controls, and 2) McAfee product suite training was not completed. Higher rating ITAs stated that: 1) they proactively worked with the Division of IT in obtaining 100% participation of cybersecurity awareness training, and 2) vulnerability reports were very helpful in identifying threats to specific devices.

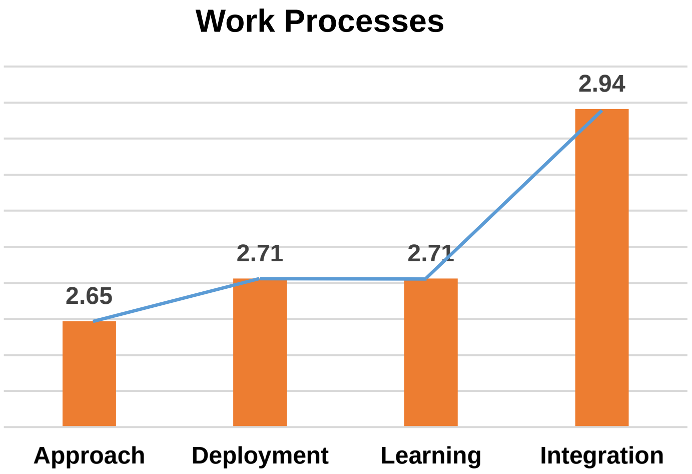


Figure 11

The ITAs were also asked to rate their operational effectiveness (see Figure 12). Specifically, how well they ensure the effective management of their cybersecurity operations. According to FIU Policy No. 1910.005, *Responsibilities for FIU Network and/or System Administrators*, the ITAs are required to maintain and make readily available to the Division of IT all documentation of all devices within their units that will connect to the University's network. Feedback from one department that rated their Operational Effectiveness as Early maturity level stated that the accuracy of their inventory list dropped 80% since attractive property limits were raised. He also did not receive access or training on Data Loss Prevention Reports.

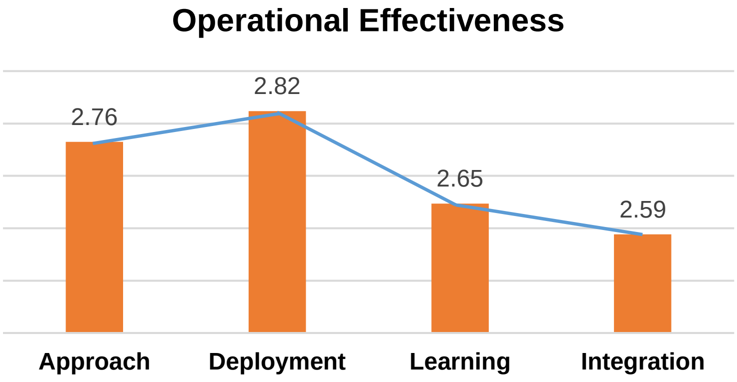


Figure 12

[1] NIST Cybersecurity Framework information is located at nist.gov/cyberframework

One ITA that rated their operational effectiveness as Mature level said that they implemented an inventory asset management process to maintain an updated list of devices. In addition, higher level rating departments tended to have better communications with the Division of IT and greater confidence that their devices were adequately protected. Also, as an additional layer of security, vulnerability scan reports are helpful in assessing the effectiveness of cybersecurity controls. One ITA who used to receive the reports said that he found it helpful in identifying threat management to endpoint devices.

Overall, ITAs are relying on cybersecurity awareness training participation rates as a way to measure the security controls effectiveness. Additional key performance indicators are needed to adequately measure the effectiveness of the University's cybersecurity controls. The ability of ITAs to review vulnerability scans and provide accurate inventory lists will lead to better device monitoring and decrease the network risk to sensitive data.

Recommendation

The Division of Information Technology should:	
2.1	Continue to leverage enhancements in cybersecurity policies, processes, and outreach efforts in order to consolidate and enhance the level of achievement already obtained.

Management Response/Action Plan:

The Division of IT will continue to enhance cybersecurity policies, processes and outreach in an ongoing manner. The Division of IT will continue to work with the Compliance Office, IT Administrators, Controllers, and other units to advocate cybersecurity awareness and develop processes to develop a safer network infrastructure.

Implementation Date: June 1, 2018