ellucian

Guam Community College Technology Assessment

for the Update of GCC's Institutional Strategic Plan and Enterprise Architecture

3/30/2022

Guam Community College

Table of Contents

Executive Summary

As part of the Update of Guam Community College's Institutional Strategic Plan, a Technology Assessment was conducted from 12/21/21 through 3/8/22. Guam Community College (GCC) partnered with Ellucian to evaluate the Management Information Systems MIS Department operations. Key elements of the assessment included meeting with a broad spectrum of college faculty and staff. Specifically, the assessment included:

1. A review of the Guam Community College Information Technology capacity, in-house applications, and other integrated applications.
2. A high-level review of the features, functions, support, configurations, and integrations of internally developed and off-the-shelf enterprise-level applications.
3. A high-level review of IT operations, its integration throughout the College, and its ability to support the institutional mission to provide quality instruction.
4. Capacity to expand distance learning.

Unique to this assessment is that it was conducted entirely remotely across 15 time zones, with data being supplied via email and conference calls. This ruled out the ability to physically inspect IT assets and most importantly the ability to engage in the dialogue and conversations that enables building the camaraderie/collaboration that face-to-face meetings facilitate.

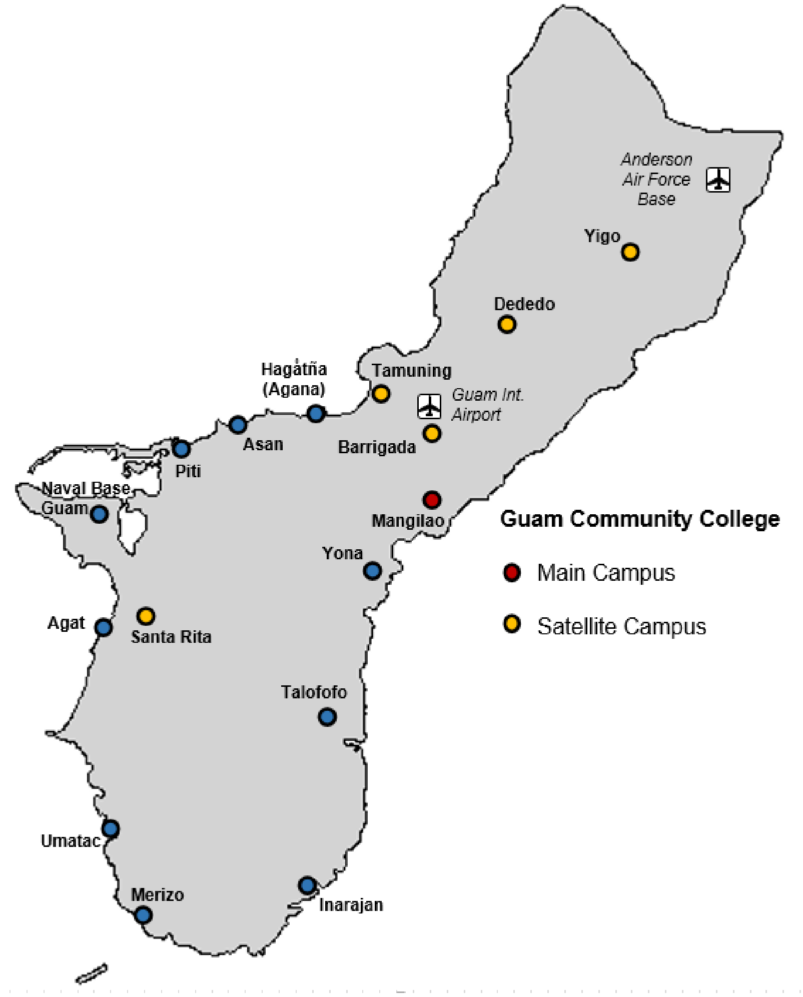
The recommendations shared in this report describe beneficial initiatives and best practices that provide context with which to view the significance of the observations presented. Ultimately, an important theme will emerge that highlights the importance of reaffirming a clear strategy across the enterprise and supporting this strategy with a robust governance structure capable of managing transformational change. This change will require a look into resource requirements but will first necessitate an internal conversation around organizational objectives and priorities.

More specific to the technology component of the enterprise strategy, the primary consideration for this report is the IT Assessment, which was performed by the Ellucian review team and will serve as a foundation for the revision of the college's IT and Strategic Plan(s). The findings describe an urgent need for business process improvements both within MIS and external to the department, system optimizations, and training/professional development at the appropriate time to be properly implemented within the GCC environment.

The common thread running through this report is the student experience. All GCC staff approached this engagement with strong interest in enhancing student services and resources, which will serve the institution well as it continues to commit the effort and resources necessary to pursue continuous improvement.

About Guam Community College

Established in 1977 by Public Law 14-77 (and amended by Public Law 31-99 in 2011). Guam Community College (GCC) is a public career and technical education institution with the main campus located in the village of Mangilao in the U.S. Territory of Guam.



GGC's mission states: "Guam Community College is a leader in career and technical workforce development, providing the highest quality, student-centered education and job training for Micronesia."

GCC is accredited by the Accrediting Commission for Community and Junior Colleges (ACCJC), Western Association of Schools and Colleges (WASC). It offers one bachelor's degree (four-year degree), 24 associate degrees (two-year programs), and 17 certificates (one-year programs). GCC also offers a U.S. Department of Labor approved Apprenticeship program in conjunction with over 100 island employers.

As Guam's only community college, it presently offers 1 associate degree fully online and is exploring expanding its' online presence and student service efforts to address decreasing enrollment, student retention, and decreasing subsidies from the Government of Guam.

Assessment Approach

Ellucian's assessment team submitted a number of requests for information over the course of the assessment. Reviewing the information provided by GCC, additional inquiries and interview requests were made. The assessment scope was crafted to evaluate key elements of GCC IT operations as well as the various policies and procedures that exist throughout the College. The focus was to understand the efficacy GCC in expanded technology solutions. The engagement included the following activities:

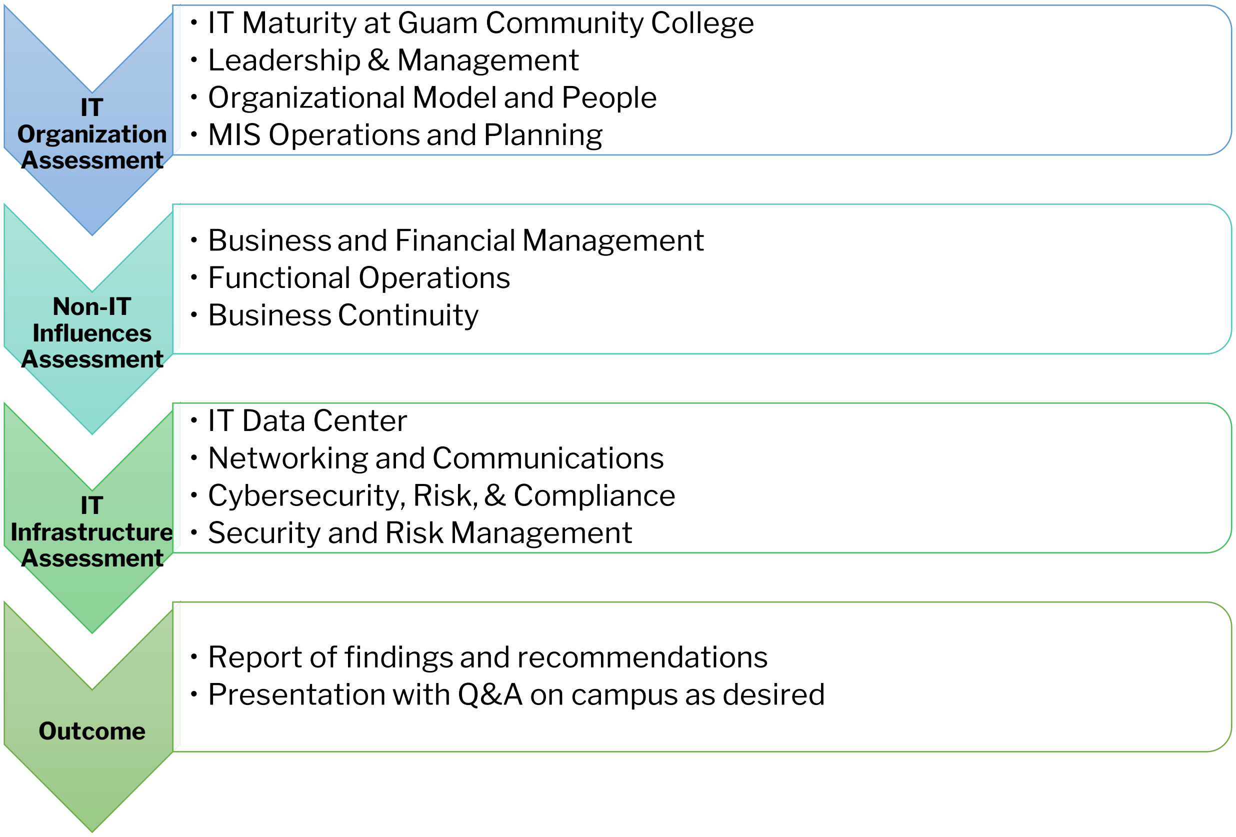
- Review with both the outgoing and interim CITO the IT organizational structure, technology planning, and overall technology operations across the College.

- Interviews with individual staff members, the IT team and senior staff.
- Examine the IT organizational structure and its alignment with strategic objectives.
- Review of multiple college provided documents. (e.g., strategic plans, budgets, disaster recovery plan, etc.)
- Literature & web research from EDUCAUSE, Chronicle of Higher Education, Gartner and similar colleges.
- Identification of potential IT peer organizations for comparison purposes.

The Ellucian team members who contributed to the assessment included:

- Jim Tisdale
- Carie Ann Potenza
- Tom Danford

The following figure depicts the key focus of the engagement and each component.



IT Organization Assessment

- IT Maturity at Guam Community College
- Leadership & Management
- Organizational Model and People
- MIS Operations and Planning

Non-IT Influences Assessment

- Business and Financial Management
- Functional Operations
- Business Continuity

IT Infrastructure Assessment

- IT Data Center
- Networking and Communications
- Cybersecurity, Risk, & Compliance
- Security and Risk Management

Outcome

- Report of findings and recommendations
- Presentation with Q&A on campus as desired

All the efforts involved in this engagement focused on identifying strengths in the existing environment and opportunities for improvement. When viewed collectively, they provide a broad overview of all key areas reviewed by Ellucian.

I. Organizational Observations and Recommendations

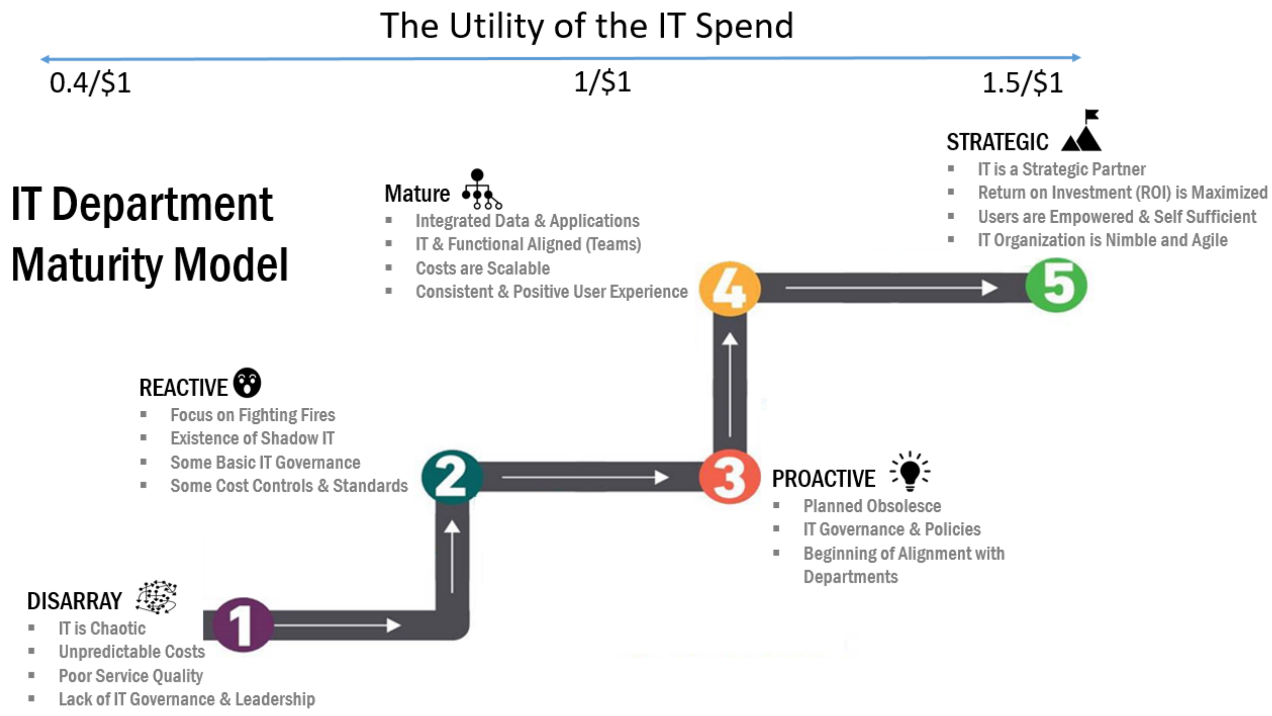
This first section of the assessment looks at the MIS department, its strategic participation in the organization, staffing and operations. It is broken down into the following four areas:

- IT Maturity at Guam Community College
- Leadership & Management
- Organizational Model and People
- MIS Operations and Planning

IT Maturity at Guam Community College

OBSERVATION: There is opportunity to improve upon the maturity of the use of Information Technology at GCC

Ellucian is continually researching and refining an IT maturity model, based on overall institutional maturity model, for higher education that evaluates and scores how colleges and universities leverage the use of technology in their organizations. The model, which ranges from "Disarray" to "Strategic," scores from zero to five and is illustrated below.


The Utility of the IT Spend
0.4/$1
1/$1
1.5/$1
IT Department Maturity Model
STRATEGIC
IT is a Strategic Partner
Return on Investment (ROI) is Maximized
Users are Empowered & Self Sufficient
IT Organization is Nimble and Agile
Mature
Integrated Data & Applications
IT & Functional Aligned (Teams)
Costs are Scalable
Consistent & Positive User Experience
REACTIVE
Focus on Fighting Fires
Existence of Shadow IT
Some Basic IT Governance
Some Cost Controls & Standards
PROACTIVE
Planned Obsolesce
IT Governance & Policies
Beginning of Alignment with Departments
DISARRAY
IT is Chaotic
Unpredictable Costs
Poor Service Quality
Lack of IT Governance & Leadership
1
2
3
4
5

The higher the organization ranks on the maturity model, the more effective its contribution to the institution's mission and each dollar spent on resources. From an IT perspective, the assessment would rank GCC's maturity level as being between "Reactive" and "Proactive."

RECOMMENDATION: GCC's executive leadership should strive to at least move the college's use of IT to the "Mature" level of the IT Maturity Model .

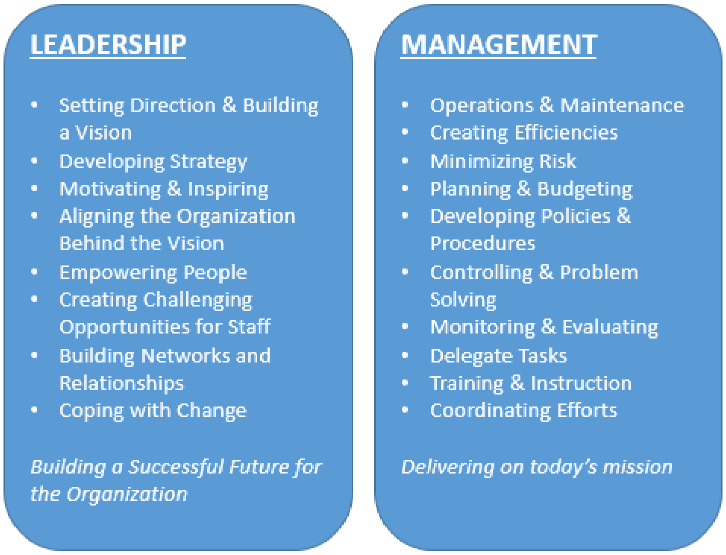
The GCC Executive team should decide upon the direction they would like to see the

College take with respect to the use of technology at the institution and which level of the maturity model they would like to achieve. This will ultimately lead to a determination as to the leadership, governance and staffing necessary to realize these aspirational goals. At a minimum the college should strive to reach the “mature” level of the Maturity Model.

Leadership & Management

OBSERVATION: The MIS Chief Information Technology Officer (CITO) has historically performed primarily in a management capacity. Leadership coupled with governance will be necessary for transformational change into a more mature IT provider.

There are major differences between leadership and management. Leadership sets the direction and vision of the IT department whereas management makes the direction and vision a reality as outlined in the graphic below.



LEADERSHIP

- Setting Direction & Building a Vision
- Developing Strategy
- Motivating & Inspiring
- Aligning the Organization Behind the Vision
- Empowering People
- Creating Challenging Opportunities for Staff
- Building Networks and Relationships
- Coping with Change

Building a Successful Future for the Organization

MANAGEMENT

- Operations & Maintenance
- Creating Efficiencies
- Minimizing Risk
- Planning & Budgeting
- Developing Policies & Procedures
- Controlling & Problem Solving
- Monitoring & Evaluating
- Delegate Tasks
- Training & Instruction
- Coordinating Efforts

Delivering on today’s mission

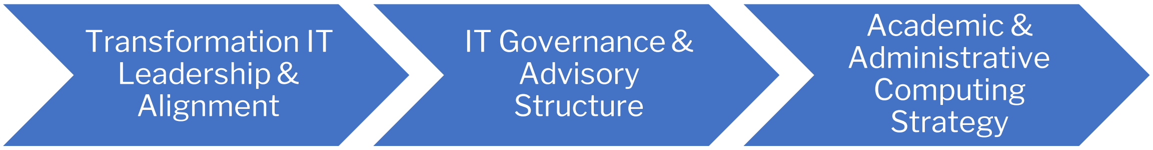
The CITO is the most senior of the MIS staff. The position reports to the Vice President, Finance & Administration. This in and of itself presents no issues as similar past assessments have shown that IT departments can function effectively whether they report to the senior finance officer (⅓), senior academic officer (⅓), and the president (⅓). However, the position as presently cast has some shortcomings:

- The job description describes mostly a management level position.
- The CITO isn’t a member of the President’s cabinet.
- There is a lack of true IT governance.
- Future plans suggest that IT strategy will not be aligned, more costly, and not as well coordinated as it could be.

The GCC CITO recent transition out of the organization provides an opportune time for the College to evaluate how to position information technology at the institution for both immediate effectiveness and long-term alignment and success. Technology is fundamental to an institution—it is a key component both short- and long-term that can have a profound positive (or negative) impact on an institution’s strategic and operational activities.

RECOMMENDATION: Align IT Leadership and Governance to better support IT goals and objectives.

The illustration below suggests the order for suggested development of leadership, governance, and strategy.


Transformation IT Leadership & Alignment
IT Governance & Advisory Structure
Academic & Administrative Computing Strategy

- Transformational IT Leadership & IT Alignment: GCC should consider transformational IT leader to develop a thriving and effective IT organization. This leader will align IT resources to work collaboratively toward a shared IT vision to best support the College. The College should look to recruit a strong, collaborative, visionary, cabinet-level IT leader who can re-calibrate and align IT to support the business vision of the new organizational model that is under study. Additional considerations include (1) rewriting the job description and (2) Interim IT leadership to assist with the job description, recruiting, and governance.

- IT Advisory & Governance Structure: Effective IT governance is critical for an institution to align organizational IT efforts to support business strategy and create value. It enables the CITO to work collaboratively with executive leadership to articulate desired outcomes and provides a framework that ensures consistency and accountability. GCC should have a governance structure that defines how the IT strategy aligns with the business and academic strategies to ensure that the College achieves its goals as well as methods to measure IT performance. Governance ensures that all stakeholders' interests are accounted for and that processes provide measurable results.

  An IT governance framework that is implemented well should provide key insights into how the IT department is functioning, what key metrics management needs, and IT's return on investment. A well-evolved IT governance framework will assist with:

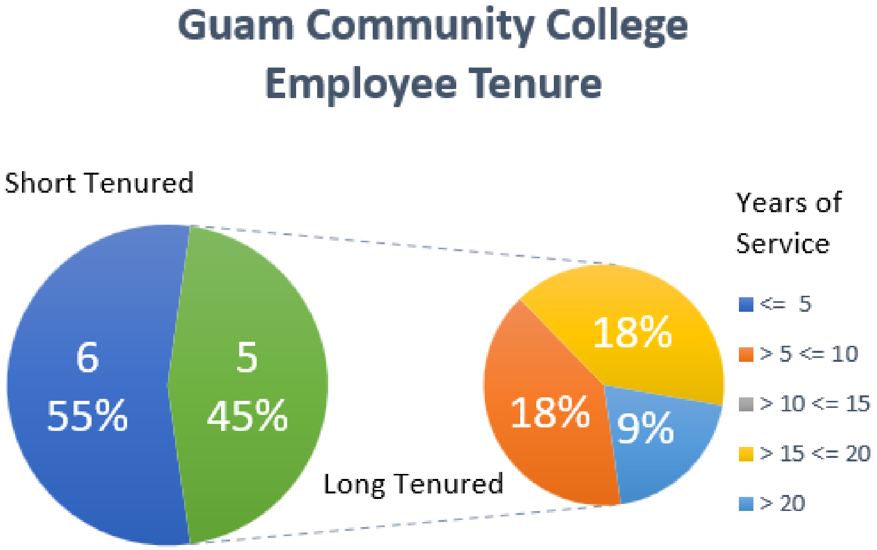
  - Aligning IT with the organization's goals and strategy
  - Enhancing project and portfolio management and alignment with the College's strategy
  - IT risk management
  - Institutional strategic planning
  - Performance measurement
  - Implanting IT into the culture of the institution
  - Demand management (e.g., demand for IT's services by college departments)
  - Optimizing IT operations
  - Increasing project visibility
  - Raising the profile of IT

- Academic & Administrative Computing Strategy: Reconsider removing (1) Academic Computing and (2) Instructional Technology responsibilities from MIS and consider how all IT at GCC can be better coordinated and led. The more compartmentalized IT responsibilities become and are spread around the college the greater the chance that the college will not benefit from economies of scale and experience higher IT costs and a reduction to service quality. The purpose of an IT organization is to improve the capability to cost-effectively manage the College's resources and serve the academic and administrative needs of faculty, students, staff, and administration. Strategically managing investments in academic and administrative computing while paying attention to both the human and technological dimensions of how they change over time will result in higher satisfaction of the constituents that use them and enable data-driven decisions.

Organizational Model and People

OBSERVATION: Challenges faced by the MIS workforce threaten the effectiveness of the department and its ability to deliver high-quality IT services.

The MIS Department at GCC is fast approaching the precipice of revolutionary change. The existing organizational structure, which was designed without consideration as to moving systems to the cloud, distance learning, or the rise of Anything-as-a-Service (XaaS - the delivery of services over the internet, rather than provided locally), would impact the department as well as the College. The MIS organization of today (See Appendix A) was designed with the intent of efficiency and effectiveness but resulted in a somewhat standalone and siloed department structure with no established cross discipline teams to involve functional users.



Further, though the College is presently served by a tight knit and competent group, there are many challenges for the future that include:

- The tenure of the existing IT staff is very disproportional with 55% (6 EEs) considered as short tenured. According to Indeed and other sources, Employees that have worked for a company for more than five years are considered long-tenured employees, while those that have worked for a company for less than five years are considered short-tenured employees. Employees with longer tenure are often valued because they have adapted to an organization's culture and have a strong understanding of the policies and processes, which results in increased productivity. Additionally, 27% (3 EEs) have greater than 15 years of service, which depending on the employee could have them qualify for a higher paying civil service position outside of GCC or even retirement. The college has no staff within the sweet spot of 10 – 15 years of tenure.

- Existing job descriptions and the actual skillsets of the staff are greatly mismatched. Though by statute some positions (termed Academic Personnel) at the college are exempt from Guam Civil Service Commission, only the CITO falls into this exempt classification with the rest of the MIS group being subject to the Commission. These positions were written in the 80's and 90's and do not reflect the technology landscape of today.

- Though a compensation/wage study was not part of this assessment, staff perceptions compared to data obtained from Openpayroll.com could indicate that GCC employees under Guam Civil Service may be paid less than other Guam Civil Service employees and both classes are paid less than non-civil service employees. This can result in the potential that GCC could be serving as a training ground for the 55% short tenured employees who could leave for higher paying and better qualified jobs outside of GCC.

- Due to the MIS department's modest size, there is a lack of upward mobility paths into more senior classifications, or management/leadership positions.

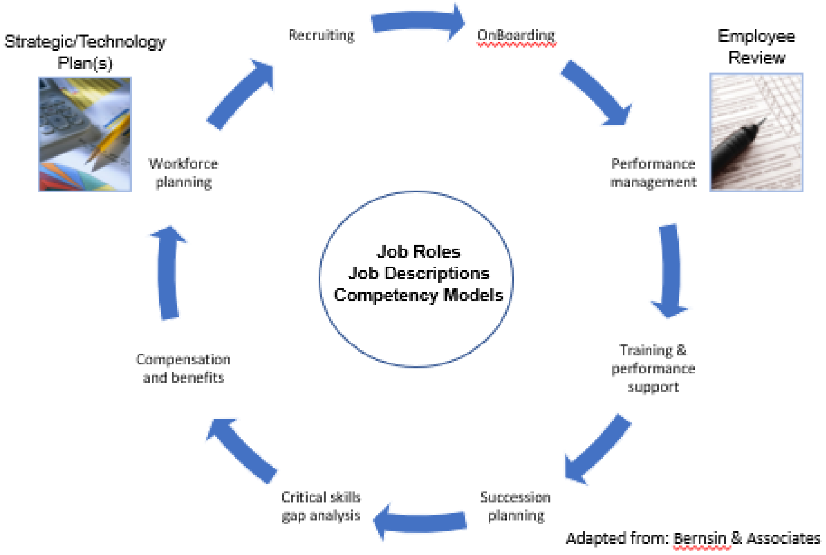
RECOMMENDATION: Begin the process of aligning the MIS organizational structure with a view toward the College's future needs by designing and implementing a talent management program for ITS.

Ideally, the long-term MIS structure should not be hurried, but rather done in conjunction with the development of the Technology Plan and with the involvement of all constituents. Principles that should be taken into consideration include:

- <u>Organize for speed, agility, and adaptability:</u> Efficiency and effectiveness do not need to be sacrificed in order to address the ever-changing digital transformations of higher education.
- <u>Authority and accountability are one in the same:</u> An imbalance of authority and accountability will only lead to challenges and frustration, which impact efficiency and effectiveness.
- <u>Exploit the power of teams:</u> Designing for adaptability requires a shift away from traditional hierarchical structures to models in which work is accomplished in teams, often cross-functional teams.
- <u>Leverage service delivery synergies:</u> Focus on customer desires, not just their needs to recognize crossover where it exists, and design accordingly.

RECOMMENDATION: Design and implement a talent management program for ITS.

Talent management (TM) is a strategy that will enable MIS to plan for, attract, retain, and develop employees. To function properly, it must be totally integrated into the MIS culture. To be effective, MIS leadership and management must go beyond the organization's technology needs and include employees' individual needs. When implemented strategically and consistently, a talent management program lays out where the organization is going, so every employee can see where he or she fits within the department. TM is an ever-evolving process that has eight components:



Adapted from: Bernsin & Associates

1. Workforce Planning (from the GCC Strategic and Technology Plans)
2. Recruiting (from proper sources as well as titles that are attractive to today's employees)
3. On-boarding
4. Performance management (employee reviews with elements of 360°)
5. Training and performance support
6. Succession planning (especially with a maturing workforce)
7. Critical skills gap analysis
8. Compensation and benefits (particularly important in the territory area and its many IT companies)

In studies by the American Society for Training and Development (ASTD), high-performance organizations statistically tend to embrace talent management elements, whereas lower performing organizations do not. Further, where organizations have adopted talent management, employee morale and engagement are higher, resulting in lower turnover and absenteeism.

RECOMMENDATION: Consider "Virtual Fractional Staffing" for specialized skill sets (such as security) and leadership activities.

Fractional staffing is where employees split their full-time hours and skills across multiple employers or clients. It is invaluable for work that is highly specialized but hiring a full-time staff member to perform it isn't warranted. Additionally, the COVID-19 pandemic has proven that many of these specialized skill sets can be performed remotely. There are many companies that offer continuously trained & certified virtual fractional (and full-time as well) staffing support.

GCC is at a point where virtual fractional staffing could be of great benefit to the institution in the areas of security and executive leadership. Targeted areas would include those roles which are important, but are not urgent such as security planning/implementing/monitoring (Chief Information Security Officer – CISO), project manager (PM), and policy, governance, budgeting, strategizing, etc. (CITO). This could make it possible to hire a director to manage the department and focus more on improving customer service.

MIS Operations and Planning

OBSERVATION: The most current adopted and documented technology plan is outdated and is more aspirational (with refutation) than a workable plan.

The document titled "Information Technology Strategic Plan – Enterprise Architecture (ITSP-EA) Update – Year 2017" was characterized as being the most recent Technology Strategic Plan. Reviewing the document, it appears to lack many of the attributes of a typical IT plan, was not consistent with staff interviews about IT at the college and is greater than 3 years old. The document references three "*concerns expressed by the visiting team in 2012 regarding resources under Standard III.C. Technology*" with the remainder of the document walking through updated strategic goals and how five of the goals are 100% completed. Many of the items cited have been completed, but interviews suggested that many were not completed or at least have not been carried forth since 2017. Examples cited include MIS staff training & development, funding, policies & procedures among others.

RECOMMENDATION: Develop a disciplined 3-Year Technology Plan for GCC.

The purpose of this technology assessment is to assist in the updating of the 2017 plan.. However, this recommendation is to suggest that future planning should depart from the planning practices of the past and be more purposeful than aspirational. Technology Planning is a leadership and management organizational process that is used to analyze the current state of technology, determine goals and objectives, set priorities, and define the resources necessary to deliver high-quality technology and services to the institution. It can deliver the following benefits to GCC:

- Provide clarity, direction, and focus for ITS: The plan's primary purpose is to connect the MIS organization's mission and vision to the College's educational planning (to include distance education) by addressing these three questions:

  1. What is the purpose of MIS? (Mission)
  2. What does MIS want to achieve in technology, staffing and support? (Vision)
  3. How is MIS going to get there? (Plan)

- A proactive rather than reactive MIS organization: Planning enables the organization to foresee future trends and obstacles and prepare accordingly. During the planning process, MIS can anticipate undesirable scenarios before they happen and take the needed precautions to circumvent them. With a strong plan, MIS can be proactive rather than reacting to the day-to-day business fires and other unanticipated situations as they arise.
- Better organizational alignment and employee engagement: Staff participation in the planning process fosters employee engagement, collegiality, and an opportunity for dialog on the direction of the MIS organization. Improving employee engagement also helps ensure everyone is on the same page when it comes time to execute the plan and empowers them to make better decisions in the best interests of the plan and its goals.

- Increased operational efficiency: Having a clearly articulated strategy provides management the roadmap to align the organization's functional activities to achieve the desired goals. A plan that is well written, with defined projects, dues dates, and deliverables, enables the staff to understand the big picture and plan for what is to be accomplished and by when, thus improving operational efficiency.

OBSERVATION: The College should adopt modern Information Technology management and governance practices.

Focusing on MIS operations should be equally, if not more important, than focusing on the technology alone. After all, even the well-managed use of dated technology can be more effective and positively impactful to the College than using leading-edge technology that is managed poorly. There are a number of modern IT governance and management practices that, when used to serve as controls, can achieve positive outcomes. The assessment found the following lacking:

- IT Governance: At present, the College has two unofficial advisory groups. One that provides input to MIS and the other consists of faculty who discuss teaching and learning technologies. These groups provide non-binding but informed guidance and recommendations on specific or ongoing issues. They also provide a positive impact on the organization as a whole, and IT in general, as they help build credibility and support for the IT organization, bring a functional perspective/knowledge/learning into IT, and create a brainstorming forum for problem solving.
- Policies and Procedures: This isn't to reflect negatively on the existing policies and procedures, but rather to suggest that they are incomplete and need to be expanded upon.

RECOMMENDATION: Working with the college senior staff and existing College governance processes, establish the technology governance structure necessary to support and transform the institution.

In order to take the existing advisory structure to the next level, establishing a technology governance process to prioritize, fund, and monitor technology initiatives would increase awareness, engagement, and communication about enterprise-wide technology projects as well as help with:

- Institutional strategic planning and aligning IT with the College's goals and strategy
- Project and portfolio management and increased project visibility
- Raising the profile of IT in a positive way and implant IT into the culture of the institution
- Optimizing IT operations and managing service demand
- Performance measurement
- IT risk management

Properly designed and implemented, the IT demand governance component (i.e. what MISshould work on) will provide a process by which the College can ensure the effective evaluation, selection, prioritization, and funding of competing IT investments, oversee their implementation, and validate measurable benefits. The IT service delivery governance (i.e. how MIS should do what it does) is further enhanced by the remaining practices below.

- IT Portfolio and Service Catalog - Information Technology Service Management (ITSM): Determining and communicating exactly what services MIS will deliver to the College is an integral component to the IT Service Delivery Program and impacts both IT demand and service delivery. IT service management can be characterized as adopting a process that focuses on customers' needs for IT services rather than the IT systems, with a focus on continual process improvement. Working inside the governance structure, it first starts with the development of a portfolio of services that is eventually refined to a catalog that clearly defines what consumers of IT can expect from ITS. This catalog of services is constantly updated by adding and removing services as dictated by the College's needs through the governance process.
- IT Service Delivery Program - ITIL or COBIT (or some combination thereof): Information Technology Infrastructure Library (ITIL) and Control Objectives for Information and Related Technologies (COBIT) are perhaps two of the more popular systems used for controlling and monitoring IT service delivery in higher education. Sometimes utilized together (in whole or in part), these frameworks offer guidance for effective management of IT services. COBIT is a methodology that targets the oversight of general IT processes, reducing costs and risk and establishing and maintaining privacy standards. ITIL, on the other hand, has a focus on service quality management, rather than technology, with a goal of delivering higher quality, reliable, more unified/standardized services. Developing a good service delivery program could easily integrate elements from both COBIT and ITIL and would greatly improve IT services at the College. Key elements of the program would also include performance metrics and service level agreements.

  For additional information on ITIL: https://www.axelos.com/best-practice-solutions/itil/what-is-itil

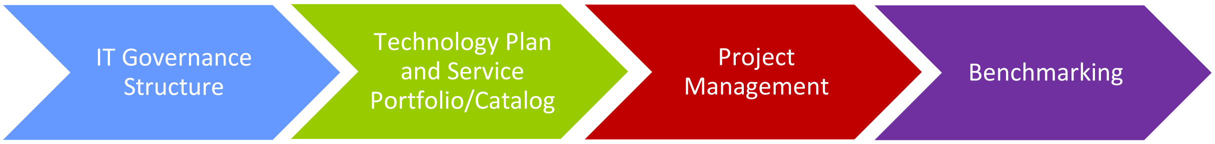
  For additional information on COBIT: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

- Project Management (PM) and Project Management Office (PMO): Project management is necessary to ensure proper expectations are set around what is to be delivered, who is to perform what tasks, by when, and at what cost. Further, it provides a feedback mechanism that delivers routine updates to all stakeholders as to project progress and can signal when a project is not going as planned. Working with both IT and the functional units, an effective project manager can negotiate reasonable and achievable deliverables, deadlines and milestones across stakeholders, IT teams, and leadership Given the number of active projects at any given time (12-15) and across multiple locations, for MIS to be successful project management must become systemic to the entire department and college wide. One aspect of the limited IT governance structure is the lack of a GCC PMO function that provides strong project leadership and maintains a project portfolio that is prioritized by the governance structure and managed to completion through the PMO.

- Change Management: The College does not have a formal change management process that would provide the means for effective discipline through communication and collaboration. The College systems are integrated applications that require effective integration of processes, communications, and resources. The lack of a change management system typically leads to a silo approach to project efforts.
- Benchmarking: Organizations from all different industries use benchmarking to gauge their successes and identify their shortcomings. Benchmarking is the process of studying the college's practices, organization, governance, functions, software portfolio, metrics, etc. as they relate to IT and then compare them with peer and aspirational organizations. As part of the assessment, Ellucian identified four potential peer institutions with the intent of surveying them for benchmarking them for the assessment (see Appendix B). However, due to time constraints, and receiving only one response, useful benchmarks were not able to be obtained. Nevertheless, those identified (and new peers) should be useful for future benchmarking projects.

  The overall objective of benchmarking is to identify problem areas that could be better and to improve performance, service satisfaction, and reduce costs both inside and outside of IT. In addition to the peers identified, a suggested / recommended first benchmarking project would be to participate in the upcoming Educause Core Data Services (CDS) survey. EDUCAUSE began the Core Data Service in 2002 with the goal of providing the higher education IT community access to fundamental data about academic and administrative computing. As the CDS is specific to the higher education it is a logical first benchmarking exercise for GCC.

RECOMMENDATION: Develop and implement transparent IT governance and management practices.



IT Governance Structure → Technology Plan and Service Portfolio/Catalog → Project Management → Benchmarking

This recommendation cannot be implemented all at once (refer to the roadmap above). As previously stated, IT governance determines what MIS should provide to the GCC community. Governance should be at the center of developing the Technology Plan discussed above and the service portfolio and services catalog. This provides the foundation for next steps related to an IT Services Delivery Program and how services are provided leading to the introduction of formal project management into the organization. Create a PMO responsible for maintaining a project portfolio that is prioritized by the College IT Governance structure and is appropriately provided resources. The PMO will provide project management expertise, ensure alignment with GCC strategy, and manage project accountability. Create a change team to organize and build policy and structure. Formalized approval of changes and scheduling are imperative. Create a change control mechanism that consists of both functional decision makers and technical expertise. Finally, once project and change management are in place, GCC is then in a position for benchmarking for continuous process improvement.

II. Financial, Functional, Policy, and Business Continuity Observations and Recommendations

This section examines important elements at the College that impact IT but are not necessarily integral to the IT department and infrastructure. It is broken down into the following areas:

- Business and Financial Management
- Functional Operations
- Business Continuity

Business and Financial Management

OBSERVATION: Key IT assets are primarily acquired using capital expenditures (CapEX) and not operational expenditures (OpEX)

Based upon interviews and budget analysis, it would appear that the majority of critical IT infrastructure is acquired with one-time (1x) "opportunistic" funding (i.e. switches, routers, Wi-Fi access points, etc. being acquired upon the construction of a new building, or CARES Act funding. Unlike many of the components of physical infrastructure, IT infrastructure has a shorter period of vendor support and equipment useful life. As there is no obsolescence planning for IT infrastructure, this has resulted in much of the College's switches, routers, and other networking equipment outdated and unsupported. This presents a significant risk to GCC which is discussed further below.

RECOMMENDATION: Consider leasing IT infrastructure equipment, taking it from CapEX to an OpEX expenditure.

GCC has demonstrated that it is moving many of its IT expenses to OpEX with its adoption of several software as a service (SaaS) projects. Obsolescence planning for aging IT infrastructure can also be moved to OpEX by moving to the leasing of equipment. From a funding perspective the benefits of a leasing vs. 1x buying IT equipment include:

<u>Lower Upfront Expense</u> – Outright purchasing equipment, needs a lot of money up front which may not be possible depending upon financial resources. Leasing enables the College to still obtain the equipment, while spreading the investment across multiple years. This is very attractive in such situations where infrastructure such as switches, wifi, etc. is being expanding or upgraded.

<u>Predictable Annual Hardware Costs</u> – In addition to reducing the initial cash outlay, switching to a model where IT equipment is leased will make costing more predictable. This is especially important in situations where the institution faces uncertainty, as has been the case with the COVID-19 pandemic, where many schools have students, faculty and staff in a remote working environment. Leasing options can span multiple years (2, 3, 5,8, etc.), spreading equipment costs over the life of the lease. By adopting this approach, equipment cost are switched from unpredictable and substantial up-front costs, to much more predictable annual/monthly costs, making them much easier to budget for.

<u>Equipment Upgrades Become Simpler</u> – Perhaps the largest problem with purchasing IT

equipment up-front is that it depreciates and becomes obsolete quickly. This is especially true for laptops, printers, computers, network gear and other similar devices.
Leasing IT equipment makes upgrading easier because you lease the most up-to-date equipment. Effectively, a lease passes the burden of obsolescence onto the lessor and not the college. When the lease expires, the school is free to take out a new lease, obtaining the most up-to-date equipment in the process as suppliers stock the most up-to-date equipment.

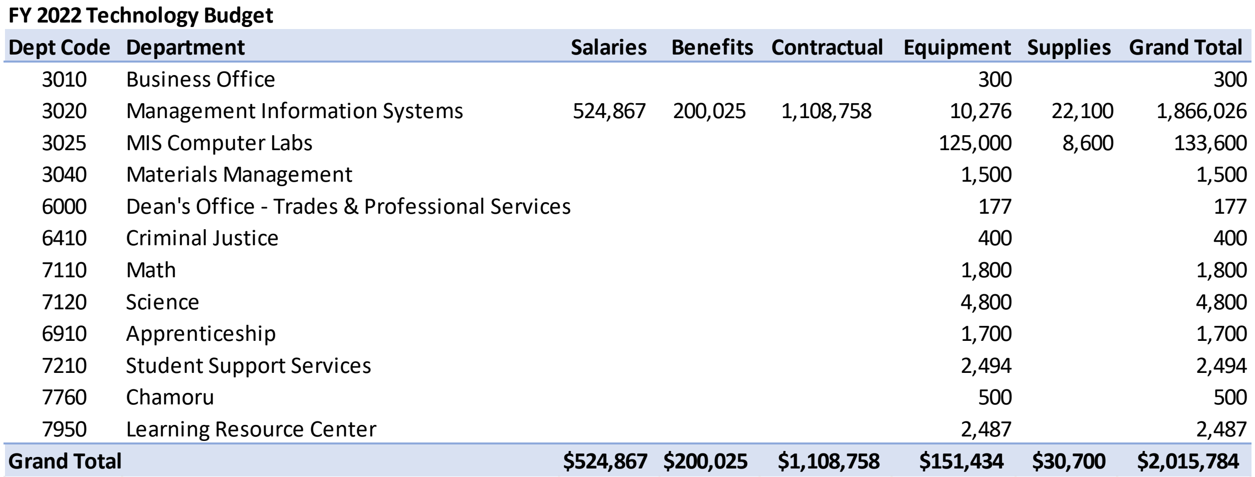
Access to Better Equipment – In addition to allowing the college to upgrade regularly, it may be able to gain access to a higher quality/standard of equipment than buying the equipment up-front. When the coronavirus pandemic set in and colleges and universities were being forced to work and teach remotely, many schools were in a situation where they suddenly needed to provide students, faculty, and staff with access to hardware such as laptops for example. By spreading these costs out over a period of years, many of the institutions were able to buy better hardware than they would have if they were paying up front.

Built-In Maintenance and Disposal – Another major advantage of leasing IT equipment the avoidance of maintenance or repair costs that are typically associated with buying equipment outright. This is because most leasing companies bundle in these protections as part of the agreement. So, if a piece of equipment goes wrong, the lessor will retrieve and fix it, or they will replace it. Depending upon how the agreement is structured, some leasing companies will allow the institution to purchase the equipment for a nominal cost, or they will bear the cost of disposal.

There is a precedent at GCC for leasing as evidenced by the current multi-functional printing devices lease.

OBSERVATION: There is no formal cost structure or budgeting process in ITS, and the budgeting that does occur is somewhat in disarray and haphazard.

For the assessment, a technology budget summary along with the budget detail were analyzed. The summary (below) lists the expenditures by department:



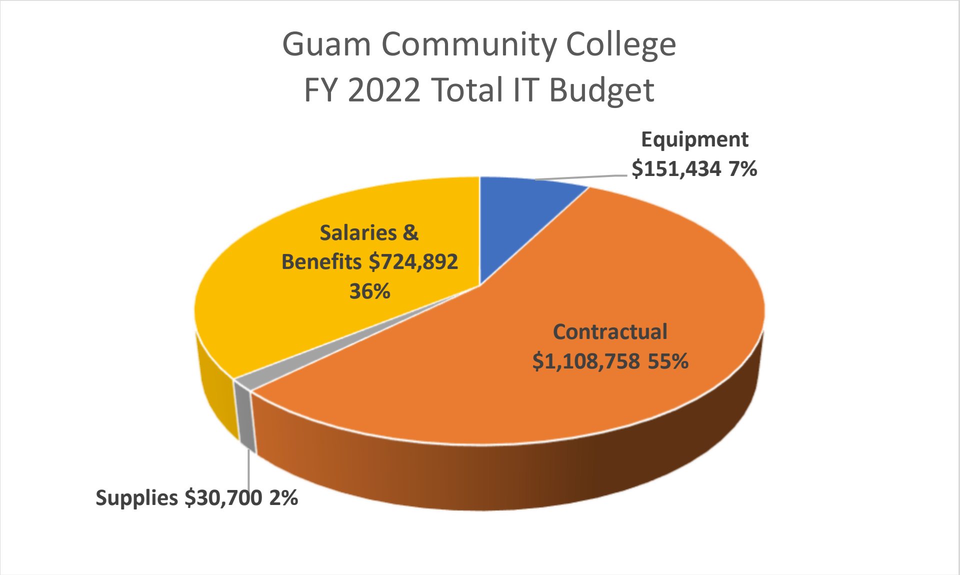
FY 2022 Technology Budget

Dept Code	Department	Salaries	Benefits	Contractual	Equipment	Supplies	Grand Total
3010	Business Office				300		300
3020	Management Information Systems	524,867	200,025	1,108,758	10,276	22,100	1,866,026
3025	MIS Computer Labs				125,000	8,600	133,600
3040	Materials Management				1,500		1,500
6000	Dean's Office - Trades & Professional Services				177		177
6410	Criminal Justice				400		400
7110	Math				1,800		1,800
7120	Science				4,800		4,800
6910	Apprenticeship				1,700		1,700
7210	Student Support Services				2,494		2,494
7760	Chamoru				500		500
7950	Learning Resource Center				2,487		2,487
Grand Total		**$524,867**	**$200,025**	**$1,108,758**	**$151,434**	**$30,700**	**$2,015,784**

Outside of the MIS department (Code 3020), most of the equipment costs are for end-user type devices such as tablets, laptops, desktops, instructional equipment and the like. Those expenses that are "Contractual" consists primarily of SaaS expenditures, software maintenance, and other recurring IT expenses that serve the GCC enterprise. MIS also has an equipment budget of $125K for computer lab equipment. All told, only 1% of the total IT expenditures are budgeted outside of the MIS department.

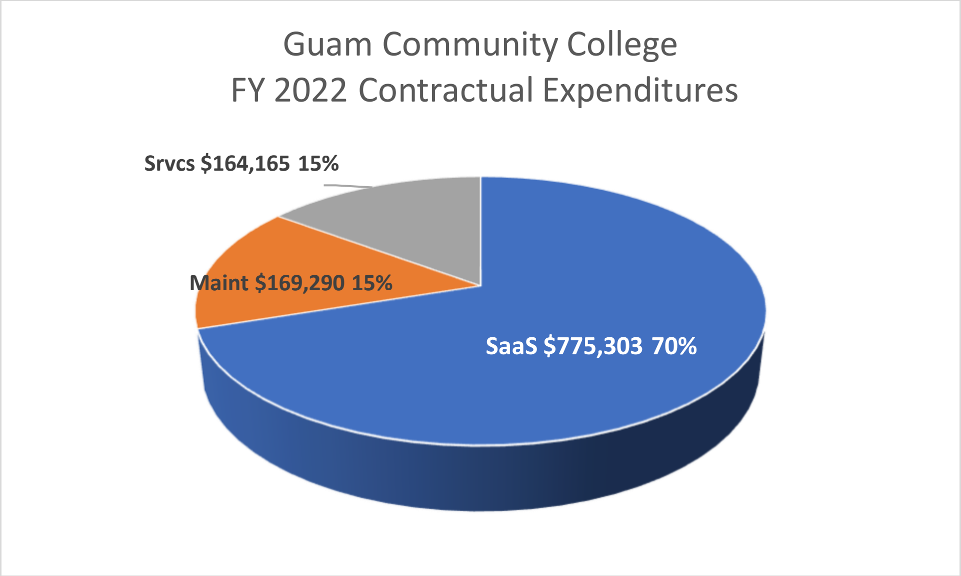
Of the $2,015,784 total budgeted for technology in 2022, the expenditures across the enterprise break down as follows:

Equipment	$151,434
Contractual	$1,108,758
Supplies	$30,700
Salaries & Benefits	$724,892
	$2,015,784



Contractual obligations that include SaaS, software maintenance, and remote services accounted for $1,108,758 which is 55% of the total budget. This breaks down as follow:

SaaS	$775,303
Software Maintenance	$169,290
Remote Services	$164,165
	$1,108,758



This means that overall SaaS comprises 39% of the total IT budget at GCC and 42% of the total MIS department budget (excluding the MIS computer lab budget).

No other prepared budgeting materials were discoverable or made available that would indicate how the funds are distributed across the various areas of the department, the total cost of ownership (TCO) of major projects (e.g., Banner, networking), or the annual delivery costs for IT services. Taken in its entirety, the budget is indicative of an IT organization that is not proactively monitoring current technology expenditures to proactively predict future funding needs.

RECOMMENDATION: Consider studying the total cost of ownership of major projects and activity-based budgeting.

In order to control cost and predict future funding requirements, it is important to understand where every dollar is being spent, escalation factors, and past contingencies. Total cost of ownership (TCO) and activity-based budgeting (ABB) are two methodologies that can be employed to monitor and control costs.

TCO differs from price in that it is an analysis of the complete cost of a major system (such as Banner) over the anticipated lifecycle of the system. This TCO considers every phase and aspect of ownership, which includes but isn't limited to hard costs—such as software purchases, hardware, maintenance, licensing, etc.—and soft costs—such as change management, documentation, and training.

Activity-based budgeting (ABB) involves accounting for the cost of the activities necessary to deliver IT service to the college community and their associated costs, rather than the traditional budget that describes cost factors (e.g. expense codes), such as computer supplies (CODE), travel (CODE), maintenance & repair (CODE), telephone (CODE), etc. This provides the transparency to determine which activities need investment, outsourcing, or even discontinuation.

ABB is more complex than TCO, which is necessary to determine ABB, so it is best to embark upon ABB after the College has a firm grasp of the major IT systems' lifecycle costs.

Functional Operations

OBSERVATION: The importance of aligning IT technology with the functional requirements should be a major consideration.

Though out of scope for this technology assessment, it is important to focus on the functional areas across the organization that are served by MIS. The best technology coupled with poor processes and user experiences will not meet the institutions desired objectives. A study with representatives from across the functional operations areas would ensure that IT is fully enabling the organizational operations. The functional assessment would identify any barriers that could be mitigated using Process Reimage and Redesign techniques to expand the use of existing technology.

RECOMMENDATION: Consider a Process Reimagine and Redesign effort with a focus on the constituent experience.

To effectively leverage technology the college owns, it is imperative to continually rethink policy, process, procedure, and overall output, to ensure the efforts of the teams across the college are working most effectively and integrating across the college collaboratively. Today the GCC Banner system contains customizations throughout the system, including back-office functions and self-service, some of which can be supported by delivered Banner 9 functionality. These customizations impede upgrades and patching, require additional effort to test the application, and train staff, without measurable value for the added efforts.

A Process Reimagine and Redesign effort with a focus on the constituent experience is needed to optimize Banner to effectively address the College's unmet needs. Acknowledging the College's current state and resource constraints, Ellucian proposes an approach that gains incremental improvement semester over semester for the student experience and quarterly improvements for the administrative experience, which would focus more on finance, human resources, payroll, and other non-student facing services. The following visual depicts the recommended approach with some key improvement areas identified.

This approach would be designed to address the priorities established by the College and work to incrementally improve the constituent experience on a semesterly basis, driving ongoing and continuous improvement each semester.

OBSERVATION: The Service Desk needs improvement.

Interviewees indicated that the self-maintained Service Desk could be more responsive and lacks a sense of urgency. Issues often require multiple requests, and the time to resolution is often measured in weeks. There is no obvious prioritization of service desk tickets. A request was made to the Service Desk for a complete Excel or CSV listing of all tickets, both closed and open, but no listing was provided.

RECOMMENDATION: Implement new Service Desk and establish Service Level

Agreements (SLAs).

Create a team to identify new Service Desk options for the College to consider. It will be important for this team to establish Service Level Agreements (SLAs) for various types of service requests and then measure performance against those SLAs in a way that is transparent to the GCC community. Additionally, consideration must be given to the implementation of a new Service Desk ticketing solution that will enable the ability to easily create, route, and monitor tickets via multiple channels.

OBSERVATION: Limited website utility for supporting IT at the College.

GCC web presence is provided by GuamWEBZ, a local web design and development company that specializes in website development and website management. Content is at the direction of the Public Information Office with guidance from a Website Committee, and Andrew Marquez from MIS provides limited support.

In exploring the GCC website, it would appear that the site is designed primarily for attracting and serving students, provide news & events, and other general information. Though there is some limited information about IT at the college (e.g., device specifications for distance learning on the distance learning page and contacting MIS on the MIS main page). There is no direct link for IT support off the home page or quick link. Additionally, the department's name is Management Information Systems (MIS) which is confusing in the academic community.

RECOMMENDATION: Define requirements for web presence and use it to augment current processes.

Students, as well as faculty and staff, require IT support as well. Work with the Website Committee to make the website more useful as an IT support resource. Suggestions for improvement include many of the items discussed in this report, but are not limited to:

- Link to the helpdesk/MIS main page on the home page, or at least the quick links
- Add end user policies and procedures (e.g., Acceptable Use, Printer Usage, Social Media Policies and Guidelines, Copyright Infringement Complaint, etc.)
- Instructions and Training (Security awareness, applications use, IT resources available, etc.)
- Recommended equipment and standards
- Catalog of services
- IT Governance, advisor meetings and minutes
- Change Management protocols
- Ideas and suggestions
- Rebrand the MIS department. Management Information Systems (MIS) is typically the name of an academic department. Ideas would be: Office of Technology Support, College Technology Support Group, Office of Technical Services, Information Technology and Services, or other appropriate name

OBSERVATION: Opportunities exist to formalize institutional IT policies across multiple domains.

GCC does its best to address IT policies and procedures as needed, which is very reactionary and many times are created due to new issues that require immediate attention, example: Social Media Policy. As discussed generally in Section I of this report, GCC would greatly benefit from modern IT management practices such as those outlined in ITIL and COBIT. Specifically, opportunities do exist to formalize institutional IT policy across multiple domains in this arena, including the following:

- IT policy and documentation: MIS is lacking policy and procedural documentation which puts the College at risk for consistency, succession training, disaster recovery, and failure to perform best practices.
- IT Budgeting Policy: Non-IT departments are currently able to procure technology assets and do not always pursue adequate analysis or coordination with IT for acquisition and support.
- Systems patching (operating system and applications): Systems patching is an ad hoc process. There are no formal maintenance windows or schedules for production systems patching and maintenance.
- Production discipline: MIS needs a formal, documented process for defining, building, and testing technical constructs and moving them to production. The absence of a documented process also impacts system security since access and permissions are not defined.

RECOMMENDATION: Formalize key areas of the IT enterprise operation to begin creating consistency and reducing risks.

- Create a team to identify needed IT policy and documentation, Prioritize the needed outcomes, and accelerate the creation of the required policies and documented procedures. Consider using COBIT, ITIL, and peer institutions as sources for best practices.
- Create a GCC policy that requires technology budgeting and acquisition through IT.
- Create a database management and upgrade/patching policy that defines database purpose, sequencing for applying and testing upgrades and patches, and also provides for compatibility analysis. This is not only important from an operational perspective but also increases security as the majority of data breaches are attributed to poor patch management. An effective policy must include a comprehensive network inventory, risk categorization, testing and auditing, along with compliance reporting. The College needs to establish a regularly scheduled production release window.

Business Continuity

OBSERVATION: Windows 2003 production servers are end of life.

GCC has one server using Microsoft Windows Server 2003 operating system (OS) used for network file-sharing. Microsoft officially ended its support of Windows 2003 and production servers are endo of life. Microsoft has also ended its support for Windows Server 2008. Planning has yet to occurred to migrate any unsupported operating systems to a supported one.

RECOMMENDATION: Complete a server inventory.

Complete a thorough server inventory with server description, IP address, server age, OS, applications, and compatibility requirements (OS vs Apps) and determine priority, virtualization, disposition date, and responsibility.

OBSERVATION: No Business Continuity Plan exists.

While we did not directly ask any respondent if the College has a Business Continuity Plan, it seems evident from the minimal documentation and inventory of systems that no effective Business Continuity Plan exists.

RECOMMENDATION: Develop a Business Continuity Plan.

The College needs to begin a comprehensive program to identify critical components required to construct a Business Continuity Plan and assign tasks and completion dates. Due to the complexity and current state, it is essential and warranted to employ an external resource.

III. Technology Infrastructure and Operations

This final section of the assessment looks at the technology infrastructure at the college and its present state. Equipment age, security and strategy are analyzed in the following areas:

- IT Data Center
- Networking and Communications
- Cybersecurity, Risk, & Compliance
- Security and Risk Management

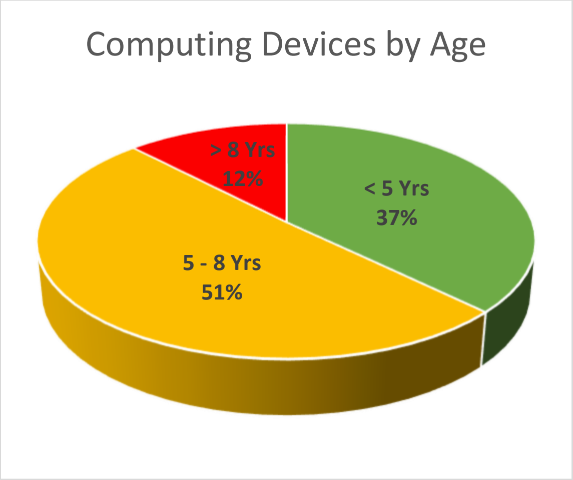
IT Data Center and Infrastructure

Based upon multiple interviews regarding the on-premise data center, it is very lacking. It was shared that on premise servers were not well protected, there is a lot of deferred maintenance, the generators don't work, and since moving Banner to the cloud it's more of a storage area than a data center.

OBSERVATION: End-of-life infrastructure and asset management.

GCC has a number of data switches between the datacenter and intermediate distribution frame (IDF) closets, many of which are 10 plus years old and are end-of-life and end-of-support. Depending upon the equipment, anything in service for less than five years is considered to be in good condition (green). As the equipment passes year five, there is a warning (orange) that the college's needs will grow past what the gear is capable of due to such items as Wi-Fi expansion, new buildings, and the adoption of high bandwidth applications. Original equipment manufacturers' (OEM) support and warranties can also come into play in this time frame. Over 8 – 10 years the equipment can become a danger (red) as security concerns of the older equipment grows, technical and upgrade support wanes, and maintenance costs rise.

A brief analysis of the IT inventory provided by GCC's is presented in the graphic below, noting that 63% of the equipment is in the orange or red timeframes.



While they are largely operational, failure would make troubleshooting them difficult as they are unsupported. The College's risk is increasing as these devices are critical in keeping the environment connected and operational. A switch failure will result in downtime for the portion of the network impacted. Additionally, there are a mix of wireless access point models in the environment today. The older models have aged to the point of only supporting legacy technologies impacting user experience. While there is an effort to replace the older models, the priority of this effort and the current status were unclear.

There are notable limits as to how well GCC can determine if the assets are safely decommissioned once end-of-life is reached. This could lead to access to sensitive data, theft, and duplicative future purchases.

RECOMMENDATION: Develop and maintain an asset inventory and lifecycle schedule.

Formally develop and maintain an inventory of all infrastructure assets (e.g., switches, access points, routers, firewalls, servers, etc.). The asset inventory should align with the National Institute of Standards and Technology (NIST) 800-53 (PM-5) framework. Multiple solutions are available such as Microsoft SCCM, ManageEngine, BMC, ServiceNow, etc.

Develop a lifecycle schedule to replace end-of-life devices that includes a budget cycle, communication strategy alerting the campus community regarding any planned downtime, and staff resourcing to complete the upgrade. The communications should consider the academic calendar to avoid downtime during critical periods.

OBSERVATION: Lack of infrastructure monitoring tools.

A variety of infrastructure monitoring and administration tools are in use today in order to monitor the network's performance and reliability and manage the environment. The primary software tool in use is InterMapper with other low or no cost systems. There are unique and overlapping functionalities between the tools currently in operation, which could likely be reduced without losing required functionality.

RECOMMENDATIONS: Document requirements and select monitoring tools.

The network and systems teams should formally review and document the specific requirements for monitoring the information systems, including inbound and outbound traffic to detect performance, stability, and security-related events. Best practices and cybersecurity framework (CSF) NIST 800-171 should be followed. No devices on the network should be end-of-life or on older versions of firmware. Documented requirements should be used to streamline the selection of industry standard monitoring tools encompassing all needs. All monitoring tools that do not serve a unique function should be retired from use.

OBSERVATION: No baseline configurations.

MIS does not employ consistently configuration management or standard baseline configurations today. Servers, networking devices, and other hardware devices on the network are configured in an ad-hoc manner each time they are set up, with some prebuilt templates used for virtual servers. This results in inconsistent configurations, troubleshooting complexity, security concerns, and performance and stability issues due to lack of standardization and testing of each configuration.

RECOMMENDATION: Establish and maintain a minimum standard configuration.

Ellucian recommends that the institution establish and maintain a minimum standard configuration for all infrastructure devices and formalize the policy and process in compliance with the NIST 800-53 (CM-8) and NIST 800-171 (3.4.1, 3.4.2) CSF. This standard can then be used as the foundational start for all new systems and network devices being configured.

OBSERVATION: General IT infrastructure housekeeping needs attention.

As the assessment was performed completely remote, this observation is based entirely upon secondhand information provided by the staff. Similar to the on-premise server room, the general IT networking infrastructure has physical security and environmental issues that should be addressed. In addition to potential theft and/or vandalization, unsecure physical access to network equipment closets, cable pulls, etc. provides attack vectors for breaking into the College network. And again, poor environments (heat, dust, humidity, etc. can take a toll on equipment and battery backup life.

RECOMMENDATION: Conduct environmental assessments in each closet and data center.

Conduct a comprehensive environmental assessment for each closet and data center, ensuring proper cable management (e.g., wire trays, cable management on racks, Velcro ties, etc.), each rack has an electrical ground, and UPS is installed for all devices and systems. Use the assessment to create an action plan, including the funds, staffing resources, and timeline needed to complete the improvements. Taking these steps will help ensure minimal disruption to the learning experience and critical back-office operations.

Networking and Communications

OBSERVATION: Guam Open Research and Education Exchange (GOREX) has great promise, but its utility for Guam Community College remains to be seen.

GOREX is a Research and Education Network (REN) exchange point that interconnects National Research and Education Networks (NREN's) in the Asia-Pacific region to the global Research and Education network fabric. It is not a commercial Internet exchange point. GOREX is managed and administered by the University of Hawaii (UoH), with the University of Guam functioning as the remote hands for GOREX for any onsite work needed. UoH also manages its own Pacific Islands Research and Education Network (PIREN), which “peers” or connects with GOREX and other RENs.

When asked of GCC: “What key initiatives are planned by Guam Community College to address the information technology challenges” the #1 response was peering with the Guam Open Research and Education eXchange (GOREX) project. Though there is a lot of promise that GOREX will eventually improve GCC’s networking capabilities, they are not there yet. When asked, the UoH manager of GOREX questioned how GCC may fit into the mold of the GOREX model.

With respect to expanding distance learning programs, though the high speed of a REN may result in faster access to cloud-based resources for the college, the most important choke point for the distance learner is the last mile connectivity that the student has to their place of study, which is usually their home. This “last mile” refers to the physical network connectivity speed that the commercial ISP delivers to the student’s home, which in isolated areas of Oceania could be quite slow. Joining GOREX will not have any impact on the last mile problem.

RECOMMENDATION: Explore and champion peering and other REN services opportunities for GCC.

Research and education networks (RENs) started out as specialized Internet service providers dedicated to supporting the needs of the research and education communities that they serve. Distinguished from commercial Internet providers, they provide a high-speed backbone network, offering dedicated channels for individual research projects.

However, in recent years RENs have started offering other services such as colocation and storage and peering arrangements with commercial services.

Peering permits two networks to connect and exchange traffic directly without having to pay a third party to carry traffic across the commercial Internet. Peering arrangements that would be beneficial to GCC would include (1) the learning management system (LMS) Moodle, (2) Amazon Web Services (AWS) for the Banner system, (3) Google services and any other cloud-based system that the College uses.

OBSERVATION: The college firewall solutions do not support next generation security features, posing a security breach threat that needs to be addressed.

The College’s existing firewall(s) are dated, approaching end-of-life (EOL) and do not support next generation security features. These “next gen” features would greatly enhance the capability of the College to prevent the more sophisticated cyberattacks that are emerging. With the recent departure of CITO, who also served in the capacity of the IT security lead, developing a security plan and strategy should become a priority.

RECOMMENDATION: Develop a comprehensive IT security strategy that leverages the most modern security practices and transcends merely replacing the existing firewalls with the most recent models.

Based upon staff interviews, this observation has already been recognized by the MIS group. However, the strategy moving forward should go beyond the traditional model of acquiring newer hardware and managing it locally. There are many new emerging security technologies that should be considered in developing the proposed new strategy including hardware authentication, user-behavior analytics, data loss prevention, deep learning, and cloud.

As more organizations use the cloud for what has traditionally been on-premises IT, approaches to security are being moved to the cloud as well. Called endpoint protection platforms (EPPs) they are an integrated suite of endpoint protection technologies that include antivirus, data encryption, intrusion prevention, and data loss prevention. EPPs detect and stop threats at the endpoint.

At present, Ellucian Managed Services (EMS) is recommending the EPP CrowdStrike to its partner schools as part of their strategy. CrowdStrike offers a cloud-native cybersecurity platform that stops breaches and secures organizations of all shapes and sizes.

OBSERVATION: Primary public DNS is hosted on premise.

GCC's public domain name system (DNS) is currently hosted using 2 on-premises advertiser servers. This means that the institution is particularly susceptible to DNS outages and vulnerable to attacks that will impact multiple Tier 1 services, such as the guamcc.edu website, email, among others, including the college's cloud services. DNS failure could also affect other critical internet-based services like active directory and remote desktop services. A third party (GoDaddy) provides a backup should the campus DNS be shut down, but it is unclear how or how long the switchover would work should the campus DNS fail due to a double denial of service (DDOS) or other outage.

RECOMMENDATION: Migrate primary DNS to a cloud DNS-as-a-Service platform.

Domain Name System (DNS) can be equated to the "phonebook" of the Internet. People access web information online through domain names, like, guamcc.edu, guam.gov, or amazon.com. Web browsers like Microsoft Edge and Google Chrome interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources. DNS hosted on campus provides a single point of failure. Cloud DNS-as-a-Service platforms are highly available and scalable. The return on investment (ROI) is high with little out-of-pocket expense. This will position the institution to ensure critical services remain available because:

- DNS service providers have large-scale DNS networks with many different points of presence (PoP). They can automatically accelerate the queries by sending them to the closest PoP, which ensures that student, faculty and staff can always access your web assets.
- Providers are hardened with multilayer security to protect from all types of DNS attacks. Additionally, they have a full team of certified security professionals.

From a security and maintenance perspective, cloud-based DNS will enable the college to retire the existing on-premise DNS servers. This removes two security attack vectors and eliminates the need for any future maintenance on them.

The Guam Open Research and Education eXchange (GOREX) discussed above in this report may present opportunities to have an off-campus DNS provider.

Cybersecurity, Risk, & Compliance

Network penetration testing is an invaluable tool for finding obvious and blatant IT security vulnerabilities at an organization. Reading the penetration test report dated 14 July 2020 would indicate that the engagement did exactly that and accordingly, each finding in the report needs be addressed. However, these types of tests have inherent shortcomings such as:

- Type of Test – Penetration tests are characterized as white and black box tests. A white box is one where some background information as well as system information is available, whereas a black box is one where only the company or school name is known. The latter type of test is preferable because it best simulates how a "bad actor" would approach breaching the school. For the most recent test, the company performing the test also conducted the two previous tests and had a specified range of IP addresses, so this would best be categorized as a white box test.

- Resources & Scope – Due to resource constraints, usually in the form of cost, penetration testing becomes limited in scope. Consultants are paid for their time whereas bad actors or hackers are not. Subsequently, testing is only conducted on the infrastructure that the client deems to be the most important. In this case, the specific IP range of 203.215.52.0/22 was specified resulting in only specific elements being tested.

- Resources & Time – Another major limitation related to scope is that of time. Again, consultants come at a cost, so the amount of time allotted to conduct testing is constrained. In this case the testing was performed from June 15 - 26, 2020. On the other hand, hackers have plenty of time and typically plan out their attacks carefully over months and even years.

- Attack Position – A final limitation that penetration testers face is that the testing access is limited to particular environments, or models from which it is presumed hackers might operate from. Since the penetration tests are limited to certain models, they are quite fallible. Hackers can diversify their position and vary their attack vectors significantly.

The observations and recommendations that follow the remainder of this section along with earlier suggestions related to network security and equipment are intended to address the inherent weaknesses of penetration testing and their impact.

OBSERVATION: The existing College cyber liability insurance policy lacks both in depth of what's covered by the policy, as well as coverage amounts. Further, the definitions & exclusions of coverage are so detrimental to the insured (GCC), it's debatable if the college could ever collect.

As understood by Ellucian, the aforementioned penetration testing is one of the requirements for the college to renew its cyber liability insurance. Accordingly, it was appropriate to perform a strict review of the insurance contract and the following short comings were interpreted:

- What's covered – As an example there would seem to be no coverage for "ransomware" and other common risks that a college would typically be subject to.
- Coverage amounts – On a per incident basis, coverage wouldn't come close to the college's potential liability for areas of the contract.
- Definitions – Are so ambiguous that any covered issue could be litigated for quite some time.

RECOMMENDATION: Explore other cyber liability insurance options while renegotiating with the existing insurance carrier.

The existing cyber liability insurance policy in its breadth and width has a lot of grey that can only be to the detriment of Guam Community College. The contract should be renegotiated while looking for other stronger underwriters.

OBSERVATION: Lack of fully formalized Information Security Plan.

Cybersecurity should be governed by robust policies, procedures, and processes. GCC has not formally adopted the NIST Cybersecurity Framework or created an overarching cybersecurity plan with controls aligning to COBIT to sufficiently support the institution's holistic cybersecurity program. Additional policies, plans, standards, guidelines, and procedures per the NIST CSF need to be developed, vetted, and approved through the GCC governance process. Such documentation, (which is either not present or outdated) would include, but not be limited to, the table shown below.

RECOMMENDATION: Implement an Information Security Plan.

We strongly recommend that GCC accelerate the creation and implementation of the Information Security Plan and supporting policies, plans, standards, guidelines, and procedures per the NIST CSF along with the associated software tools. The implementation of these formalized documents will require a concerted effort by IT and institutional leadership, but it's a critical component of the College's risk management efforts. Procurement of the tools necessary to enforce the policies outlined should be given high priority as a failure to adequately protect sensitive information can quickly become an overwhelming financial burden. The cost of the PII scanning tool, for instance, is minimal with a high return on investment (ROI). See Appendix C for the Recommended Security Policies, Procedures, Standards, and Guidelines as outlined by the National Institute of Standards and Technology.

Security and Risk Management

OBSERVATION: There is a need to clearly define and publicize an IT security strategy and leadership role in conjunction with a new security policy framework.

With the departure of the most recent CITO, GCC's current level of IT security leadership is deficient and needs additional attention and support. The longer it takes to deploy a new security policy framework, the more at-risk the College is to falling victim to an attack.

- Missing security program and big picture of awareness

  - It needs to be recognized that these IT security responsibilities must be picked up, managed and conveyed to the institution as well as filling the CITO role.
  - Awareness of frameworks and controls such as the National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), General Data Protection Regulation (GDPR), Family Educational Rights and Privacy Act (FERPA), etc. have not translated into practices, procedures, plans, or policies to secure or protect GCC in a comprehensive way.
  - Infiltration and vulnerability detection tools and practices are insufficient for protecting the College.
  - The college could benefit greatly by enacting proactive security-awareness programs such as mandatory annual security awareness training, unannounced phishing testing, and other measures as part of its IT security planning.
- Compliance, standards, controls, and risk-based security focus with detailed direction and defined deliverable actions are needed to increase network-wide security.
  - Lack of collaboration around security-focused projects between teams.
  - Formal policies, procedures, and/or practices to safeguard IT could be improved upon.

RECOMMENDATION: Obtain the services of an IT security officer (or its equivalent) to lead and be accountable for IT security.

IT security is everyone's responsibility. However, someone has to be tasked with setting the expectations, defining the policies/procedures, fielding the countermeasures, monitoring the conditions and reporting on the outcomes. This can be accomplished in several ways:

- Promotion – Assigning the duties to an existing qualified employee and divey up some or all of the promoted employee's responsibilities amongst remaining staff.
- Hiring – Create and recruit for a new IT security position.
- Multiple Hybrids – That would include but are not limited to:
  - Hire a virtual fractional IT security professional (discuss previously in this document) with on-campus support from the existing staff.
  - Work with an Endpoint Protection Platform (discussed earlier in this section) and an on-campus resource or virtual fractional IT security professional.

Regardless of the direction selected, there will be a party with the responsibility for bringing consensus, policies, and practices together to safeguard GCC. A key part of the security role is to collaboratively communicate a unified message and vision for all cybersecurity programs and drive the security culture across the entire organization.

Key outcomes for both the security program and role are to support the adoption and implementation of industry best practice cybersecurity frameworks, such as NIST 800-171 and NIST 800-53 controls, which higher education institutions are asked to comply with by the Federal Student Aid (FSA). These frameworks support new federal rules intended to better safeguard sensitive and protected information—Controlled Unclassified Information (CUI). This will ensure proper emphasis is placed on such risks throughout the College.

OBSERVATION: Security policies, procedures, and practices for creating a cybersecurity aware culture at GCC are inadequate.

Currently, GCC does not have security awareness training program for end users. Security information received by end users is emailed reactively to phishing email scams that were already impactful to faculty and/or staff. The College does not have a simulated phishing message platform to elevate and validate end user awareness of fraudulent email messages. Phishing email messages are a key method by which fraud is perpetrated against organizations, and phishing awareness programs are proven to be effective in helping to combat this issue.

Additionally, no proactive awareness communications are occurring (e.g., posters, social media posts, training, newsletters, digital signage, workshops, etc.). The consequences are not clearly defined for faculty and staff members that place GCC assets at risk electronically—until the security policy framework is deployed.

Human deficiencies, as related to cybersecurity, cannot be overstated. In almost every instance, humans are the biggest security risk to an organization. This is generally due to lack of education on basic security practices. Often, staff do not even realize that they have a role in security, let alone what their role *actually is* in the complex and ever-changing world of cyber risk. Often, they cannot be persuaded to care without increased awareness. Properly safeguarding personally identifiable information (PII; a term used to describe data elements, such as social security numbers and credit card numbers) is something that is the responsibility of all that have access, but often users don't even understand the risks they may be taking from activities such as basic data exports to Excel. A single breach from a simple phishing email can end up costing millions of dollars, as many other higher education breaches have proven.

Lack of compliance with proper security policies, procedures, and practices could also result in failed audits, penalty fees, data breaches, data manipulation, and increased legal, financial, and reputational risk.

RECOMMENDATION: Develop a formal information security management system (ISMS).

IT leadership should commence developing formal information security management systems:

- An overarching cybersecurity plan outlining the detailed cybersecurity framework, policies, procedures, standards, and plans.
- Fully implement an information security awareness program:
    - Develop policies to support the procedures and frequent practices to raise awareness of responsibility for personal technology among all staff and students. Deploy frequent enterprise phishing educational tests to faculty and staff.
- IT security policies, plans, procedures, and practices should be developed and implemented to minimize risk, maximize compliance requirements, and ensure data security while following NIST 800-171 CSF, ISO controls, HIPPA requirements, FSA requirements, FERPA, GDPR standards, etc.

OBSERVATION: Onboarding, role-based access, vendor, and third-party security management programs need development.

Technology and cloud vendors with access to sensitive College data assets are not currently required to complete a security assessment survey to determine if their organizations adhere to best practices.
Non-disclosure agreements for employees, third parties, and vendors is lacking and inconsistent:

- Employees do not receive onboarding non-disclosure agreements or annual cybersecurity education, which increases the institution's risk of a data breach.
- For vendors, a formal policy supporting secure practices, such as the implementation of non-disclosure agreements (NDA), background checks, certifications, etc. was not consistent. All vendors that have any access to GCC information should be operating under a common set of policies that ensure consistency across the institution and maximizes data protections.
- Job role changes are handled on an ad-hoc basis. In the event an employee transfers to another office, their permissions may remain the same due to the lack of process and regular audit.

Disclosing confidential information without written responsibility increases the institution's liability. Any abuse of access will increase the liability for the institution as a whole with fewer consequences available against the individual violator.

RECOMMENDATION: Formalize policies and procedures for all existing and new employees, third parties, and vendors working for the College.

GCC leadership, in conjunction with legal counsel, should confirm their non-disclosure agreements (NDA) comply with the below NIST and ISO cybersecurity framework references. All cloud providers and vendors engaged presently or in the future for activities with access to college data assets need to complete a vendor security assessment survey. Formalize policy and procedures for all existing and new employees, third parties, and vendors working for the College to safeguard the institution and its assets, including an HR workflow for role changes. This recommendation is aligned with ISO 13.2.4, NIST SP 800-53 PL-4, PL-6, SA-9, and PR IP-11.

OBSERVATION: Backup and data retention policies and practices may be insufficient.

With the 2018 migration of the Banner ERP system from being on-premises at the GCC campus to the cloud as a software as a service (SaaS) offering, multiple security concerns were addresses. Nevertheless, data in Banner does get stored locally, and student recruitment data can be accumulated locally prior to its being input into Banner. As stated earlier in this report, functional review is outside of the scope of this assessment. However, given the importance of Federal Student Aid, it is suggested that the retention policies and backups are reviewed to ensure they are adequately aligned with compliance requirements and industry practices. Specifically ensure that:

- Adequate retention periods are clearly defined to comply with Federal Student Aid (FSA), territory, and government requirements.
  - Per the FSA School Eligibility and Operations 2017–2018 manual, a school must keep records relating to a student or parent borrower's eligibility and participation in the Direct Loan or FFEL program for three years after the end of the award year in which the student last attended the school. A school must keep

    all other records relating to the school's participation in the Direct Loan or FFEL program for at least three years after the end of the award year in which the records are submitted. https://ifap.ed.gov/fsahandbook/attachments/1718FSAHbkVol2Ch7.pdf

- Ensure NIST 800-171 3.8.9 and NIST 800-53 CP-9 compliance requirements for data safeguarding and backups are being met.
    - The protection of controlled information is of paramount importance and can directly impact GCC's ability to carry out business operations.
    - Local data/drive encryption is taking place on any backup server and there are standards in place to classify encryption data types needed. NIST 800-53 PR.DS-1, PR.DS-2, & PR.DS-6.
- Backups are being validated and tested on a regular basis as part of a procedure or policy to ensure quality.

This applies for both data that is being stored locally and in the cloud as the risk is the lack of FSA audit compliance, compliance fees, loss of Title IV Federal funding, possible data loss from inadequate practices, increased liability, and college brand damage. GCC should take risk mitigating measures to ensure onsite and cloud data repositories are secure and in compliance with the standard discussed above.

RECOMMENDATION: Align backup practices, procedures, and policies with higher education standards, policies, and controls.

Align backup practices, procedures, and policies with higher education standards and NIST 800-171 3.8.9 and NIST 800-53 CP-9 policies and controls to protect and preserve student data for at least the minimum required records retention period (e.g., 3 years to 7 years). Refine local backup processes improving backup frequency, replication locations (offsite data), validation processes, and consider cloud storage for long-term local archival purposes. Ensure that there is a singular view of these policies and that they are enforced for all systems, (including GCC's ERP SaaS provider) regardless of system location.

OBSERVATION: Privileged access management and Multi-Factor Authentication (MFA) at GCC are not in use.

Privileged access management (PAM) controls and approaches are absent. Identity theft is more prevalent today than ever and without multi-factor authentication in place, it becomes an even more attractive target for hackers. Successful breaches are on the rise due to weak or compromised credentials. Aside from the financial liability of a breach, the brand damage and/or possible data corruption can negatively affect the institution.

It is important to note that Ellucian has noticed that continental US (CONUS) cyber liability insurance underwriters are not renewing existing or underwriting new institutions that do not use MFA. This trend will most likely extend to colleges and universities outside the continental US (OCONUS). So, GCC being an OCONUS institution should plan for this possibility.

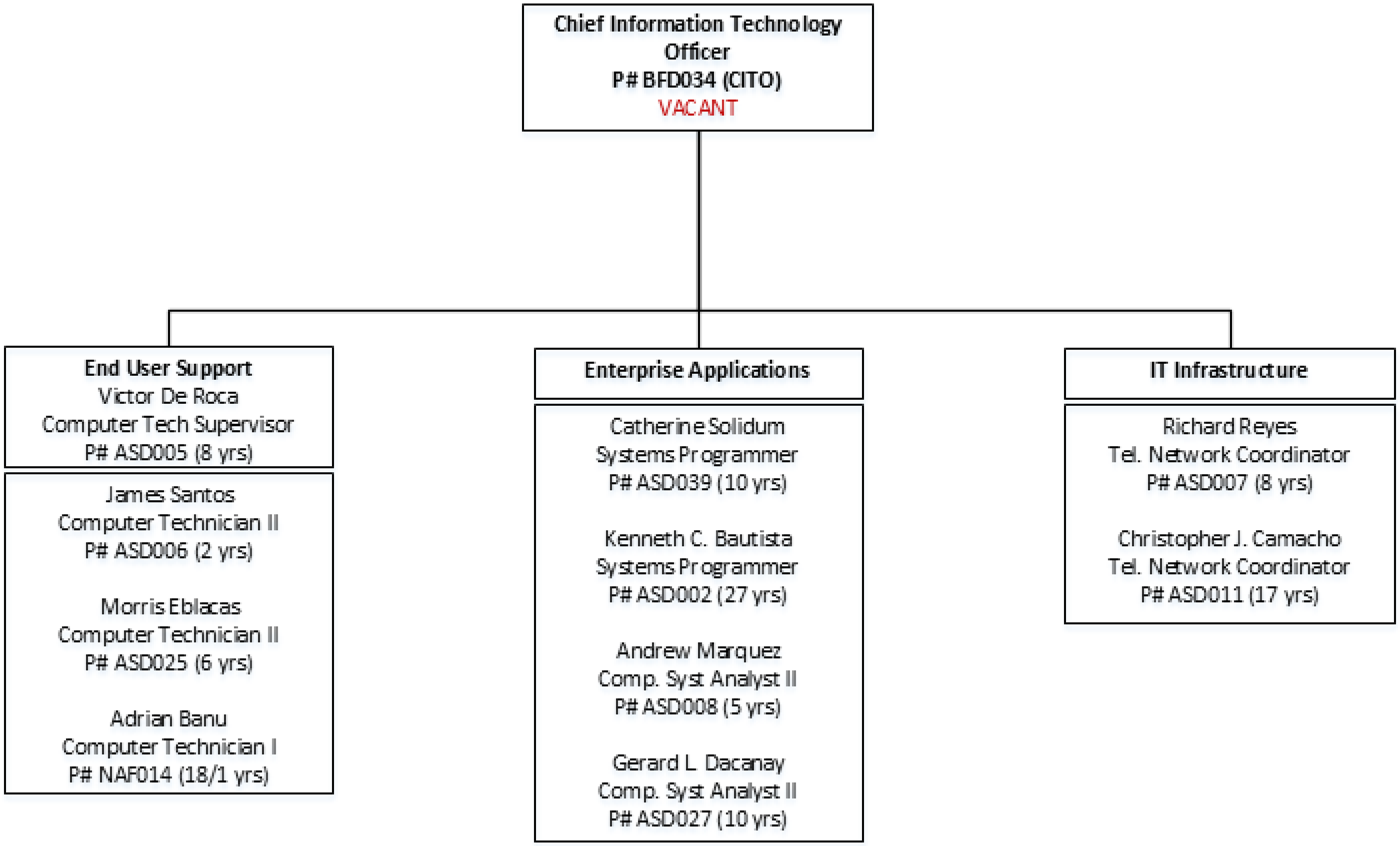
RECOMMENDATION: Enable multi-factor authentication.

Enable the use of multiple-factor authentication for local network access to privileged accounts and for network access to non-privileged accounts. For example, all users including faculty and staff, should have MFA-enabled for Gmail and MyGCC portal access. Align GCC authentication and identification practices to NIST 800-171 3.5.3, 3.5.4 control areas with supporting policies, procedures, and logical controls.

Next Steps

Taken in total, these observations and recommendations represent a collective set of improvements that would bring GCC from an organization that is relatively reactive in nature to one that is strategic and operating at the highest levels of organizational maturity. As a practical matter, this journey will not be taken in one step, but will be comprised of a series of strategic shifts carefully orchestrated by an integrated leadership team with an increasingly robust governance and change capability. As a key enabler to the enterprise strategy, MIS will benefit from the next step of IT strategic planning exercise. The Ellucian team anticipates that GCC will also accrue benefits from this report to the broader leadership, organizational maturity, and constituent experiences across the institution.

Appendix A: GCC IT Organizational Chart



Chief Information Technology Officer
P# BFD034 (CITO)
VACANT

End User Support
Victor De Roca
Computer Tech Supervisor
P# ASD005 (8 yrs)

James Santos
Computer Technician II
P# ASD006 (2 yrs)

Morris Eblacas
Computer Technician II
P# ASD025 (6 yrs)

Adrian Banu
Computer Technician I
P# NAF014 (18/1 yrs)

Enterprise Applications

Catherine Solidum
Systems Programmer
P# ASD039 (10 yrs)

Kenneth C. Bautista
Systems Programmer
P# ASD002 (27 yrs)

Andrew Marquez
Comp. Syst Analyst II
P# ASD008 (5 yrs)

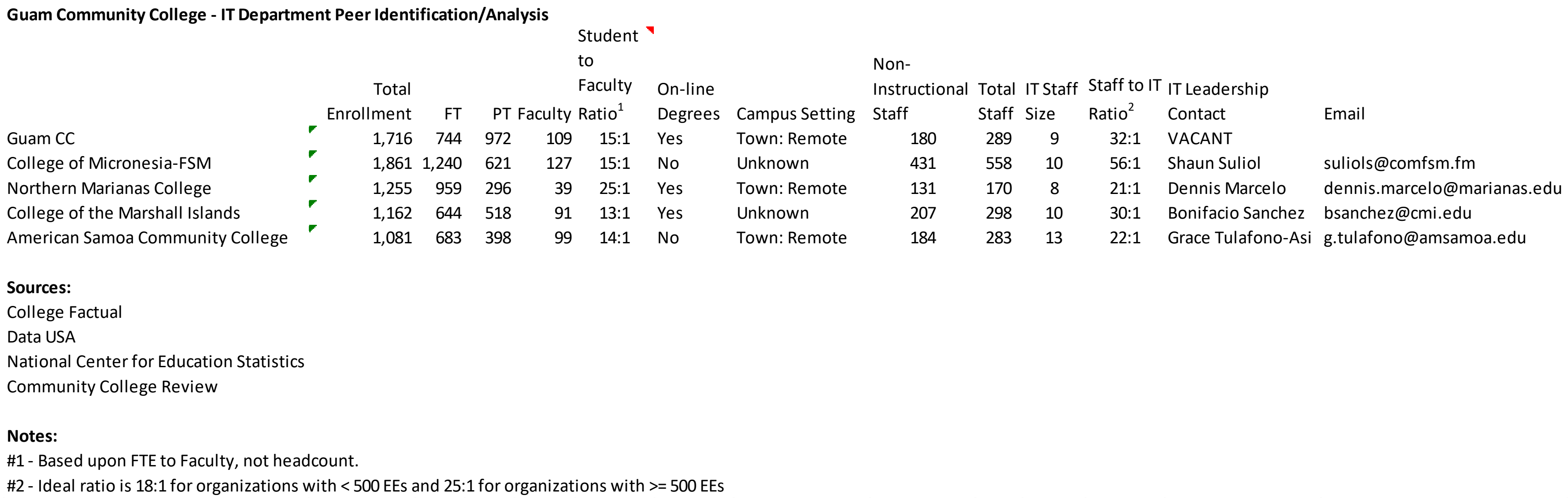
Gerard L. Dacanay
Comp. Syst Analyst II
P# ASD027 (10 yrs)

IT Infrastructure

Richard Reyes
Tel. Network Coordinator
P# ASD007 (8 yrs)

Christopher J. Camacho
Tel. Network Coordinator
P# ASD011 (17 yrs)

Appendix B: GCC IT Peers



Guam Community College - IT Department Peer Identification/Analysis

	Total Enrollment	FT	PT	Faculty	Student to Faculty Ratio[1]	On-line Degrees	Campus Setting	Non-Instructional Staff	Total Staff	IT Staff Size	Staff to IT Ratio[2]	IT Leadership Contact	Email
Guam CC	1,716	744	972	109	15:1	Yes	Town: Remote	180	289	9	32:1	VACANT	
College of Micronesia-FSM	1,861	1,240	621	127	15:1	No	Unknown	431	558	10	56:1	Shaun Suliol	suliols@comfsm.fm
Northern Marianas College	1,255	959	296	39	25:1	Yes	Town: Remote	131	170	8	21:1	Dennis Marcelo	dennis.marcelo@marianas.edu
College of the Marshall Islands	1,162	644	518	91	13:1	Yes	Unknown	207	298	10	30:1	Bonifacio Sanchez	bsanchez@cmi.edu
American Samoa Community College	1,081	683	398	99	14:1	No	Town: Remote	184	283	13	22:1	Grace Tulafono-Asi	g.tulafono@amsamoa.edu

Sources:

College Factual
Data USA
National Center for Education Statistics
Community College Review

Notes:

#1 - Based upon FTE to Faculty, not headcount.
#2 - Ideal ratio is 18:1 for organizations with < 500 EEs and 25:1 for organizations with >= 500 EEs

Appendix C: Recommended Security Policies, Procedures, Standards and Guidelines

Description	NIST SP 800-53
Information Security Policy	controls from all families
Acceptable Use Policy	AC-1 Access Control Policy and Procedures
	IA-1 Identification and Authentication Policy & Procedures
Governance	AC-1 Access Control Policy and Procedures
	IA-1 Identification and Authentication Policy & Procedures
	AR-1 Governance and Privacy Program
Social Media Policies and Guidelines	controls from all families
Compliance	controls from all families
Peer-to-Peer File Sharing	controls from all families
Copyright Infringement Complaint Procedures	controls from all families
Access Control	AC-1 Access Control Policy and Procedures
	IA-1 Identification and Authentication Policy & Procedures
Awareness & Training	AT-1 Security Awareness and Training Policy and Procedures
Audit & Accountability	AU-1 Audit and Accountability Policy and Procedures
Assessment	RA-1 Risk Assessment Policy & Procedures
	PM-5 Information System Inventory
	CA-2 Security Assessments
Applications Assessment/ Evaluation Guide	controls from all families
OWASP (The Open Web Application Security Project) Testing Guide	controls from all families
Configuration Management	CM-1 Configuration Management Policy and Procedures

Data Classification Standard	RA-2 Security Categorization
Server Standard	RA-2 Security Categorization
Smart Phones and Mobile Storage Device Standard	RA-2 Security Categorization
Contingency Planning	CP-1 Contingency Planning Policy and Procedures
Identification & Authentication	AC-2 Acct Management
	IA Family
Electronic Signatures Policies and Procedures	IA-5
Password Standard	IA-5
Incident Response	IR-1 Incident Response Policy and Procedures
Security Breach Notification Policy	IR-1 Incident Response Policy and Procedures
	SI-5 Security Alerts, Advisories, and Directives
Incident Response Procedure	IR-1 Incident Response Policy and Procedures
	SI-5 Security Alerts, Advisories, and Directives
Incident Response Policy	IR-1 Incident Response Policy and Procedures
	SI-5 Security Alerts, Advisories, and Directives
Incident Management Policy	IR-1 Incident Response Policy and Procedures
	SI-5 Security Alerts, Advisories, and

	Directives
Maintenance	MA-1 System Maintenance Policy & Procedures
Media Protection	MP-1 Media Protection Policy & Procedures
Physical/Environmental	PE-1 Physical and Environmental Protection Policy and Procedures
Physical Security - Data Center	PE-1 Physical and Environmental Protection Policy and Procedures
Planning	PM-9 Risk Management Strategy
	PM-11 Mission/Business Process Definition
	SA-14 Criticality Analysis
Planning	PM-9 Risk Management Strategy
	PM-11 Mission/Business Process Definition
	SA-14 Criticality Analysis
Personnel Security	PS-1 Personnel Security Policy and Procedures
Pre-employment Screening	PS-1 Personnel Security Policy and Procedures
System & Services Acquisition	SA-1 System and Services Acquisition Policy & Procedures
Systems Acquisition	SA-1 System and Services Acquisition Policy & Procedures
Applications Assessment/ Evaluation Guide	SA-1 System and Services Acquisition Policy & Procedures
Business Procedures	SA-1 System and Services Acquisition Policy & Procedures
Systems & Communications	AC-4 Information Flow Enforcement

	SC-1 System and Communications Protection Policy and Procedures
Network Policies	AC-4 Information Flow Enforcement
	SC-1 System and Communications Protection Policy and Procedures
System & Information Integrity	SC-1 System and Communications Protection Policy and Procedures
Digital Certificates Policy	SC-1 System and Communications Protection Policy and Procedures
Cellular Devices	SC-1 System and Communications Protection Policy and Procedures
Applications Assessment/Evaluation Guide	SC-1 System and Communications Protection Policy and Procedures
OWASP (The Open Web Application Security Project) Developer Guide	SC-1 System and Communications Protection Policy and Procedures