# TABLE OF CONTENTS

## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>About Enterprise Risk Management</td>
<td>2</td>
</tr>
<tr>
<td>The ERM Process</td>
<td>4</td>
</tr>
<tr>
<td>Enterprise Risk Assessment Results Summary</td>
<td>5</td>
</tr>
<tr>
<td>Enterprise Risk Assessment Heat Maps</td>
<td>6</td>
</tr>
<tr>
<td>Enterprise Risk Mitigation Overview</td>
<td>9</td>
</tr>
<tr>
<td>Physical Space Constraints Risk Mitigation</td>
<td>11</td>
</tr>
<tr>
<td>Information Security Risk Mitigation</td>
<td>15</td>
</tr>
<tr>
<td>Perceptions of Campus Security Risk Mitigation</td>
<td>20</td>
</tr>
<tr>
<td>Workflow Process Risk Mitigation</td>
<td>25</td>
</tr>
<tr>
<td>Funding Formula Risk Mitigation</td>
<td>28</td>
</tr>
<tr>
<td>The ERM Process in 2014 and Beyond</td>
<td>32</td>
</tr>
<tr>
<td>Contact Information</td>
<td>33</td>
</tr>
<tr>
<td>Appendix A: University System of Georgia Risk Management Policy</td>
<td>A-1</td>
</tr>
<tr>
<td>Appendix B: Key Risk Assessments</td>
<td>B-1</td>
</tr>
</tbody>
</table>
Executive Summary

Georgia State University operates in a risk environment of growing uncertainty. To assist the University and its academic and administrative leadership in visualizing, assessing and mitigating the risks that threaten its mission, the Office of Enterprise Risk Management (ERM) was tasked with creating a sustainable process to identify, assess, and manage risks across the enterprise to ensure attainment of key organizational objectives and avoid surprises. The process for ERM shall be implemented in a manner consistent with the Board of Regents of the University System of Georgia Risk Management Policy attached as Appendix A.

In connection with its vision and mission, the Office of Enterprise Risk Management is pleased to present the Georgia State University 2013 Enterprise Risk Management Annual Report. The Office of ERM has helped University leadership identify, assess and mitigate enterprise risks through the following process:

**Risk Identification** – This phase consisted of facilitated sessions with over 60 academic and administrative leaders across all areas of the University. In these sessions, University leadership was asked to identify what they viewed as the key risks to the University achieving its strategic objectives. From these sessions, over 80 separately identifiable risks were selected for further assessments.

**Risk Assessment** – This phase consisted of facilitated group sessions with over 90 University academic and administrative leaders. In these sessions, groups identified the likelihood and potential impact of each of the identified risks. Based on these results and further consultation with leadership, the Office of ERM and the University selected five key risks (in no particular order) to further mitigate in 2013 as follows:

- Physical space constraints impede Georgia State University from accomplishing its strategic objectives;
- Georgia State University users fail to protect University data;
- Georgia State University constituents have poor perceptions of campus safety and security;
- Workflow processes are either too cumbersome or non-existent, leading to inefficiencies; and
- Georgia State University would be adversely affected by not maximizing the availability of appropriations under the funding formula.

**Risk Mitigation** – Based on the results of the Assessment phase, primary risk owners for each key risk and its relevant sub-components were identified and potential mitigating activities were documented in accordance with the procedures laid out by the Board of Regents of the University System of Georgia. These results are attached to this Annual Report as Appendix B. The Office of ERM worked with the primary risk owners to begin and/or complete the actions contained in this report.

**Conclusion and Outlook** – The Office of ERM is confident that Georgia State University maintains a robust program to manage enterprise risks and was pleased at the high level of cooperation and assistance of the University and its leadership in the further analysis and improvements to its risk management culture in fiscal year 2013. Moving forward into fiscal year 2014, Georgia State University will build on the work contained and finalize the mitigation steps in various stages of implementation. Furthermore, Georgia State University will select additional key risks identified in the assessment to further analyze and mitigate.
About Enterprise Risk Management

WHAT IS ENTERPRISE RISK MANAGEMENT (ERM)?

Enterprise Risk Management is a process-driven tool that enables senior management to visualize, assess, and manage significant risks that may adversely impact the attainment of key organizational objectives. The Office of Enterprise Risk Management works within the University community to create a sustainable process to identify, assess, and manage risks across the enterprise to ensure attainment of key organizational objectives and minimize uncertainty.

WHY IS ERM IMPORTANT?

- **Survivability**: Unmanaged risks can destroy or severely damage people, institutions, reputations, or careers.
- **Accountability**: The Board of Regents and external stakeholders expect Georgia State University to manage risk.
- **Freedom**: Knowledge that risks are managed frees University management to focus on long-term strategic goals, objectives, and initiatives.
- **Expectations**: Proactive risk management is a bottom-line expectation from the Chancellor, the Board of Regents, the President of the University and the public.

VISION

The Office of Enterprise Risk Management seeks to enable an effective framework for Georgia State University to evaluate and prioritize its institutional risk mitigation activities. Successful implementation of an enterprise risk management framework can enhance the opportunities to advance organizational objectives.

MISSION STATEMENT

The Office of Enterprise Risk Management will facilitate the visualization, assessment and management of enterprise risks and facilitate the creation of processes and control points to mitigate identified institutional risks. The Office of Enterprise Risk Management will enable Georgia State University to balance risk across the enterprise by having a point of reference to view and evaluate risk and a common methodology for addressing risks.
E RM GOALS

- Conduct and facilitate enterprise risk assessments, focusing on the likelihood and impact of institutional risks;
- Present results of risk assessments to leadership and provide recommendations for further risk mitigation efforts;
- Ensure the implementation of Enterprise Risk Management processes consistent with the Board of Regents University System of Georgia Risk Management Policy; and
- Improve controls, processes and training to maximize risk management and identify areas where additional risk may be assumed.
The ERM Process

PHASE I – ENTERPRISE RISK IDENTIFICATION

The Director of Enterprise Risk Management facilitated brainstorming sessions across the University, learning what each college / academic support unit does and what unique risks each faces. Sixty individuals were interviewed, including representatives from every college and core administrative function.

Over 200 individual risks were identified, and 81 risks were selected to be assessed.

PHASE II – ENTERPRISE RISK ASSESSMENT

The Director of Enterprise Risk Management facilitated 17 small group risk assessment meetings. More than 90 people attended these risk assessment meetings.

Each person was asked to assess the likelihood and impact of a group of identified risks using instant response (“clicker”) technology. These meetings served dual roles of gathering data and discussing risks in a cross-functional manner.

The attendees were asked to consider each risk in light of Georgia State University’s strategic objectives, which were identified as follows:

- Become a national model for undergraduate education by demonstrating that students from all backgrounds can achieve academic and career success at high rates.
- Significantly strengthen and grow the base of distinctive graduate and professional programs that assure development of the next generation of researchers and societal leaders.
- Become a leading public research university addressing the most challenging issues of the 21st century.
- Be a leader in understanding the complex challenges of cities and developing effective solutions.
- Achieve distinction in globalizing the University.

PHASE III – RISK MITIGATION

Based on the results of the Enterprise Risk assessments, the University selected five risks with eleven components for further review and reported these to the BOR central office. A copy of these final risks and objectives reported to the BOR are attached as Appendix B. The Director of Enterprise Risk Management coordinated with key risk owners to prepare documentation of further control points to mitigate these risks and risk components.
Enterprise Risk Assessment Results Summary

After interviews and small group meetings, the Office of ERM identified the University's top 20 risks. The Overall Rank represents the responses of all attendees (likelihood x impact / 2). The Provost rank represents the overall rank of individuals who indicated they report to the Provost (excluding IS&T). Colored rows indicate the risks that were ultimately selected for further mitigation efforts during this first year.

<table>
<thead>
<tr>
<th>TOP 20 RISKS</th>
<th>OVERALL RANK</th>
<th>PROVOST RANK</th>
<th>RISK SUMMARY STATEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Appropriations Decline</td>
</tr>
<tr>
<td>2</td>
<td>7</td>
<td>7</td>
<td>Healthcare Costs</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>6</td>
<td>Education Cost</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>8</td>
<td>Staffing – Administrative</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>4</td>
<td>Financial Aid Changes</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>5</td>
<td>Retention</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>3</td>
<td>Inversion &amp; Compression</td>
</tr>
<tr>
<td>8</td>
<td>17</td>
<td>17</td>
<td>IS&amp;T User Security</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>2</td>
<td>Physical Space Availability</td>
</tr>
<tr>
<td>10</td>
<td>9</td>
<td>9</td>
<td>Perception of Safety</td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>12</td>
<td>Risk to IS&amp;T Infrastructure</td>
</tr>
<tr>
<td>12</td>
<td>14</td>
<td>14</td>
<td>Workflow Processes</td>
</tr>
<tr>
<td>13</td>
<td>10</td>
<td>10</td>
<td>Employer Subsidies</td>
</tr>
<tr>
<td>14</td>
<td>16</td>
<td>16</td>
<td>Aging Physical Infrastructure</td>
</tr>
<tr>
<td>15</td>
<td>13</td>
<td>13</td>
<td>Non-productive Employees</td>
</tr>
<tr>
<td>16</td>
<td>31</td>
<td>31</td>
<td>Hiring Efficiency</td>
</tr>
<tr>
<td>17</td>
<td>18</td>
<td>18</td>
<td>Grant Availability</td>
</tr>
<tr>
<td>18</td>
<td>20</td>
<td>20</td>
<td>Pedestrian Safety</td>
</tr>
<tr>
<td>19</td>
<td>21</td>
<td>21</td>
<td>Data Management</td>
</tr>
<tr>
<td>20</td>
<td>22</td>
<td>22</td>
<td>Training - Management</td>
</tr>
</tbody>
</table>

All assessed risks were categorized into the following five areas:

- Financial
- Compliance
- Strategic
- Reputational
- Operational
Enterprise Risk Assessment Heat Maps

The following risk profiles for each area show the likelihood of a given risk against the potential impact. It is important to note that ERM is not about eliminating all risk; rather, ERM recognizes risks cannot be avoided, but through good management, uncertainty can be minimized. By assessing risk in this fashion, University leadership can determine whether a given risk should be avoided, retained, transferred or reduced. Highlighted risks were selected for further mitigation efforts. The charts are not to scale and are edited to clearly present the information.
ENTERPRISE RISK ASSESSMENT HEAT MAPS

Risk Profile – Compliance Risks

Risk Profile – Strategic Risks
ENTERPRISE RISK ASSESSMENT HEAT MAPS

Risk Profile – Reputational Risks

Risk Profile – Operational Risks
Enterprise Risk Mitigation Overview

Based on the Enterprise Risk Assessment, consultations with University leadership and further analysis, Georgia State University selected five overall risks with eleven components for further mitigation activities. These were reported to the Board of Regents of the University System of Georgia at the beginning of 2013 (attached as Appendix B). Each risk and risk component was assigned to a key risk owner who was responsible for addressing the risks. These key risk owners are identified specifically in the section of this report dedicated to the key risk. The risks identified for further mitigation are summarized below.

**PHYSICAL SPACE RISKS**

*Risk Statements.* Physical space constraints impede Georgia State University from achieving its strategic objectives.

A. Insufficient or poorly managed availability of top quality research space negatively affects ability to recruit and retain research faculty.

B. Insufficient or poorly managed availability of top quality instructional lab space negatively affects educational offerings.

C. Aging physical infrastructure creates financial challenges to plan for repair or replacement of physical plant elements exceeding their useful lives.

D. Many schools and administrative departments are not together in similar physical locations reducing efficiencies that are possible with adjacent work areas.

**IS&T SECURITY RISKS**

*Risk Statements.* Users fail to protect University data.

A. Improper use of portable storage devices or use of non-centrally managed storage puts data at risk of being misplaced or misappropriated.

B. Users are too likely to respond to phishing attacks and provide sensitive data such as passwords.

**PERCEPTION OF SAFETY RISKS**

*Risk Statements.* Constituents of the University have poor perceptions of Campus Safety & Security.

A. Additions of visible security or other uniformed personnel will contribute to improved perceptions of security on campus.
B. Georgia State University constituents may not receive adequate marketing of the University’s actual safety causing perceptions to overcome reality.

WORKFLOW PROCESS RISKS

Risk Statements. Workflow processes are either too cumbersome or non-existent leading to inefficiencies in task completion.

A. Workflow processes are too cumbersome for certain tasks.

B. Certain processes do not have defined workflows leading to uncertainty.

APPROPRIATIONS RISK

Risk Statements. Georgia State University would be adversely affected by not maximizing availability of appropriations under the funding formula.

A. Maintaining and improving retention, progression and graduation metrics in a declining resource environment.
Physical Space Constraints Risk Mitigation

BACKGROUND AND OVERVIEW

Georgia State University is located in downtown Atlanta in a vibrant, urban setting. Accordingly, and as part of a large city, the University faces particular physical space issues that may be somewhat unique to Georgia State University as compared to other University System of Georgia member institutions. Georgia State University might be described as land-locked in the sense that geographic (no undeveloped real estate contiguous to campus) and financial (high real estate prices) constraints limit the University’s ability to expand or build new facilities. Moreover, as the University celebrates its centennial, many of its facilities are older and continue to require significant investments to be maintained and/or expanded. In light of these particular University issues, the University’s leadership together with the Office of ERM identified the following risk statements.

Risk Statements. Physical space constraints impede Georgia State University from achieving its strategic objectives.

A. Insufficient or poorly managed availability of top quality research space negatively affects ability to recruit and retain research faculty.

B. Insufficient or poorly managed availability of top quality instructional lab space negatively affects educational offerings.

C. Aging physical infrastructure creates financial challenges to plan for repair or replacement of physical plant elements exceeding their useful lives.

D. Many schools and administrative departments are not together in similar physical locations reducing efficiencies that are possible with adjacent work areas.

RESEARCH LAB SPACE QUALITY AND QUANTITY

In connection with mitigating the risks of insufficient or poorly managed research space, the Vice President of Research & Economic Development was assigned as the key risk owner and identified the following activities over the past year.

Matching Space Utilization with Research Productivity

The Office of the VP of Research & Economic Development has begun an iterative and ongoing process to better match research space with research productivity by looking at productivity on a square foot basis. Reports matching research productivity to research space utilized are updated on a regular basis to adjust for changes in productivity and/or modifications in space utilized. These quantitative reports will be used to allocate research space to the most productive primary investigators. Those primary investigators that
are less productive will have appropriate grace periods to resume their productivity or be at risk of losing some or all of their existing research space.

These productivity measures were used in part to identify the appropriate tenants of the additional Petit Science Center space expected to come on board in Spring 2015 following completion of the Petit Science Center expansion project. As further discussed below as it relates to the quality of research space, the Petit expansion project is designed for more open research lab space with multiple research teams sharing an open floor plan. This design will also allow for more research to occur on a square foot basis than it would with more traditional designs of non-shared space, increasing overall utilization per square foot of research space.

**Assessing and Adjusting Quality of Research Space**

In addition to continuing to find appropriate methods to allocate existing and expanding research lab space, the quality of research lab space was assessed to determine the best places to further invest. The end result of the quality analysis led to two primary policy changes.

First, Georgia State University will discontinue making new investments, beyond basic upkeep, into its second and third tier research lab space. Future resources for improvements and build outs will be directed to the University’s first tier research space, such as the space located at the Petit Science Center.

Second, large portions of future expansion will be completed using an open floor plan designed to have multiple primary investigators engaged in research in cohort space. This approach serves two objectives: maximizing space utilization and improving the likelihood of cross-disciplinary knowledge sharing amongst University researchers.
PHYSICAL SPACE CONSTRAINTS RISK MITIGATION

INSTRUCTIONAL LAB SPACE QUALITY AND QUANTITY

In connection with improving Instructional Lab space quantity and quality, the Senior Vice President Finance was assigned as the key risk owner and identified the following activities over the past year.

In connection with analyzing instructional lab needs, the University conducted a study. The Sasaki study identified an instructional/teaching lab space deficit of 20,000 assignable square feet. Georgia State University is currently working on concepts to develop additional instructional labs with an addition to the centrally located Classroom South building. When completed the 35,000 GSF (21,000 ASF) facility will consist of one 200 seat tiered classroom, twelve instructional labs, elevator lobby and student social space. This centrally located addition will help not only to mitigate the deficient identified in the Sasaki study but also provide state of the art instructional space. Additional instructional lab will be programmed into the proposed Science Park Phase III and Phase IV projects.

In the interim, the University is studying the feasibility of lab offerings on Friday afternoons and improving the teaching lab space utilization during the regular weekdays. The idea of Saturday lab classes will also be reviewed with faculty and staff members. Finally, the University is reviewing “virtual” instructional lab software to determine its viability as a teaching tool.

PHYSICAL INFRASTRUCTURE

In connection with improving physical infrastructure planning, the Senior Vice President Finance was assigned as the key risk owner and identified the following activities over the past year.

Georgia State University currently has about 9 million gross square feet (gsf) of space in 55 buildings to support its academic and research missions, including parking and housing facilities. The University uses 35 buildings with approximately 5 million GSF of space for its core mission of teaching, student services and research. The University acquired 15 of these 35 buildings from other entities and retrofitted for teaching, research and academic support functions. Many of these buildings are old and not easily adaptable to provide modern learning environments that meet the latest technology requirements.

Current Georgia State University maintenance and operations project database and other studies identified about $70,000,000 in deferred maintenance, capital renewal, plant adaptation, and routine maintenance costs. The total replacement value of the facilities owned by Georgia State University is modestly estimated at $1 billion. According to APPA standards, about 1.5 percent of the replacement value, or $15 million should be invested in the maintenance of facilities each year.

Though the funding to Georgia State University is far below the suggested levels, recent infrastructure projects through Board of Regents MRR and University funding have improved the reliability and efficiency of the University’s critical building systems such as elevators, HVAC equipment (chillers, cooling towers, air handling units etc.), and roof replacements.
Robust MRR and University funding for infrastructure projects should continue to be a high priority to reduce the deferred maintenance backlog. Campus-wide infrastructure improvements are required to sustain an efficient, economical and timely preventive maintenance plan for Georgia State University's facilities.

**IMPROVING WORKPLACE PROXIMITY**

In connection with improving workplace proximity, the Senior Vice President Finance was assigned as the key risk owner and identified the following activities over the past year.

One of the goals in the Georgia State University 2005-2015 Master Plan update is to establish a central core of campus academic facilities and a secondary zone for support functions. This was also emphasized in 2012 Master Plan with a focus on Campus Core District.

In 2008, the University acquired 75 Piedmont Avenue (formerly Citizens Trust) building and relocated and consolidated several IS&T staff functions from Classroom South building. Vacated office space in Classroom South was renovated to provide state of art classrooms reinforcing the central academic core for the convenience of students and faculty. An additional fifteen classrooms, computer labs and small seminar rooms were added to the building on 2010 using an infill design concept which has become popular for both faculty and students.

In the past year, six floors of the 25 Park Place building have come on-line allowing the Department of Communication to relocate their entire department from cramped space in 1 Park Place. Additionally, all undergraduate advising functions have been moved out of 75 Piedmont Avenue and Sparks Hall and consolidated at 25 Park Place, giving students one location to obtain all of their advising services. An additional four to six floors of 25 Park Place are expected to come available during fiscal year 2014 to help continue the process of gaining efficiencies from providing adjacent work areas with access to convenient parking.
Information Security Risk Mitigation

BACKGROUND AND OVERVIEW

Georgia State University Information Systems & Technology (IS&T) operates to support a tremendously large, dispersed and transient population that is dependent on technology. While there are many IS&T related risks that have potential to disrupt services, including physical risks, University leadership and the Office of ERM determined that the most pressing risks relate to the user community and protection of data. While centralized servers and storage are available to the campus community, there are still many system users that rely on non-centralized storage or maintain poor practices as it relates to the use of portable storage devices. Moreover, the rise of phishing attacks represents a significant security risk, especially in light of the large population served at Georgia State University. As recently as September 2013, certain members of the faculty and staff received a phishing attempt asking users to upgrade/update their account. While these risks are likely shared by the community of member institutions of the University System of Georgia, they are particularly acute at Georgia State University given the size of the student population.

In light of these particular issues, the University’s leadership together with the Office of ERM identified the following risk statements.

Risk Statements: Users fail to protect University data.

A. Improper use of portable storage devices, or use of network storage that is not centrally managed, puts data at risk of being misplaced, destroyed or misused.

B. Users are too likely to respond to phishing attacks, inadvertently revealing sensitive data such as passwords.

DATA CLASSIFICATION POLICY AND EXPANSION OF RESEARCH DATA MANAGEMENT POLICY

In conjunction with improving data classification and data management, the University’s Chief Information Officer was identified as the key risk owner and identified the following activities in connection with risk mitigation.

Policy Review

IS&T conducted comprehensive review of the Georgia State University policy library and identified policy gaps. Currently, IS&T is working with other units to enhance University policies in this area. The goal is to identify critical and at-risk data so that the University can implement additional security controls on this data, without increasing the burden on users of low-risk or public data.

During the Information Security Policy gap analysis, the “Information Protection and Access” policy (7.20.4) was identified as a vital control to improve information security and limit risk of data breaches and loss. The “Information Protection and Access” policy stipulates how University data is properly categorized
and classified. This policy is being revised to clarify the roles and responsibilities of data stewards and how they can work with IS&T’s information security staff to protect university data.

The policy explains the data classifications that are assigned to data in order to facilitate selection of appropriate security controls based on the classification, value, and risks associated with the data in question.

There are numerous standards that may apply to sensitive and confidential data, such as:

- The Family Educational Rights and Privacy Act (FERPA), which addresses the handling of educational and student data;
- The Payment Card Industry Data Security Standards (PCI-DSS), which addresses the handling of credit cards and related information;
- The Health Insurance Portability and Accountability Act (HIPAA), which addresses health-related data; and
- The Gramm-Leach-Bliley Act (GLBA), which addresses financial data.

Georgia State University is improving its internal standards and linking them to the Federal Information Security Management Act (FISMA) standards to ensure more complete coverage of security controls, enhance the University’s overall security posture by using a national standard, and enhance the University’s ability to compare vendor products which provide identical or complementary controls against a normalized baseline.

While each of these standards has its own classification and terminology, the University’s policy is being updated to provide a more general set of definitions that are easier to apply. Typically, data will be classed as “Unrestricted,” “Sensitive” or “Confidential.” Each successive class demands a more stringent set of information security controls and provides a correspondingly higher level of data protection.

During the Information Security Policy gap analysis, the “Minimum Information Security Environment” policy (7.20.7) was identified as an area for improvement. A review of this policy is under way and changes will be made that provide clearer guidance on the controls and security measures that should be in place for each of the three main data classes.

IS&T is also looking at other policies that may need to be added or changed to provide more clear and effective controls over critical University data. Because this problem is not unique to Georgia State University, IS&T is working with other schools within the University System of Georgia (USG) to share ideas, knowledge and best practices that promote data security and governance. IS&T is focused on working with peer research institutions in the USG as it seeks innovative ways to maintain security in the challenging environments of cooperative research.

**Policy Communications**

IS&T is amending its new employee orientation packets to include information focused on cyber security. The updated employee orientation addresses many existing cyber security issues and threats. These items
explain why information security is important and what legislation governs various data security classifications. Topics include financial records, covered under the Gramm-Leach-Bliley Act (GLBA), health data, covered under Health Insurance Portability and Accountability Act (HIPAA) and FERPA. Awareness of compliance with laws, rules and regulations, as well as the importance of security guidelines are emphasized to each of the University’s new employees.

During the orientation, employees are made aware of the tools available to them that can detect malware, prevent data loss, block network-based attacks, and stop identity-based attacks. The materials reviewed demonstrate how user behavior, coupled with antivirus software, can protect computers and the data they contain from external threats.

This orientation also provides employees their first introduction to the identity security concepts that are key to data security. Good password practices are discussed, as well as how to identify a phishing attack and how good security habits will help protect them from malware. These concepts will be reinforced in future training through both the SANS “Securing the Human” and the Phishme.com tools.

The IS&T security homepage at http://technology.gsu.edu/technology-services/it-services/security/ was enhanced to help users easily find links to tools they can use to secure University systems and data, as well as their own computers and mobile devices, from viruses, malware and other cyber threats. The site provides information on data encryption for PCs and will soon expand to include data encryption solutions for Apple Macintosh systems. The site provides information on tools to enhance network security, such as virtual private networks (VPN) and firewalls. Visitors to the page can learn how to arrange a detailed security assessment, which is especially vital for those who interact with sensitive and confidential data.

October is National Cyber Security Awareness Month and IS&T will hold events to increase user awareness and understanding of the security risks the University faces, the policies that are in place to help limit those risks, and what
steps individuals can take to help protect university data.

Additional Steps

The McAfee Enterprise Policy Orchestrator (EPO) system was enhanced by deployment of the Host Intrusion Prevention Software (HIPS) module. This module provides additional security, above and beyond traditional anti-virus software. HIPS applies firewall protection via classic firewall rules, but it also provides enhanced firewall protection by using a reputation service that permits the University to block attacks from known malicious sites which have already been identified by other McAfee customers. Through the reputation service, Georgia State University gains the advantage of threat information that McAfee has collected from all its customers. Also, HIPS protects systems against buffer overflow attacks, a common class of network-based attacks. Finally, HIPS protects systems by using application sandboxing, which isolates vulnerable software, like the web browser, to contain the damage an attack on such vulnerable code might otherwise inflict. Overall, HIPS provides a high level of protection, even against attacks for which there are no known signatures, making it effective against zero-day attacks.

Georgia State University also works with McAfee to identify new malware that currently lacks known signatures and to develop appropriate signatures for them. In partnership with McAfee, the University has two McAfee interns (University computer science students) working on site helping with the identification of new threats. This process allows IS&T to quickly react to new attacks and limit their effect on University systems. The partnership is so successful that IS&T’s Information Security has worked with other universities to help them implement similar strategies.

IS&T also provides McAfee Endpoint Protection software. This software encrypts data so that if stolen a thief cannot gain access to sensitive or confidential data. This protection is especially important for systems like laptops where physical security controls are less effective.

IS&T is developing a roadmap to address these, as well as the rest of the SANS top 20 security threats. The roadmap includes funding requests for a scanning tool that will help identify where sensitive data may be stored, so that the data can be secured. IS&T has initiated a funding request for remote device management tools which allows remote wiping of critical data, location identification of lost or stolen devices, and centralized device management to ensure that critical security controls are in place on mobile devices.

IS&T is helping departments move critical data into the campus’s main data center. IS&T provides hosting space within the data center on a space-available basis at no charge. IS&T will seek additional funding to expand this offering, should more space be needed. The Robinson College of Business, College of Arts and Sciences and the College of Law have relocated systems to the data center. These moves improve security and provide savings for the University in the form of reduced facilities costs.

IS&T is working to address the full lifecycle of the University’s critical data. IS&T recently reviewed its own internal practices for data destruction for end of life devices, as defined by the Department of Administrative Services for the University System. IS&T has a contract with Iron Mountain to ensure physical destruction of server disks and has procedures in place for strong data wipes of workstation disks.
During National Cyber Security Awareness Month, IS&T will be reminding the user community about the importance of proper data destruction when a device reaches the end of its life and must be discarded. IS&T is investigating the possibility of expanding the Iron Mountain contract to cover more than just IS&T devices.

**INCREASE THREAT AWARENESS AND APPLY BEST PRACTICES**

In connection with mitigating the risks of phishing and social engineering attacks, the IS&T Department has undertaken the following actions.

**Securing the Human**

IS&T has purchased one-year licenses for the “Securing the Human” SANS Security Awareness video series. Plans for distribution and communication are under way. The video series will be available to all faculty and staff. As shown by the prevalence of successful attacks that use social engineering, users and their behaviors are often the weakest link in any security plan. These videos are designed to increase users' awareness of risk and how to avoid them. The content is provided in video format to make it convenient for busy workers and students to view the material at their convenience.

**Phishme.com**

Phishme.com licenses were purchased in late June, with plans to implement them in October 2013 during National Cyber Security Awareness Month. The license covers faculty, staff and students. The phishme.com license allows Georgia State University to probe its defenses against social engineering attacks, in the form of faux social engineering emails crafted to be similar to what an attacker would send. IS&T can then analyze response rates to measure the effectiveness of security awareness training. Not only does the University get general response rate information, but it also identifies specific users who may be more vulnerable to these kinds of attacks and can provide targeted training to increase awareness within these populations.
Perceptions of Campus Security Risk Mitigation

BACKGROUND AND OVERVIEW

As a result of its urban setting, Georgia State University faces particular issues as it relates to crime, but more importantly, as it relates to the perceptions of faculty, staff, students, prospective students and parents as to the downtown environment. While statistics show that actual crime on campus is relatively low, the perceptions of campus constituents continue to indicate an endemic concern about campus safety and security. This is an issue that is somewhat unique to the University (although shared with Georgia Tech). In light of this issue which can have an impact on overall job or student satisfaction, student recruiting and the overall reputation of the University, the University's leadership together with the Office of ERM identified the following risk statements.

Risk Statements. Constituents of Georgia State University have poor perceptions of Campus Safety & Security.

A. Additions of visible security or other uniformed personnel will contribute to improved perceptions of security on campus.

B. University constituents may not receive adequate marketing of the University’s actual safety causing perceptions to overcome reality.

PANTHER AMBASSADOR PROGRAM

In an effort to ensure adequate uniformed personnel to improve the perception of campus safety and security, the Department of Enterprise Risk Management undertook a review of the Panther Ambassador Program to evaluate whether it is currently having, or is likely to have, a positive impact on perceptions of campus safety and security.

The Panther Ambassador program began in August 2012 (pre-dating the conclusion of the Enterprise Risk Assessment) as a way to provide a visible security presence as well as assistance to faculty, staff and students as they move around campus during the evening and nighttime. The Panther Ambassador program is a contracted service with Contemporary Services Corporation (CSC) and operates daily between the hours of 6:00pm and 1:00am. CSC owns the shuttles, T-3s and bicycles used on patrols and is responsible for any liabilities associated with the program.

Duties of the Panther Ambassadors include standing at pre-defined posts to provide visibility and oversight, providing shuttle rides on six passenger carts, assisting with street crossings, escorting people from classroom buildings to parking decks and other services as situations dictate.

Monday through Friday there are nine Ambassadors on duty with one supervisor. On Saturday and Sunday there are two Ambassadors circulating around campus.
The nine weekday posts consist of four shuttle routes, three roving T-3 routes, and two stationary posts. Patrol routes and posts are decided upon based on the location of the campus population. Special events or situations may cause the routes to change.

**Additional Benefits**

In addition to the defined duties discussed, the Panther Ambassadors provide additional benefits to the University campus. These include, but are not limited to:

- Reporting malfunctioning street and building lights to the appropriate authorities
- Crowd control and assistance during emergency situations
- Working with University Police to decrease crime
- Asking loiterers to move along

**Evaluation of Effectiveness**

To evaluate the effectiveness of the program, Enterprise Risk Management (ERM) staff conducted interviews with Georgia State University management, students and CSC staff. ERM staff also analyzed CSC’s nightly reports, and reviewed student usage statistics. Finally, ERM staff participated in two separate "ride-alongs", conducting informal interviews with over 30 students using the shuttle service.

In the opinion of the ERM staff, the program is well organized under the Associate Vice President for Finance & Administration at Georgia State University and leadership at CSC. CSC maintains a pool of fifteen employees trained to man the nine posts on campus. Each night CSC staff report for duty between 5:00 and 6:00. A brief staff meeting is conducted to make everyone aware of any special events taking place on campus, and a rotating duty roster is presented. Employees rotate through several posts throughout a shift to keep them alert.

CSC sends a nightly report to Finance and Administration. The format of these reports has been evolving since the inception of the program, but by February 2013 they became fairly standardized into their current form. These reports include activity logs and usage statistics.

In February, CSC began using hand clickers to track the number of students using the shuttles on campus. The average daily usage in March (which included spring break) was 99 students, and daily shuttle usage in March ranged from a low of thirteen to a high of 256. The average number of students per shuttle was 28.

The average daily usage in April was 230, and daily shuttle usage in April ranged from a low of 71 to a high of 570. The average number of students per shuttle was 67.
During “ride-alongs” on the campus shuttles, it was clear that students appreciate the program very much, and the students spoken to offered universal praise. Several students also noted that they would like to see the hours for the shuttles expanded. While these informal discussions do not represent a scientific survey, it should be noted that on the two “ride-along” occasions, the riders were overwhelmingly female. It should also be noted that all drivers were courteous and professional.

**Additional Recommendations**

Following completion of the effectiveness review, the Office of Enterprise Risk Management recommended the following as potential improvements.

**Uniforms**

Georgia State University should give some thought to how the CSC employees acting as Panther Ambassadors are identified. While the yellow CSC shirts do stand out and make it obvious to students and/or undesirables that security is around, some consideration might be given to more clearly identifying the Panther Ambassadors personnel as affiliated with the University.

**Outcome:** CSC and the University (using Foundation funds for the Georgia State University shirts) each purchased blue shirts with Georgia State University and CSC logos on them to better identify the ambassadors as part of the University’s service network, but under the employment of an outsourced company (CSC).
PERCEPTIONS OF CAMPUS SECURITY RISK MITIGATION

**Seatbelts**

Not all the golf cart drivers wore their seatbelts, and drivers did not request that students buckle their restraints before the golf cart was under way. While CSC is ultimately responsible for the safety of the services it provides, CSC should strongly consider requiring drivers and students to wear the seatbelts in the carts while in motion.

**Outcome:** As a result of the ERM office’s recommendation, policies were promptly changed to improve seatbelt usage and signs were posted in each vehicle.

**Post 8 Hours**

Post 8 is the stationary post located at the intersection of Ellis and Piedmont Ave. across Ellis from Piedmont North housing. In addition to normal observation of students, this post also provides the service of stopping Northbound traffic on Piedmont Ave. from making a right onto Ellis towards the highway when students are properly walking through the crosswalk across Ellis. Given that this duty is most valuable during rush hour; this is a Post that would benefit beginning earlier in the day (e.g., 4:30 or 5:00).

**Outcome:** Hours for post 8 were changed to 5pm – 12midnight. This change has been perceived positively.

**Publicity**

Many students interviewed during “ride-alongs” were first time users of the service. While freshmen students living on campus seemed relatively aware of the service, many other students indicated that they had never heard of the program. Given the positive impressions of students using the service, more publicity will only help increase perceptions of safety on campus.

**Outcome:** The University made flyers describing the program for the Panther Ambassadors, Housing and Incept leaders to distribute as part of the new students information packet.

**PUBLIC RELATIONS EFFORTS**

In order to improve perceptions related to public relations efforts, the Public Relations (PR) and Marketing Communications department of Georgia State University as the key risk owner undertook an analysis of proposed actions to begin the process of improving public relations and tracking efforts in connection with perceptions of campus safety and security.

PR and Marketing Communications, in concert with Campus Police, the Office of Institutional Effectiveness and Staff Council, will conduct a survey to gauge campus perception of safety and security. This survey, to be issued in the fall, will provide new information and serve as a benchmark on which to measure the impact of future communications activities.

PR and Marketing Communications has revamped the website for safety and security as part of its overall redesign of the university’s web presence. The new site does a more effective job of aggregating critical
safety and security information and provides users with easier access to crucial contact information. Public Relations and Marketing Communications will work with Campus Police and others to use the site to highlight new developments and programs on safety and security on campus.

PR and Marketing Communications introduced in the fall a new internal newsletter called “Our Community.” It replaces “GSU Digest,” and provides additional opportunities to report about programs, initiatives and success stories in safety and security.

Because of the increasing impact and importance of social media, PR and Marketing Communications is working with Safety and Security to more aggressively communicate safety-related issues and incidents affecting the campus through social media.
Workflow Process Risk Mitigation

BACKGROUND AND OVERVIEW

Many respondents to the risk assessment indicated a belief that poor or non-existent workflow processes presented a risk to Georgia State University as it greatly decreased efficiency of faculty and staff. Through an iterative and ongoing process of identification and improvement of workflow processes, efficiency can be improved and the University can continue to maximize the impact of each academic support dollar used to support the University. Accordingly, the following risk statements were identified.

**Risk Statements.** Workflow processes are either too cumbersome or non-existent leading to inefficiencies in task completion.

A. Workflow processes are too cumbersome for certain tasks.
B. Workflow processes may not exist for certain functions and those functions would benefit from increased certainty of accomplishing a task.

IDENTIFICATION OF WORK FLOW PROCESS OPPORTUNITIES

The Office of ERM as the key risk owner took two primary steps to identify opportunities to improve workflow processes at the University. First, the Director of ERM together with the Comptroller’s office conducted facilitated sessions with the College of Arts & Sciences and the College of Law to identify recommended improvements. From these sessions, two primary areas of suggested improvements were identified: improving purchase order closure processes and improving the hiring process. The hiring process work process was deferred for review because the University had just acquired software that was supposed to represent great improvements in the process. Accordingly, review of the hiring process was deemed to be better left until fiscal year 2014 to analyze the effects of the process improvements that were just implemented.

Second, the Office of ERM and the Comptroller’s office in the context of their day-to-day work identified numerous areas where opportunities for improvement were available. From these, the Office of ERM worked on numerous workflow process improvements or creation, the most significant of which are discussed below.

WORK FLOW PROCESS IMPROVEMENTS

**Purchase Order Closure**

As part of the facilitated sessions, the University administrative teams identified that the purchase order closure process was unnecessarily time consuming and complex. In many cases, college administrative personnel had to manually close hundreds or thousands of purchase orders that had minimal balances
remaining (in many cases these were travel related). The problem became particularly exacerbated as the University approached year end and the various University operating units had funds encumbered under purchase orders that may have been completed.

To approach the problem, the Office of ERM and the Comptroller discussed creating an automated process to close purchase orders that had a minimal difference between the purchase order amount and the amount disbursed. In discussions with the Purchasing department and the Spectrum Office, it was determined that an auto-close process would be beneficial and could be implemented. Furthermore, the Disbursements department began more carefully managing the “Final” field that users could select to indicate that the expense reimbursement for a particular travel purchase order was the final disbursement and the purchase order could be closed.

As a result of the initial implementation of the auto-close process in January 2013, open PantherMart purchase orders were immediately reduced by over 10,000 open purchase orders from 23,902 open purchase orders to around 11,800. The auto-close process closes an average of 300 POs per night, POs that previously required manual intervention. As a result of the ongoing effectiveness of the PO auto-close process implemented and created by the Spectrum office, the University now averages only about 6,000 open POs per month and many of these close without the necessity of manual intervention.

**1099 Process and Procedure**

Each calendar year, Georgia State University is required to upload a file to the United States Internal Revenue Service (IRS) documenting all payments made for services to certain categories of providers. Historically, this process has been very labor intensive, requiring substantial manual intervention, primarily on the part of the Disbursements department. Additionally, the time frame for completing these tasks is fairly short given the large amount of potentially qualifying transactions. For example, the query used to pull potential transactions requiring a 1099 for calendar year 2012, produced in excess of 76,000 journal lines requiring review.

In past years, those 76,000 lines would be reviewed using manual Excel sorting to remove corporations, non-profits, non-relevant transactions, annual amounts less than the IRS limits, etc. Additionally, this work would largely pull many of the Disbursements office personnel off of other tasks associated with the day-to-day processing of disbursements transactions.

To complete calendar year 2012, however, the Director of ERM, working together with Disbursements, utilized further advanced Excel techniques, such as the VLookup function, to greatly reduce the amount of manual review required (some will always be necessary in the event the journal lines do not provide enough detail to determine whether or not a transaction is subject to receiving a 1099). Following implementation of the new procedures, the total work amount was greatly reduced and the University was able to produce the 1099's in three weeks versus the prior completion time of a full six weeks. From the 76,000 lines of data, only approximately 6,000 lines related to IRS 1099 transactions and the improved processes greatly reduced the time necessary to get to the proper transactions.
WORKFLOW PROCESS RISK MITIGATION

It is anticipated that the 1099 process for calendar year 2013 could be completed in as little as a week, with a minimum of manual intervention now that the processes have been improved and used for the prior calendar year.

**Unclaimed Property**

Georgia State University often receives letters from unaffiliated third parties that offer to recover (for a finder’s fee) unclaimed property from the State of Georgia Department of Revenue. The University does not use these services. However, as the result of one of these letters, the Office of ERM completed a thorough review of any escheated property currently being held by the State of Georgia Department of Revenue. As a result of this review, the University was able to recover over $30,000 held at the State level.

As a result of that recovery, the Office of ERM will undertake an annual review of unclaimed property to identify any recoverable assets. Furthermore, although unlikely to be in amounts similar to that recovered from the State of Georgia, the Office of ERM will expand its efforts and search neighboring states as well to identify any additional unclaimed property.

**PCI-DSS Compliance**

Payment Card Industry Data Security Standards (PCI-DSS) compliance is a requirement of the major credit card issuers and the University is subject to these standards as a result of accepting credit and debit cards in its ordinary course of business. The Office of ERM has taken over primary responsibility for assuring PCI-DSS compliance, which is an ongoing process.

As part of its initial efforts in this area, the Office of ERM recently completed the first University-wide inventory of all payment processing locations (whether it was a payment terminal (swipe), on-line or otherwise). From this inventory, the Office of ERM, together with Revenue, Receivables & Cashiering Services, Auxiliary Services, and IS&T is finalizing its approach to complete additional self-assessment questionnaires for each processing location. While no major potential data breach risk has been identified to date, this process has and will continue to improve the University’s PCI-DSS compliance and control over its “cardholder data environment.”

**FUTURE IMPROVEMENTS, FURTHER PROCESS IMPROVEMENTS**

The Office of ERM anticipates continuing its work in the area of work process improvements and creation over the ensuing years. Currently, future projects include: evaluation of the hiring process, improvements in payment streams, including potentially utilizing the PayMode payment system. Additionally, further follow-up on the projects in process will continue.
Funding Formula Risk Mitigation

BACKGROUND AND OVERVIEW

The Enterprise Risk Assessment identified declining state appropriations as the number one risk facing the University. While FY 2013 saw a slight rebound in the level of state appropriations, their percentage of total revenues accounted for 29%, compared to 46% in FY 2008. FY 2013 appropriations were $178 million, compared to $228 million in FY 2008, a 22% reduction. The level of state appropriations will continue to be a risk for the foreseeable future. The state is transitioning away from appropriations based on enrollment to a formula based on graduation and retention. This new formula has not yet been finalized and the full impact to the University is still unknown.

Accordingly, the following risk statement was identified.

Risk Statements. Georgia State University would be adversely affected by not maximizing availability of appropriations under the funding formula.

A. Maintaining and improving retention, progression and graduation metrics in a declining resource environment.

ADVISING PROGRAMS

In its ordinary course of improving retention, progression and graduation and as mitigation to the Risk Statement, Georgia State University and the Office of Enrollment and Academic Affairs as key risk owner have implemented a comprehensive initiative to improve student outcomes while minimizing time and credit hours to earn a degree by providing more effective academic advising.

Overhaul of Academic Advising

The University and its colleges maintained six different advising offices with little coordination between them, no common record keeping, and no common training. As prescribed by the 2011 Georgia State Strategic Plan, the University has hired 42 additional academic advisors to bring our student-advisor ratio to the national standard of 300-to-1. We have established a common record system, common training, and a campus-wide University Advising Council. In August 2012, the University went live with a cutting-edge, web-based GPS Advising system based on seven years of RPG data and over two million student grades. The system, which monitors 30,000 students with nightly updates from Banner, uses 700 markers to track when students go off path academically and offers predictive analytics for how each student will do for every major and every course in the curriculum.

Outcome: In its first ten months of operation, the GPS system was used in almost 15,000 advisement sessions. 2,452 students were converted from off path to on path for graduation, and 900 had their
schedules corrected during registration when markers were triggered indicating that they had signed up for wrong or inappropriate courses.

Deployment of Transition and Graduation Advisors

In addition to hiring more professional advisors assigned to individual students, since 2010, Georgia State University has been hiring a team of advisors dedicated to specific challenges faced by groups of students collectively. 6-year graduation rates for students who change majors after the completion of 75 hours, for instance, are 20 points lower than overall rates. Transition and Graduation Advisors work with students and departments to help ease the students’ transition between majors and to resolve roadblocks to graduation.

Outcome: In the first two years of the program, the advisors saved more than 700 students from having to enroll extra semesters in order to graduate.

REDUCING STUDENTS THAT DROP OUT FOR LACK OF AID

In its ordinary course of improving retention, progression and graduation, the University and the Office of Enrollment and Academic Affairs has implemented a comprehensive undertaking in connection with increasing financial aid as will most likely keep students enrolled.
Led by President Mark Becker and the Georgia State University Foundation, the University has raised over $10 million in new scholarships over the past twelve months. In 2010, the University opened a fully staffed Scholarship Resource Center and created a searchable data base of scholarship opportunities for students.

**Outcome:** Disbursements to students from institutional scholarships and grants increased 263% since 2011. In its first year of operation, the new scholarship data base was used by more than 9,000 students.

**Reduce Negative Impacts of Unmet Need**

With a large increase in the number of students dropped for non-payment in recent terms, Georgia State University initiated the Panther Retention Grants program in 2011. Within hours of the fee drop, personnel in enrollment services proactively reach out to hundreds of students who have just been dropped, offering small grants. In some cases, the difference between a student staying enrolled or not hinges on as little as $300—a surprising claim until one realizes that 40% of Georgia State students come from households with annual incomes of $30,000 or less.

**Outcome:** Over the past year, 1,700 students were returned to classes after having been dropped as a result of this program. The grant recipients meet with financial aid counselors, and more than 90% have re-enrolled for subsequent semesters without requiring additional grants.

### Panther Retention Grants

- Provide emergency funds to students who are registered for classes but who are dropped for non-payment
- As little as $300 has meant the difference between a student dropping out and being able to continue on the path to a college degree

**Grants Awarded:**

<table>
<thead>
<tr>
<th>Term</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fall 2011</td>
<td>41</td>
</tr>
<tr>
<td>Spring 2011</td>
<td>132</td>
</tr>
<tr>
<td>2012-2013 AY</td>
<td>1700</td>
</tr>
</tbody>
</table>

**Decrease Negative Effects of the Loss of the HOPE Scholarship**

At Georgia State University, 74% of freshmen come into the University supported by the HOPE Scholarship, and the scholarship is worth $7,000 per year. In 2008, 51% of HOPE freshmen lost the scholarship by the
end of their first year due to their GPA dropping below 3.0. Of these students, only 9% ever gained the scholarship back again. For the others, their likelihood of graduating dropped 40 points, from 61% to 21%. Sadly, the vast majority of students who dropped out after losing HOPE left Georgia State in good academic standing; they were on the path to graduating, they just lacked a 3.0 GPA. In 2009, the University piloted Keep HOPE Alive, a program offering students $500 a semester for the first two semesters after they had lost HOPE. In return for the funds, they signed a contract agreeing to attend a series of academic skills and financial literacy workshops and to meet with their academic advisors regularly during the year.

**Outcome:** Last year, over 60% of the students in the program recovered Hope by their next check point, as compared to only 9% gaining HOPE back among students not in the program (see chart below). The program has helped to raise HOPE retention rates on campus from 49% in 2008 to 75% last year and has proven so effective that the Goizueta and the Coca-Cola Foundations both directed funds to the initiative as part of recent gifts to the University.

---

**Keep HOPE Alive**

- **Targets students who have lost HOPE**
- **Grants students $500/semester for one year on the condition they attend year-long series of academic skills workshops and individual advisement sessions**
- **Institutional HOPE Retention Rate 2008: 49%**
  **Institutional HOPE Retention Rate 2012: 75%**
The ERM Process in 2014 and Beyond

In fiscal year 2014, the Office of ERM will continue to follow-up on the mitigation activities for the key risks selected for mitigation from the 2013 assessment as detailed in this Annual Report. Additionally, with the input of senior University leadership, at least three more key risks will be identified for further mitigation. While ultimate selection is still ongoing, Georgia State University will likely look at further efforts around employee morale and retention, the hiring process as a workflow process and as a key risk, as well as inversion and compression. Additionally, the Office of ERM will look to further identify quantitative and qualitative metrics to measure progress against each identified risk.

In fiscal year 2015, the Office of ERM will perform a new assessment to identify any new key risks and gauge progress against the key risks for which mitigating activities have already been progressing.
Contact Information

Office of Enterprise Risk Management, Georgia State University
Sparks Hall, Suite 400
33 Gilmer Street
Atlanta, GA 30303
Tel 404-413-3068
Fax 404-413-3075

Matthew S. Morrison
Director of Enterprise Risk Management
mmorrison12@gsu.edu

James Greenwell
Enterprise Risk Management Analyst
jgreenwell@gsu.edu

Dave Lakly
Enterprise Risk Management Analyst
dlakly1@gsu.edu
Appendix A: University System of Georgia Risk Management Policy

7.15 Risk Management Policy

7.15.1 Risk

Risk refers to the probability of an event and potential consequences to an organization associated with that event’s occurrence. Risks do not necessarily exist in isolation from other risks; as a result, a series of risk events may result in a collective set of consequences that is more impactful than the discrete set of consequences associated with risk events taking place in isolation. Risk is inherent to any activity. It is neither possible, nor advantageous, to entirely eliminate risk from an activity without ceasing that activity. The safest ships are the ones that do not sail, but that is not what they are designed for.

A risk is defined as Major when the combination of an event’s probability and the potential consequences is likely to:

1. Impair the achievement of a University System of Georgia (USG) strategic goal or objective;
2. Result in substantial financial costs either in excess of the impacted institution’s ability to pay or in an amount that may jeopardize the institution’s core mission;
3. Create significant damage to an institution’s reputation or damage to the USG’s reputation; or,
4. Require intervention in institutional or USG operations by the Board of Regents and/or an external body.

Major Risks are a subset of the larger category of Significant Risks referenced in the Risk Management Policy. Major Risks are the most critical risks and must meet the definition of Major Risk as defined in Section 7.15.1 of this Policy Manual. Significant Risks includes Major Risks but also include less critical risks. The definition of Significant Risk will be detailed in the System-level procedures manual referenced in Section 7.15.5.4 of this Policy Manual. However, the level at which a risk becomes Significant will vary by institution given each institution’s risk tolerance, resources, and ability to manage risk events. (BoR Minutes, August 2010)

7.15.2 Purpose

The Board of Regents recognizes that the proper management of risk is a core leadership function that must be practiced throughout the USG. The Enterprise Risk Management (ERM) framework shall be the accepted framework for USG risk management. ERM is defined as a process-driven tool that enables management to visualize, assess, and manage significant risks that may adversely impact the attainment of key organizational objectives. It is the responsibility of USG and institutional leaders to identify, assess, and manage risks using the ERM process. The successful implementation of ERM policies and practices can enhance potential opportunities to help achieve organizational objectives.

Some level of risk is not only expected in normal everyday activities but can be beneficial. However, acceptance of risk shall not include:

1. Willful exposure of students, employees, or others to unsafe environments or activities;
2. Intentional violation of federal, state, or local laws;
3. Willful violation of contractual obligations; or,
4. Unethical behavior.

Risk management decisions should be made after conducting a cost-benefit analysis; such analysis should take into account the potential costs associated with the identified risk should the risk event take place as compared to the costs associated with mitigating the risk. It should be noted that these costs are not only financial but may also include substantial damage to reputation, opportunity costs, potential litigation, distraction from core missions, obsolescence and others.

While it is challenging to properly assess some risk events prior to them happening, Major Risks that could result in significant long-term damage to the USG or a USG institution must be identified to the Board and the Chancellor as soon as possible. Acceptance of Major Risks must be at the discretion of the Board and the Chancellor. The System-level procedures manual referenced in Section 7.15.5.4 of this Policy Manual shall provide additional guidance on the timing and form pertaining to the reporting of Major Risks. Significant Risks should be identified in a timely manner. Significant Risks specific to an institution or unit shall be accepted and/or managed by the institution’s president or the president’s designee.

Categories of risks managed through the ERM framework include:
1. Strategic Risks – Affect ability to carry out goals and objectives as articulated in the USG Strategic Plan and individual Institution Strategic Plans;
2. Compliance Risks – Affect compliance with laws and regulations, student, faculty and staff safety, environmental issues, litigation, conflicts of interest, etc;
3. Reputational Risks – Affect reputation, public perception, political issues, etc;
4. Financial Risks – Affect loss of or ability to acquire assets, technology, etc; and,
5. Operational Risks – Affect on-going management processes and procedures.

An identified risk may fall into multiple categories. (BoR Minutes, August 2010)

7.15.3 General Objectives

The purpose of the Risk Management Policy is to strengthen the proper management of risks through proactive risk identification, risk management, and risk acceptance pertaining to all activities within the University System Office and USG institutions.

The Risk Management Policy is intended to:
1. Ensure that Major Risks are reported to the Board and the Chancellor for review and acceptance;
2. Result in the management of those risks that may significantly affect the pursuit of the stated strategic goals and objectives;
3. Embed a culture of evaluating and identifying risks at multiple levels within the USG and USG institutions;
4. Provide a consistent risk management framework in which the risks concerning USG and institutional business processes and functions are identified, considered, and addressed in key approval, review and control processes;
5. Ensure that institutions communicate **Significant Risks** to the USG level so risk can be measured across the System;
6. Inform and improve decision-making throughout the University System;
7. Meet legal and regulatory requirements;
8. Assist in safeguarding USG and institutional assets to include people, finance, property and reputation; and,
9. Ensure that existing and emerging risks are identified and managed within acceptable risk tolerances.

(BoR Minutes, August 2010)

### 7.15.4 Applicability

The Risk Management Policy applies to all USG institutions and the University System Office. (BoR Minutes, August 2010)

### 7.15.5 Implementation

#### 7.15.5.1 Frameworks and Procedures

An institution-wide approach to risk management shall be adopted by all USG institutions. It is expected that risk management processes will be embedded into the institution’s management systems and processes. All risk management efforts will be focused on supporting the institution’s objectives. Therefore, each institution president shall develop a campus risk management framework and associated procedures that include:

1. Formal and ongoing identification of risks that impact the institution’s goals;
2. Development of risk management plans;
3. Monitoring the progress of managing risks;
4. Periodic updates of risk management plans; and
5. Reporting of risks so that **Significant Risks** can be rolled up to the System level.

### 7.15.5.2 Risk Management Methodology

Risks may be managed by using one or more of the following methods:

1. Avoid (eliminate, withdraw from or do not become involved in an activity creating risk);
2. Retain (accept the risk and plan for the expected impact);
3. Transfer/Share (move the risk to another party by hedging against undesired outcome or reduce the risk through processes such as insurance); and,
4. Reduce (control the risk through additional or optimized controls).

### 7.15.5.3 Oversight

Each president shall designate in writing a Risk Management Policy coordinator to assist campus administrators in maintaining the campus risk management framework and procedures. The Risk Management Policy coordinator shall have sufficient authority to ensure high-level management of the institution’s risk management efforts.

At the System level, the Chancellor shall designate an executive-level position to oversee implementation of the Risk Management Policy across the University System of Georgia. The Chancellor also shall designate a Risk Management Policy coordinator to assist University System Office (USO) administrators in maintaining the USO
risk management framework and procedures. The Committee on Internal Audit, Risk and Compliance is the Board committee that shall provide oversight to implementation of the Risk Management Policy and review Major Risks on behalf of the Board of Regents.

7.15.5.4 Accountability

Campus risk management framework and procedures shall be reviewed annually. Periodic reviews for compliance with the system wide guidelines shall also be conducted by internal audit or a similar accountability function. Additional procedures for risk management policy reporting and implementation shall be established in a System-level procedures manual. (BoR Minutes, August 2010)
Appendix B: Key Risk Assessments
### GSU RISK REPORT – KEY RISK AREA #1 PHYSICAL SPACE

<table>
<thead>
<tr>
<th>Mitigating Activities</th>
<th>Objective</th>
<th>Responsible Party, Planned Activities, Dates &amp; Resources</th>
</tr>
</thead>
</table>
| **Key Risk Area #1:** Physical space constraints impede GSU from accomplishing its strategic objectives.  
Enterprise Risk Owner: Jerry Rackliffe, SVP Finance & Administration                  |                                                                           |                                                                                                                           |
| 1a. RISK COMPONENT: Insufficient or poorly managed availability of top quality research space negatively affects ability to recruit and retain research faculty, impacting the University’s ability to build a research profile that will continue to expand its economic development outcomes through innovation.  
(1) CONTROL OBJECTIVE #1: Assess sufficiency of overall quantity of research space and identify most efficient utilization of available and planned space.  
Evaluate productive use of existing research space and evaluate yield.  
Move to a model that allocates space on productivity rather than seniority / historical use. | Establish and implement both short- and long-term strategies that will yield the most efficient utilization of existing research space and maximize productivity and yield in any planned expansion. | Person/group responsible for implementing the Process:  
James Weyhenmeyer, VP, Research & Economic Development  
Planned activities and target date for implementation of the process:  
Establish criteria for allocation of research lab space:  June 30, 2013.  
Recommendations on changes to most efficiently utilize existing research lab space to facilitate knowledge creation, discovery, innovation and translation: June 30, 2013  
Integrate anticipated completion date for Science Park Phase II and its impact on lab space and utilization: June 30, 2013  
Resources Required and possible source:  
Access to Facilities leadership and personnel. No additional funding or financial resources required (excluding planned funding of Science Park Phase II). |
| 2. CONTROL OBJECTIVE #2: Assess the overall quality of existing research lab space.  
Conduct a comprehensive analysis of the quality of existing research space to align with the short- and long-term goals that the University has identified as current and potential areas of research focus. | Ensure that existing research lab space is of sufficient quality to meet the research faculty needs and the anticipated needs of faculty hires under the Second Century Initiative program, and to meet, or exceed when possible, the regulatory mandates for the use of space. | Person/group responsible for implementing the Process:  
James Weyhenmeyer, VP, Research & Economic Development  
Planned activities and target date for implementation of the process:  
Analysis of relative quality of existing research lab space:  June 30, 2013.  
Recommendations on improvements to quality of existing research lab space:  June 30, 2013  
Resources Required and possible source: |
<table>
<thead>
<tr>
<th>Mitigating Activities</th>
<th>Objective</th>
<th>Responsible Party, Planned Activities, Dates &amp; Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to Facilities leadership and personnel. No additional funding or financial resources required (excluding planned funding of Science Park Phase II and renovations necessary to meet specific space certifications (e.g., biosafety labs).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1b. **RISK COMPONENT**: **Insufficient or poorly managed availability of top quality instructional lab space negatively affects educational offerings.**  
   (1) **CONTROL OBJECTIVE #1**: Assess sufficiency of overall quantity of lab space and identify most efficient utilization of available space.

   Evaluate conclusions of the Sasaki study as they relate to the **quantity** of instructional lab space needed at GSU. Determine next steps to improve **efficient utilization** of existing instructional lab space and identify future expansion needs.

   Maximize existing instructional lab space through efficient utilization and identify future needs for instructional lab expansion, if necessary.

   **Person/group responsible for implementing the Process**: Jerry Rackliffe, SVP, Finance and Administration

   **Planned activities and target date for implementation of the process**:  
   Identification of future requirements for additional instructional lab space: June 30, 2013.
   Recommendations on changes to most efficiently utilize existing instructional lab space without further expansion: June 30, 2013

   **Resources Required and possible source**:  
   Access to Facilities leadership and personnel. No additional funding or financial resources required unless investments are determined to be necessary to increase quantity of instructional labs requiring new building or retrofitting of existing space.

   (2) **CONTROL OBJECTIVE #2**: Assess quality of existing instructional lab space.

   Identify appropriate facilities management personnel to conduct a comprehensive analysis of the **quality** of existing instructional lab space.

   Ensure that existing instructional lab space is of sufficient quality to meet academic and instructional needs.

   **Person/group responsible for implementing the Process**: Jerry Rackliffe, SVP, Finance and Administration

   **Planned activities and target date for implementation of the process**:  
   Analysis of relative quality of existing instructional lab space: June 30, 2013.
   Recommendations on improvements to quality of existing lab space: June 30, 2013

   **Resources Required and possible source**:  
   Access to Facilities leadership and personnel. No additional funding or financial resources required unless investments are determined to be necessary to increase quality of existing instructional lab space.
<table>
<thead>
<tr>
<th>Mitigating Activities</th>
<th>Objective</th>
<th>Responsible Party, Planned Activities, Dates &amp; Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>1c. RISK COMPONENT: Aging physical infrastructure creates financial challenges to plan for repair or replacement of physical plant elements exceeding their useful lives.</td>
<td>Improve accuracy of planning for major infrastructure repair or replacement. Identify appropriate amounts of emergency funding availability for high-priority infrastructure repair and replacement and work to ensure adequate balances are maintained.</td>
<td>Person/group responsible for implementing the Process: Jerry Rackliffe, SVP, Finance and Administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Planned activities and target date for implementation of the process: Document five-year infrastructure outlook for major repair and replacements: June 30, 2013.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Resources Required and possible source: Access to Facilities leadership and personnel. No additional funding or financial resources required unless investments are determined to be necessary to increase reserves to cover anticipated near future repairs or replacements.</td>
</tr>
<tr>
<td>1d. RISK COMPONENT: Many schools and administrative departments are not together in similar physical locations reducing efficiencies that are possible with adjacent work areas.</td>
<td>Identify and reduce the number of groups that do not operate entirely out of the same spaces. Look for additional efficiencies by co-locating groups of personnel that perform the same or similar functions.</td>
<td>Person/group responsible for implementing the Process: Jerry Rackliffe, SVP, Finance and Administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Planned activities and target date for implementation of the process: Identification of groups that need to be located together: June 30, 2013. Make necessary moves to ensure groups are located together in connection with also located to SunTrust and Atlanta Life buildings: December 31, 2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Resources Required and possible source: Access to Facilities leadership and personnel. Funding to cover movements of groups to new locations (not expected to be significant.</td>
</tr>
</tbody>
</table>
### GSU RISK REPORT – KEY RISK AREA #2 INFORMATION SECURITY

<table>
<thead>
<tr>
<th>Mitigating Activities</th>
<th>Objective</th>
<th>Responsible Party, Planned Activities, Dates &amp; Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Risk Area #2: <em>Users fail to protect Georgia State University data</em>&lt;br&gt;Enterprise Risk Owner: J.L. Albert, Associate Vice President and CIO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 2a. RISK COMPONENT: Improper user of portable storage devices or use of non-centrally managed storage puts data at risk of being misplaced or misappropriated.<br>(3) CONTROL OBJECTIVE #1: Create and implement a data classification policy.

<table>
<thead>
<tr>
<th>Identify where data classified as non-public is being stored.</th>
<th>Centralize (as much as feasible) non-public data to the GSU data center storage or provide tools and best business practices to users.</th>
<th>Person/group responsible for implementing the Process: J.L. Albert, Associate Vice President and CIO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planned activities and target date for implementation of the process:</td>
<td>Create policy document: March 31, 2013 Prior to implementation of policy, consult with internal audit, finance and any other party responsible for controls. Gain policy approval: April 30, 2013 Create Communications plan for policy implementation: April 30, 2013 Implement policy: May 1, 2013 Identify tools for non-centralized data (encrypted thumb drives, encrypted technology for laptops, phone home): March 31, 2013 Acquire funding and purchase tools: June or July 2013 Provide tools to campus: July 2013 Centralize GSU servers to GSU data center: July 1, 2013 – July 1, 2014 Validate data destruction at end of life for portable storage devices, (copiers, external hard drives, laptops, smart phones, notebooks, etc.): June 30, 2013 Incorporate new policy and procedures information into security awareness training: When policies and procedures are final</td>
<td></td>
</tr>
<tr>
<td>Resources Required and possible source:</td>
<td>Access to executive management and legal counsel. Additional funding or financial resources are required for tools and centralization. Tools like Identity finder and encrypted thumb drives should be procured for the university. Reduction in decentralized storage requirements could result.</td>
<td></td>
</tr>
<tr>
<td>Mitigating Activities</td>
<td>Objective</td>
<td>Responsible Party, Planned Activities, Dates &amp; Resources</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>(4) CONTROL OBJECTIVE #2: Expand the Research Data Management Policy to an institution-wide policy.</td>
<td>Determine potential gaps in the data policies.</td>
<td>Person/group responsible for implementing the Process: JL Albert, Associate Vice President and CIO</td>
</tr>
<tr>
<td></td>
<td>Ensure that identified gaps are filled to provide an institution-wide policy.</td>
<td>Planned activities and target date for implementation of the process:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Create appropriate policy documents (data management, data classification, data retention): March 31, 2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prior to implementation of policy, consult with internal audit, finance and any other party responsible for controls.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gain policy approval: April 30, 2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Create procedures, standards, and best practices for data management.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Create Communications plan for policy implementation: April 30, 2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Implement policy: May 1, 2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identify tools for non-centralized data: March 31, 2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acquire funding and purchase tools: June or July 2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provide tools to campus: July 2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Resources Required and possible source: Access to executive management and legal counsel. Additional funding or financial resources are required for tools and centralization. Reduction in decentralized storage requirements could result.</td>
</tr>
</tbody>
</table>

2b. RISK COMPONENT: Users are too likely to respond to phishing attacks and provide sensitive data such as passwords.

(2) CONTROL OBJECTIVE: Increase awareness of information security threats and best practices.

<table>
<thead>
<tr>
<th>Identify gaps in existing information security awareness program.</th>
<th>Shore up security awareness programs to incorporate information concerning phishing threats.</th>
<th>Person/group responsible for implementing the Process: JL Albert, Associate Vice President and CIO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Planned activities and target date for implementation of the process:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incorporate additional information into the student and employee orientation sessions: July 2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Purchase licenses for phishme.com: June or July 2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Initiate awareness training: July 2013</td>
</tr>
<tr>
<td>Mitigating Activities</td>
<td>Objective</td>
<td>Responsible Party, Planned Activities, Dates &amp; Resources</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Resources Required and possible source: Purchasing licenses for Phishme.com will require additional funding.</td>
</tr>
</tbody>
</table>
### GSU RISK REPORT – KEY RISK AREA #3 PERCEPTIONS OF CAMPUS SECURITY

<table>
<thead>
<tr>
<th>Mitigating Activities</th>
<th>Objective</th>
<th>Responsible Party, Planned Activities, Dates &amp; Resources</th>
</tr>
</thead>
</table>
| Key Risk Area #3: **GSU constituents have poor perceptions of campus safety and security.**  
Enterprise Risk Owner: Jerry Rackliffe, SVP Finance & Administration | | |
| 3a. RISK COMPONENT: **Additions of visible security or other uniformed personnel will contribute to improved perceptions of security on campus.**  
(1) CONTROL OBJECTIVE #1: Ensure that adequate numbers of visible uniformed personnel are appropriately allocated at key points on campus. | Evaluate effectiveness of the Panther Ambassador program. Identify whether presence is delivering a benefit to perceptions of campus safety. Consider expansion if warranted.  
Ensure that GSU has optimized presence of police or other uniformed personnel distributed in key areas at times of high student traffic and/or at times of high risk perception (dark) or in poorly perceived areas of campus. | Person/group responsible for implementing the Process:  
Jerry Rackliffe, SVP Finance & Administration  
Planned activities and target date for implementation of the process:  
Complete analysis of Panther Ambassadors program benefits through end of Spring Semester: June 30, 2013.  
Expand program if indicated for Fall Semester 2013: July 31, 2013. |
| | | Resources Required and possible source:  
If warranted, consideration of expanding Panther Ambassadors program, requiring additional contracted personnel. Consideration to have the optimal number of uniformed police personnel as well. |
| 3b. RISK COMPONENT: **GSU constituents may not receive adequate promotion of GSU’s relative safety leading to misperceptions of overall safety and security of campus.**  
(1) CONTROL OBJECTIVE #1: Develop a methodology to track progress of messaging around safety and security on campus. | Survey the university community on safety and use that as a benchmark to determine the impact of future programs.  
Create a survey that can be used over time to gauge progress and impact of safety messaging plans. | Person/group responsible for implementing the Process:  
Don Hale, Vice President Public Relations & Marketing Communications  
Planned activities and target date for implementation of the process:  
Begin meeting with police in summer 2013 to create survey and plan, execute survey in fall 2013. |
| | | Resources Required and possible source:  
Access to police administration, resources to produce and distribute survey to relevant constituents. |
<table>
<thead>
<tr>
<th>Mitigating Activities</th>
<th>Objective</th>
<th>Responsible Party, Planned Activities, Dates &amp; Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop a communications plan in concert with University Police and Facilities to promote an understanding of the safety initiatives already in place as well as future safety initiatives.</td>
<td>Build awareness of safety services available to the campus community and programmatic support offered by the university</td>
<td>Person/group responsible for implementing the Process: Don Hale, Vice President Public Relations &amp; Marketing Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Planned activities and target date for implementation of the process:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Begin meeting with police in summer 2013 in connection with survey creation to create initial messaging plan, incorporate safety and security messaging plan into materials beginning spring semester 2014.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Resources Required and possible source: Access to police administration, resources to produce promotional and messaging materials developed under the plan.</td>
</tr>
</tbody>
</table>
### Key Risk Area #4: Workflow Processes

**Objective:** Workflow processes are either too cumbersome or non-existent leading to inefficiencies in task completion.

**Enterprise Risk Owner:** Matthew Morrison, Director Enterprise Risk Management

<table>
<thead>
<tr>
<th>Mitigating Activities</th>
<th>Objective</th>
<th>Responsible Party, Planned Activities, Dates &amp; Resources</th>
</tr>
</thead>
</table>
| **4a. RISK COMPONENT:** Workflow processes are too cumbersome for certain tasks. | (1) CONTROL OBJECTIVE #1: Identify through interviews of key personnel any workflows that are perceived as too cumbersome. | Person/group responsible for implementing the Process: Matthew Morrison, Director ERM  
Planned activities and target date for implementation of the process:  
Improvements of process implemented and tested: June 30, 2013  
Resources Required and possible source: Access to several College Administrative Officers and other financial management across GSU. No additional funding or financial resources required unless large efficiencies are identified in a manner that a technology solution would assist. |
| Identify core workflow processes that are perceived as cumbersome or not productive. Identify areas where improvement can be made. | Identify and streamline current workflow processes to improve productivity. |  
| | |  |
| (2) CONTROL OBJECTIVE #2: For each cumbersome workflow process, identify elements of the process that are necessary controls to ensure that any proposed process improvements do not impair controls. | Person/group responsible for implementing the Process: Matthew Morrison, Director ERM  
Planned activities and target date for implementation of the process: Prior to implementation of revised policies, consult with internal audit, finance and any other party responsible for controls. Complete prior to June 30, 2013.  
Resources Required and possible source: Access to internal audit and other financial management across personnel GSU. No additional funding or financial resources anticipated. |  |
<table>
<thead>
<tr>
<th>Mitigating Activities</th>
<th>Objective</th>
<th>Responsible Party, Planned Activities, Dates &amp; Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify areas where a lack of core workflow processes impede productivity.</td>
<td>Identify if any areas where productivity would be improved by the creation of a new policy, process or procedure.</td>
<td>Person/group responsible for implementing the Process: Matthew Morrison, Director ERM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Planned activities and target date for implementation of the process:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New processes implemented and tested: June 30, 2013.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Resources Required and possible source:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access to several College Administrative Officers and other financial</td>
</tr>
<tr>
<td></td>
<td></td>
<td>management across GSU. No additional funding or financial resources required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unless large efficiencies are identified in a manner that a technology solution would assist.</td>
</tr>
<tr>
<td>Mitigating Activities</td>
<td>Objective</td>
<td>Responsible Party, Planned Activities, Dates &amp; Resources</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Key Risk Area #5: GSU would be adversely affected by not maximizing availability of appropriations under the funding formula.** Enterprise Risk Owner: Tim Renick, Associate Provost Enrollment & Academic Affairs | **5a. RISK COMPONENT: Maintaining and improving retention, progression and graduation metrics in a declining resource environment.**  
(1) CONTROL OBJECTIVE #1: Increase the number of students who reach the point of degree conferral while minimizing time and credit hours to degree. | Implement new advising procedures to identify students who are off track for degree conferral at the earliest possible time.  
Facilitate students’ ability to meet graduation requirements while minimizing courses that do not apply to their degree programs.  
Person/group responsible for implementing the Process: Tim Renick, Vice Provost and Chief Enrollment Officer  
Planned activities and target date for implementation of the process: Implementation of a new advising process based on the initiation a web-based advising tracking system to quickly identify off-track students, as well as the hiring and training of 42 advisors. Implementation will be complete April 1, 2013.  
Resources Required and possible source: New web-based advising system (vendor and resources already secured), 42 new advisors (resources identified, hiring is underway), new space to house the University Advisement Center (space secured in the 25 Park Place building; move-in is underway). **(2) CONTROL OBJECTIVE #2: Reduce the number of continuing students who drop out or stop out because of a lack of sufficient funds.** | Develop means of maximizing the impact of scholarship and financial aid dollars  
Implement data-based processes for the awarding of need-based aid to increase student retention and graduation  
Person/group responsible for implementing the Process: Tim Renick, Vice Provost and Chief Enrollment Officer  
Planned activities and target date for implementation of the process: Deploy additional scholarship funds through data analysis from the Office of Financial Aid and the Office of Student Retention. Use predictive models for student success to create the most efficient use of available funds, including the expansion of the Panther Retention Grant Program to restore students to classes who have been dropped due to insufficient funds and Keep Hope Alive to help students who has lost the Hope Scholarship. Process is ongoing and phases are already being implemented. We will conduct a full assessment of progress by...
<table>
<thead>
<tr>
<th>Mitigating Activities</th>
<th>Objective</th>
<th>Responsible Party, Planned Activities, Dates &amp; Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>July 1, 2013.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Resources Required and possible source:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIF funding and scholarship funds from the GSU Foundation; the collaboration of the Office of Financial Aid, the Scholarship Office, the Office of Student Retention, and Institutional Research. As part of GSU’s 2012 Completion Plan for Complete College Georgia, these efforts are already underway.</td>
</tr>
<tr>
<td>(3)</td>
<td>CONTROL OBJECTIVE #3: Increase the number of at-risk freshmen who progress in timely fashion to the point of graduation.</td>
<td>Ensure that at-risk freshmen have the greatest opportunity for academic success. Increase the number and percent of freshmen who reach the point of degree conferral, especially among students in at-risk populations such a first-generation, low-income and underrepresented students.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Person/group responsible for implementing the Process: Tim Renick, Vice Provost and Chief Enrollment Officer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Planned activities and target date for implementation of the process: Develop a 7-week Summer Success Academy for fall freshmen applicants who the data show will have low likelihoods of progression without early interventions. The program was piloted Summer 2012 with excellent results. Full implementation: Summer 2013.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Resources Required and possible source: Programming and scholarship support (funds have been identified). Staffing to provide students with frequent and proactive academic support throughout the program; we will be using the 42 new advisors hired under the initiative described in Objective 1 to support an expanded number of Summer Success Academy students. As part of GSU’s 2012 Completion Plan for Complete College Georgia, these efforts are already underway.</td>
</tr>
</tbody>
</table>