

Starting an Enterprise Risk Management Program from Scratch: A Case Study

Alan Hansen – Broward College

Scott Wightman – Gallagher

Agenda

1. Enterprise Risk Management (ERM) Overview and Its Role in Governance
2. ISO 31000 – The International Risk Management Standard
3. Risk Ownership Model
4. Generic Implementation Plan
5. Broward College: A Case Study

ERM Overview and Its Role in Governance

Risk

Traditional Definition

The possibility
that something
bad or
unpleasant will
happen.

Merriam-Webster

Risk Management

Traditional Definition

Minimizing the
adverse effects
of accidental
losses.

The Institutes

Risk

Broadened Definition

Risk

Broadened Definition

The effect of
uncertainty on
objectives.

ISO 31000

Risk Management

Broadened Definition

Coordinated
activities to direct
and control an
organization with
regard to risk.

ISO 31000

Why is Risk Management Important?

1.

All organizations exist to achieve their objectives.

2.

Many internal and external factors affect those objectives, causing uncertainty about whether the organization will achieve its objectives.

3.

The effect this uncertainty has on an organization's objectives is "risk."

Why is Risk Management Important?

1.

All organizations exist to achieve their objectives.

2.

Many internal and external factors affect those objectives, causing

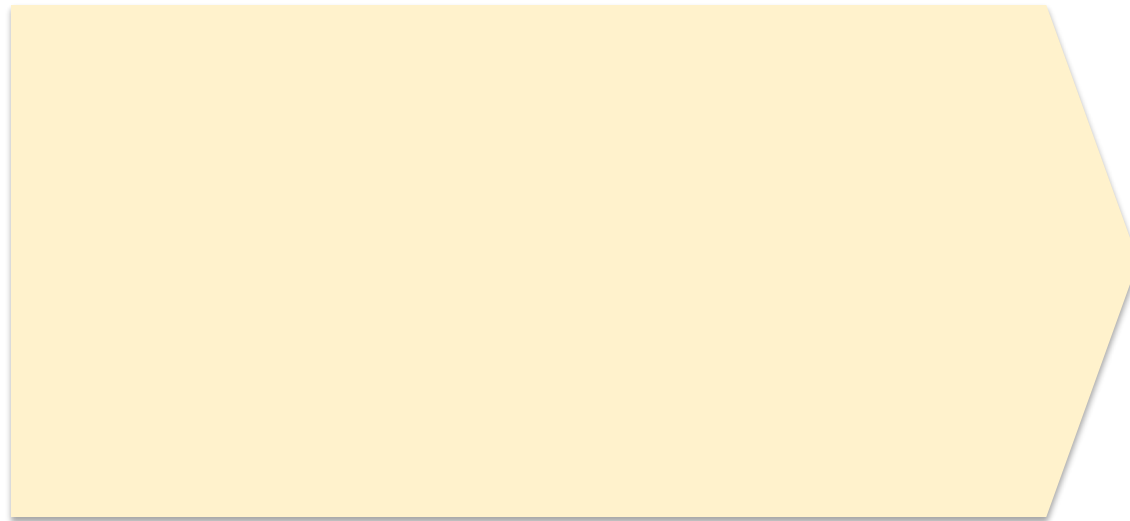
3.

The effect this uncertainty has on an organization's objectives is "risk."

In summary, the management of risk is central to the livelihood and success of all organizations.

achieve its objectives.

The *New View* of Risk



The *New View* of Risk

RISK can be a threat or opportunity

The *New View* of Risk

RISK can be a threat or opportunity

Anything that can harm, prevent, delay, **or enhance** an organization's ability to achieve objectives = RISK

The *New View* of Risk



The *New View* of Risk

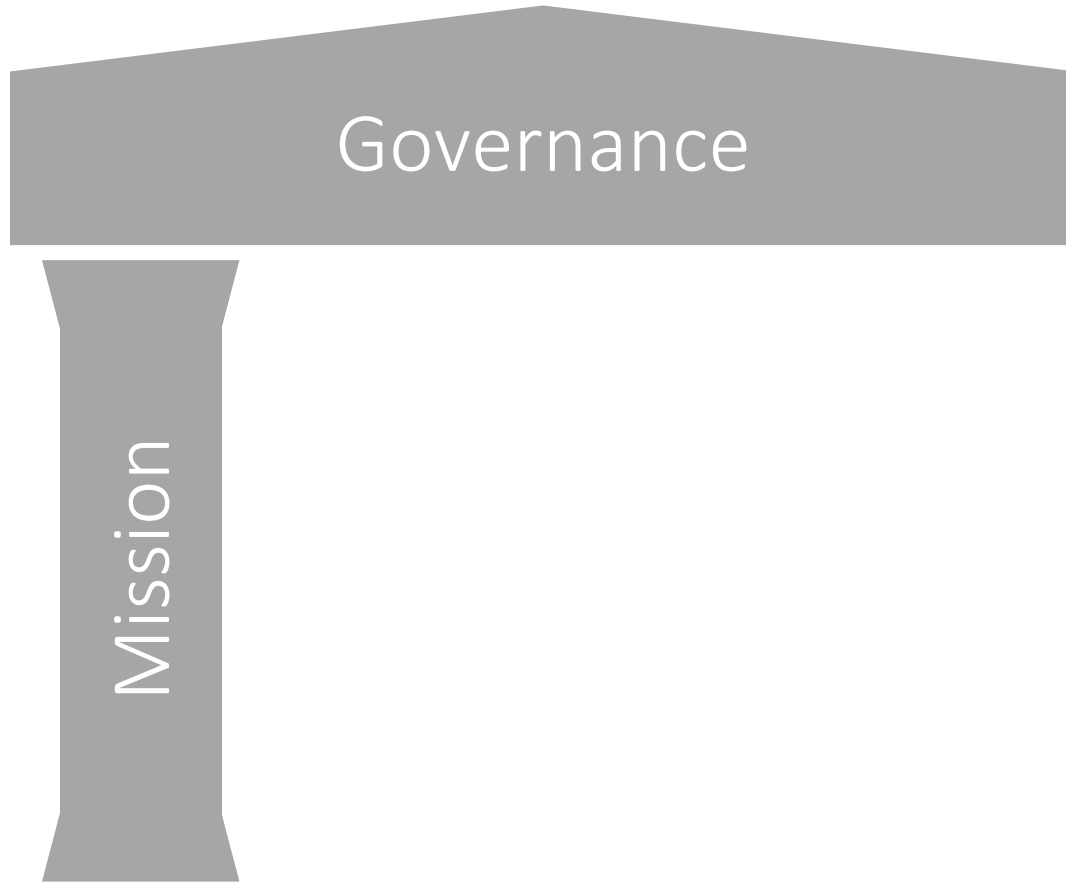


Risk Management as an Integral Pillar of Governance



Governance

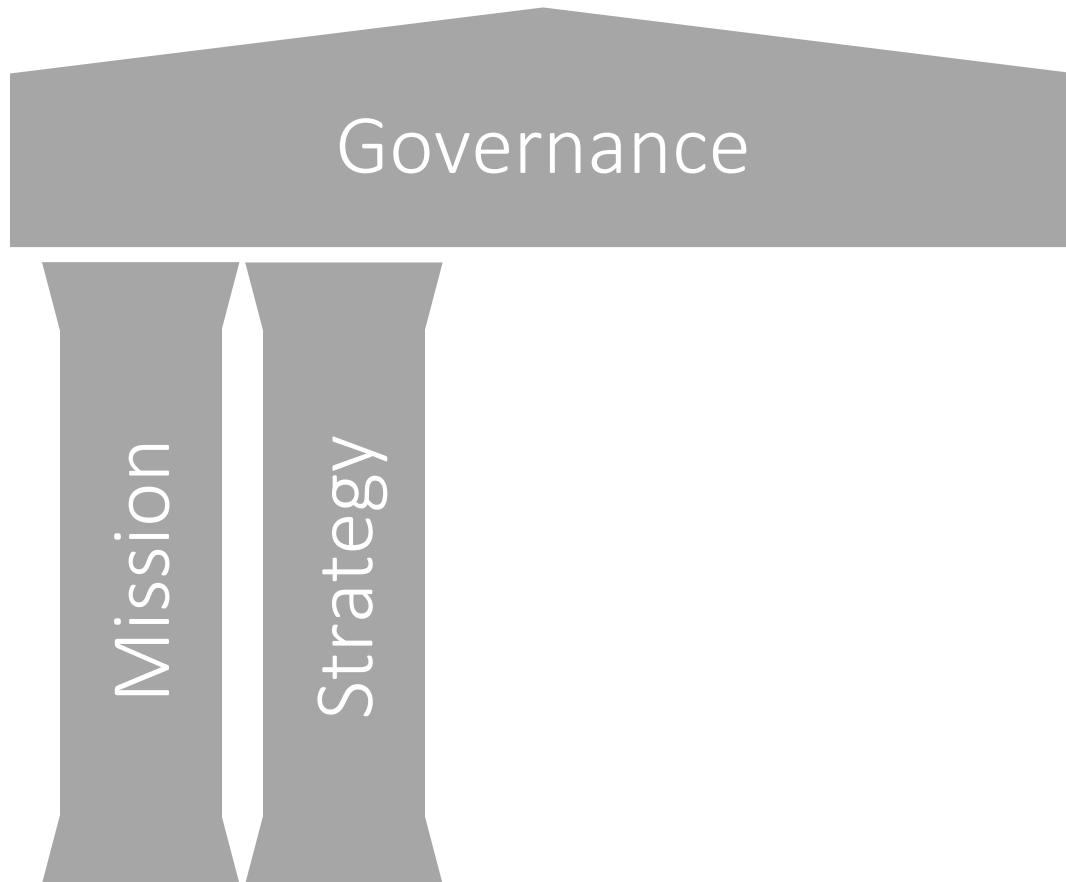
Risk Management as an Integral Pillar of Governance



Mission

The board sets the overall mission and objectives of the organization and insists that its culture and values are aligned with that mission.

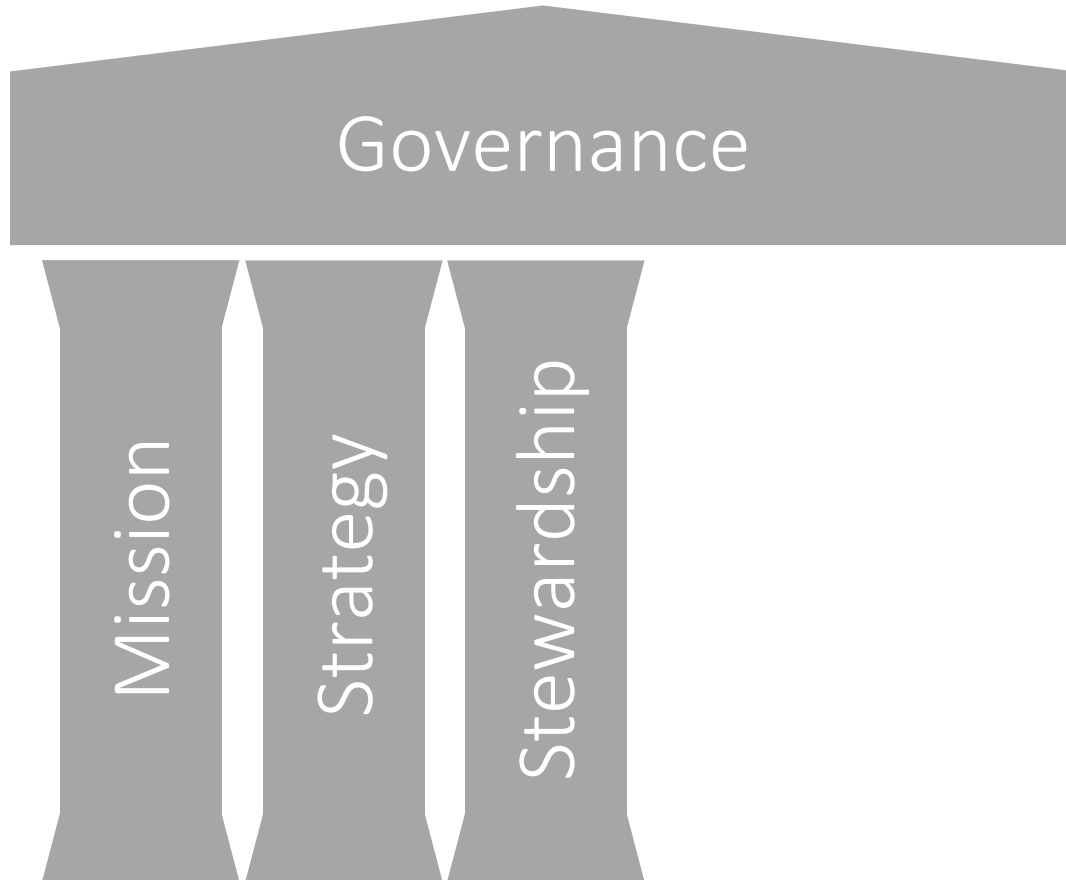
Risk Management as an Integral Pillar of Governance



Strategy

Senior leadership, in conjunction with the board, develop strategic plans to carry out the organization's mission and objectives.

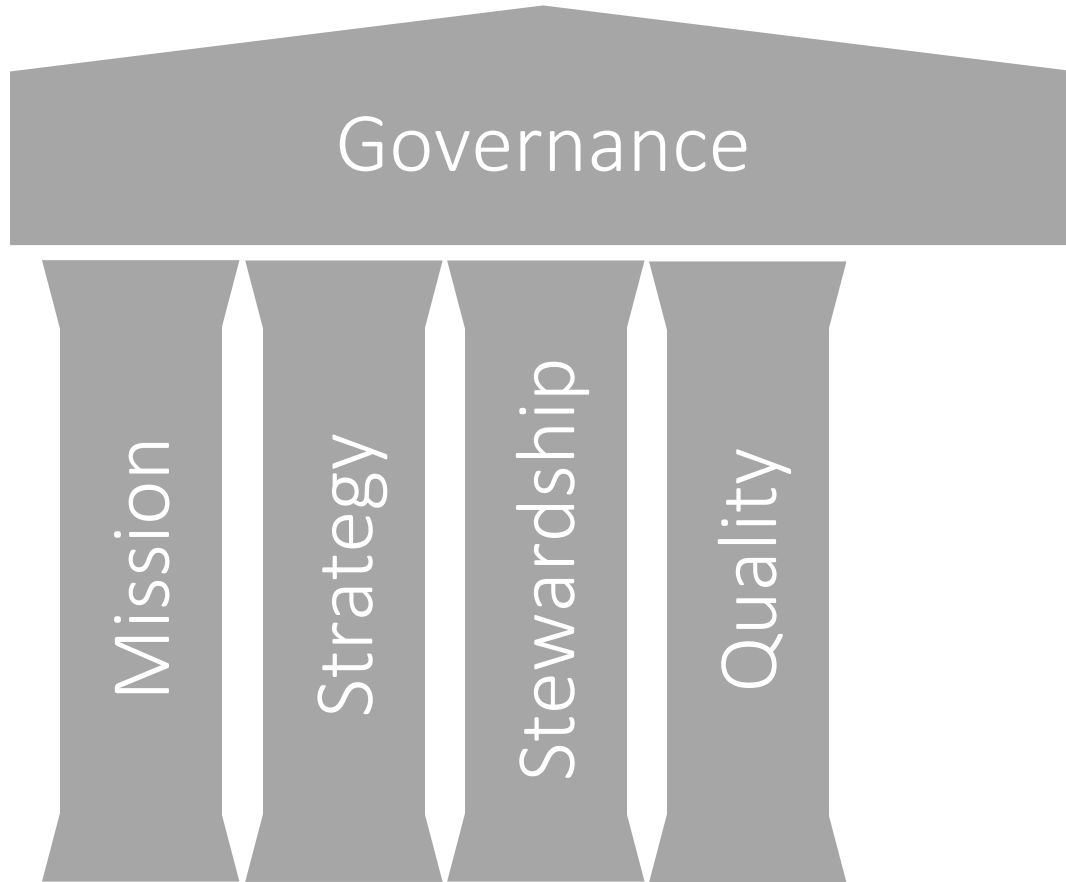
Risk Management as an Integral Pillar of Governance



Stewardship

Financial resources are developed and maintained to ensure the mission and strategic plans are adequately funded.

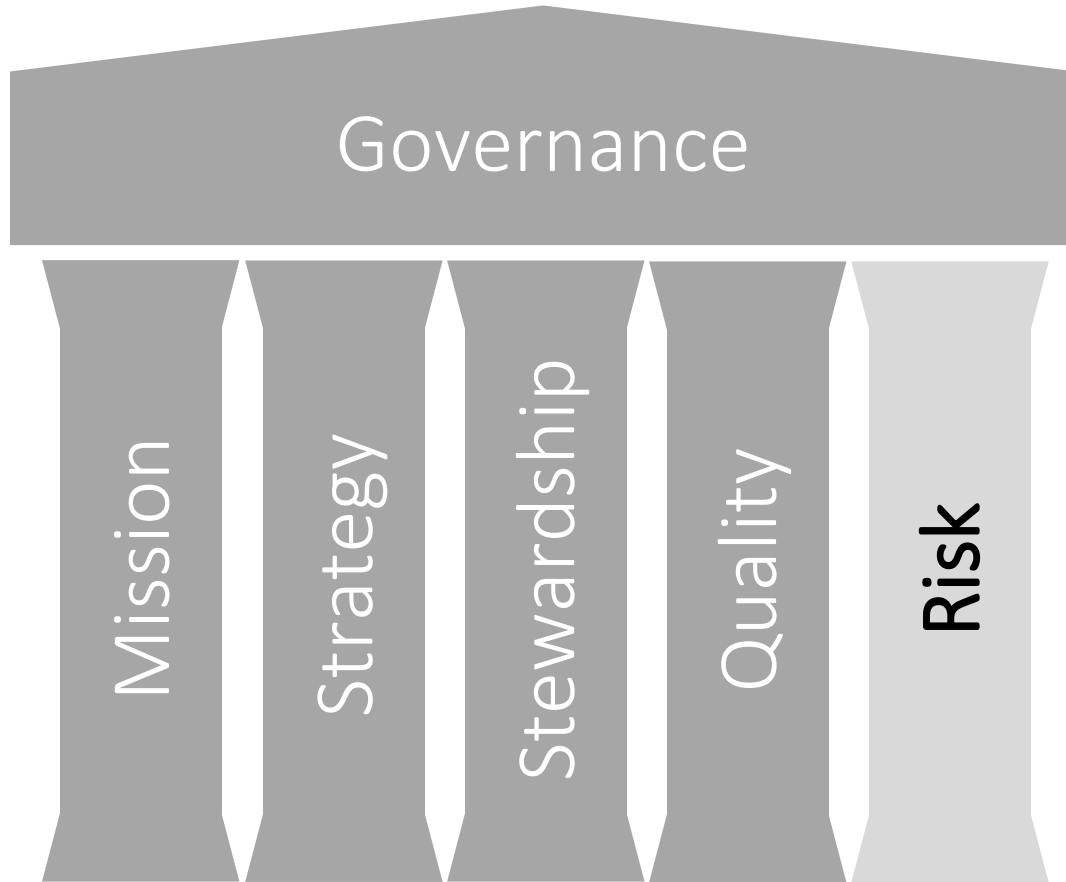
Risk Management as an Integral Pillar of Governance



Quality

The quality of the organization's programs are planned for and tested in order to maintain demand for the "product" in the long-term.

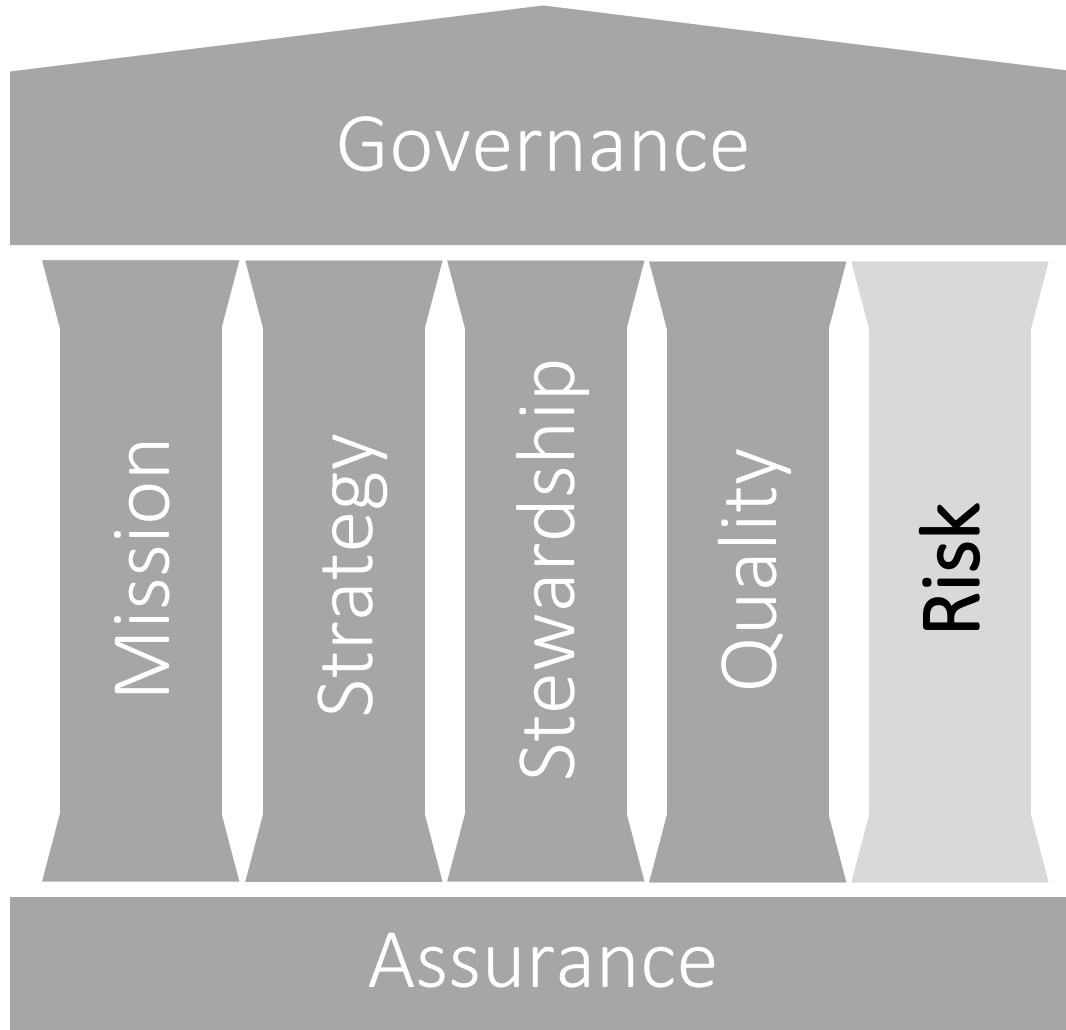
Risk Management as an Integral Pillar of Governance



Risk

Risks to the organization in meeting its organizational objectives, including threats and opportunities, are identified, assessed, and treated.

Risk Management as an Integral Pillar of Governance



Assurance

A strong management structure and culture is maintained to ensure proper reporting and accountability, and internal and external audits are utilized to bring board assurance.

ISO 31000

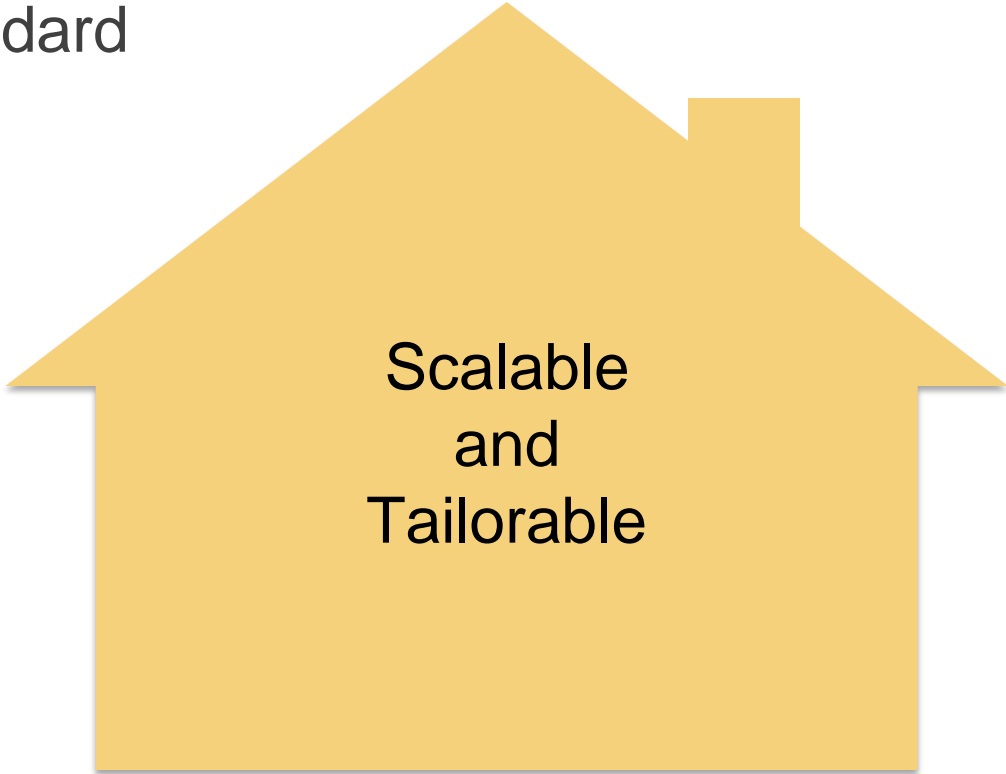
ISO 31000

The International
Risk Management
Standard



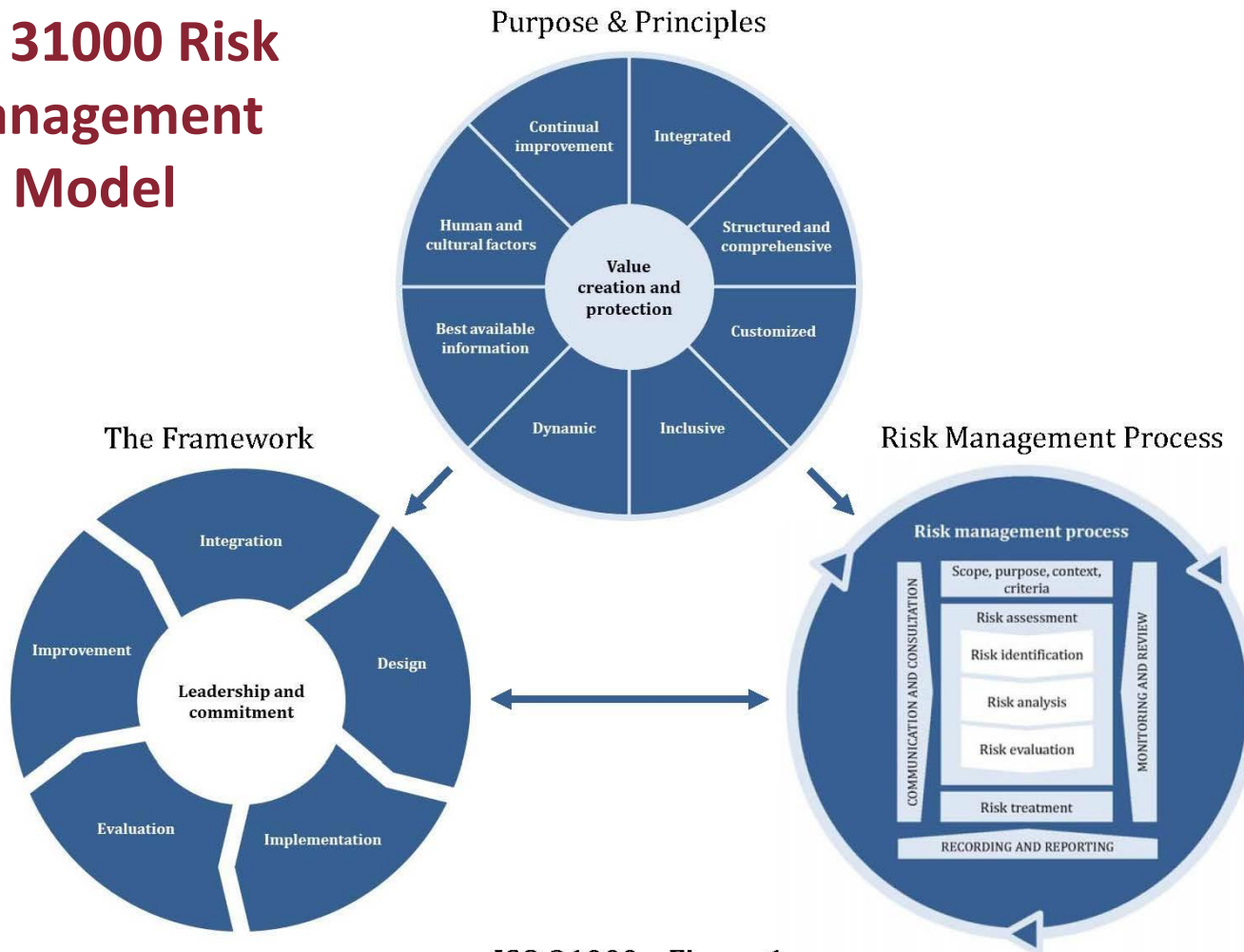
ISO 31000

The International
Risk Management
Standard



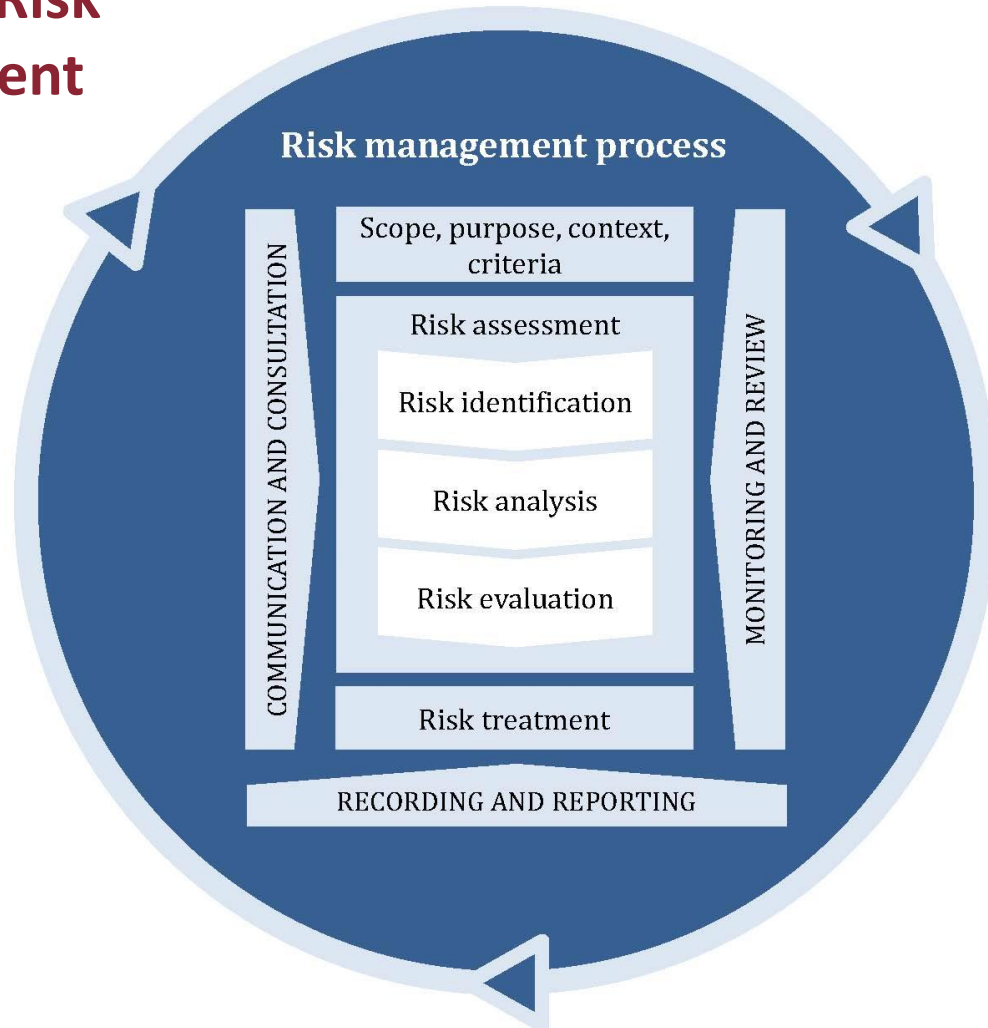
Scalable
and
Tailorable

ISO 31000 Risk Management Model



ISO 31000 – Figure 1

ISO 31000 Risk Management Model



Risk Ownership Model

Centralized Oversight- Decentralized Implementation

		Oversight	
		Centralized	Decentralized
Implementation	Centralized	Where some have developed, but centralized implementation requires significant staff and does not take advantage of current subject matter expertise	
	Decentralized	Oversight is at highest levels, including board, but implementation is pushed out to experienced subject matter experts through risk and compliance “ownership”	Where most entities have been, although with some limited departmental oversight, but does not incorporate board-level reporting and accountability

Employment of “Ownership” Model is Critical

- Pushing work out to subject matter experts is essential to success
- Risk owners and compliance obligation owners:
 - Develop risk treatment and compliance assurance plans
 - Assemble work teams
 - Communicate and report
 - Monitor and evaluate
- At what level of the organization should ownership reside?

Administrative Tools

- Spreadsheets
- Enterprise software
- Governance, Risk & Compliance (GRC) software
 - As part of RMIS
 - As stand-alone cloud system

Functions to look for:

- Detailed risk and compliance obligation registers with multiple data points
- Dashboards for each risk and obligation with the ability to rank risks and catalogue treatment plans
- Risk rankings that flow into interactive, institutional heat maps
- Ability to manage delegations using email assignments and workflow through calendars
- Reporting tools for use at all levels of the organization

Generic Implementation Plan

Generic Implementation Plan

Common ERM Implementation Steps

Implementation Step Descriptions and Recommended Output

1	Laying the Groundwork	Build the case for ERM, understand the level of <i>Mandate and Commitment</i> from senior leaders and the governing board, review roles and capabilities, and begin the work to develop a sustainable framework.
2	Design a Risk Management Framework	Develop a written <i>Risk Management Framework</i> document which answers two primary questions: 1) Why do we manage risk at our organization? and 2) How do we manage risk at our organization?
3	Form and Train a Risk Committee	Pull together a <i>Risk Committee</i> or other group of leaders for training and initial discussions regarding implementation steps, implementation step owners, and timelines.
4	Develop an Initial Risk Register	Through group brainstorming and/or structured interviews with key stakeholders – with or without the help of an industry sample list of risks – begin outlining the universe of risks facing the organization. The output will be an initial <i>Risk Register</i> .
5	Rank Risks on Likelihood and Impact	Using the established risk register, rank each risk on its: 1) likelihood of occurrence, and 2) impact on the organization. The output will be a traditional <i>Heat Map</i> , highlighting the risks creating the greatest uncertainty around the organization meeting its objectives.
6	Assign and Train Risk Owners	In order to decentralize the implementation process to subject matter experts throughout the organization, assign <i>Risk Owners</i> to each risk and train them on their responsibilities.

Generic Implementation Plan

7	Develop Risk Treatment Plans	Request that each risk owner develop a narrative <i>Risk Treatment Plan</i> designed to reduce the uncertainties of meeting the organization's objectives for each assigned risk.
8	Delineate Specific Controls and Actions from Treatment Plans	Risk owners should then break down each risk treatment plan into specific controls, and those controls into particular action items, creating a <i>Risk-Control-Action Hierarchy</i> .
9	Develop Reporting and Accountability	In order for any ERM program to sustain itself overtime, the following must be embedded into the process: 1) regular <i>Reporting</i> to senior leaders, and 2) <i>Accountability</i> for risk owners.
10	Generate Communication Plan	A <i>Communication Plan</i> is important to make sure ERM principles and practices are embedded into the organizational culture overtime.
11	Monitor and Review Risk Management Process Components	The risk register, heat map, risk ownership, and risk treatment plans must remain dynamic. Many organizations will build their <i>Risk Management Process Review</i> into an established business process such as strategic planning or budgeting.
12	Monitor, Review and Continually Improve Framework	The organization should monitor, review and continually improve the <i>Risk Management Framework</i> developed in the second step above. This review would focus on governance, accountability, process management, and any further efficiencies possible.

Broward College: A Case Study

Broward College



- Est. 1957
- 13 locations across Broward County, in South Florida
- 68,000+ students per year
- Launched ERM in 2019





What I Needed to Launch ERM...

- Affordable
- Easy to manage at all levels
- Software (user friendly)
- Efficient (workload low, return high)
- Champion/Lobbyist
- Integrate
 - Pre or post-launch
 - Consider existing cycles when setting ERM cycle and dates

ERM Organization at Broward College



ERM at Broward College

Risk Owner

- Document & Develop Controls
- Risk Treatment Plan
- Drives Risk Assessment & Identification

ERCM Committee

- Quarterly Meeting
- Oversight
- Resources

Executive Team

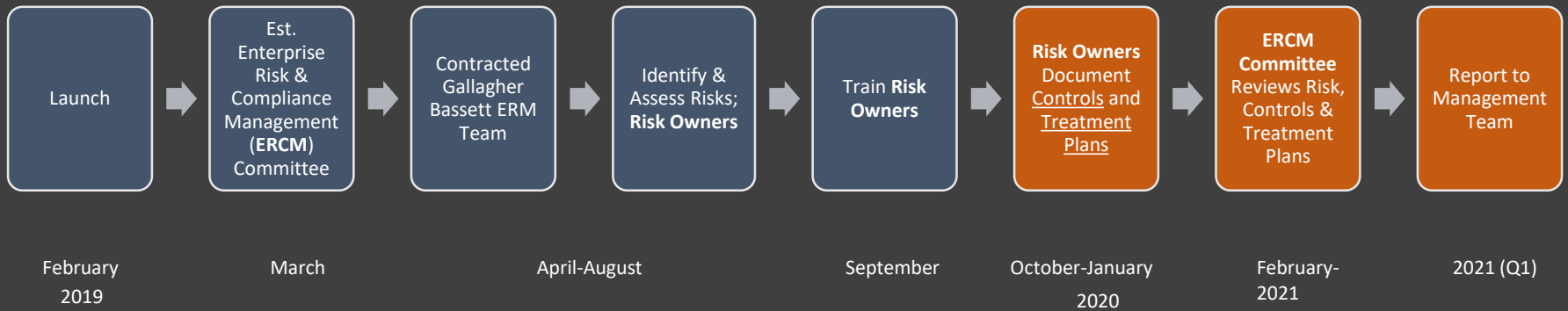
- Annual Report
- Additional Resource Support

ERM Update to ERCM 2/10/2021



- Implementation Timeline
- Heat Map
- Annual Risk Reviews
 - Summary of Changes as of 2/10/21
- ERCM Risk Review Schedule
- Refresher on ERCM Risk Review

ERM Implementation Timeline



Sample Heat Map (2019)



Broward College RISKMAP

RISK LIKELIHOOD	5–Almost Certain Normally occurs at least annually	Lack of Athletics Success Asset Management Controls Employee Grievance/Complaint Procedures Staff Quality	Employee Discrimination and Harassment	Protection of Minors Door Security/Access Control Inappropriate Relationship Between Faculty and Students Campus Emergency Preparation	Employee Compensation Structure Failure of Communication System Personal Information Protection	
	4–Likely Likely to occur in next 3 years	Facility Infrastructure Failure State Setting of Tuition Sunshine Law Compliance Employee Travel Incident	Financial and Economic Factors Federal and State Funding Strategic Workforce Planning Vehicle Accident Involving Institution Driver Physical Security Measures Student Alcohol and Drug Abuse	Recruiting Diverse Student Populations Improper Use of Gifts Fundraising Goals Environmental Incident eDiscovery Response Failure of IT System to Continue Services Accident with Contracted Transportation	Student Retention Equitable Academic Experience Decline in Student Applications Unfunded Mandates Workplace Violence	
	3–Possible May occur every 10 years	Third Party Intellectual Property Rights	Diversity in Curriculum Inaccessibility of Facilities Construction Controls Building Safety Code Compliance Reporting to Department of Education Vendor Contract Management Copyright and Fair Use Policies	Aligning Curriculum with Demand Academic Freedom Policies Lack of Grant Compliance Loss of Grant Funding Academic Misadvisement Media and Social Media Portrayals Depletion of Endowment Principal Serious Workplace Injury Management of Unrestricted Reserve Fund Depletion of Investment Principal Disproportionate Enrollment of Students with Financial Need Board Duties, Orientation, Assessment Ineffective Insurance Protection	Financial Aid Compliance Food Safety Off Campus Volunteering Alumni Engagement	Student Financial Aid Compliance Maintenance of Full Board Violence by Terrorist or Other Intruder Counseling Services
	2–Unlikely Unlikely in foreseeable future		Long-Term Debt Plan Internal Theft Controls CEO Compensation and Assessment Free Speech Rights Consistency in Student Organizations	Athletics Program Compliance Inconsistent Naming Policies Alumni Program Vendors Corporate Community Partnerships Tax Compliance Management Campus Crime Awareness	Balance of Traditional and Online Learning Student Records Enrollment Beyond Capacity Athletics Injury Response Equitable Athletic Experience Acceptance of Impaired Real Estate Budget Errors or Inadequate Modeling Cash Management Control Faculty and Staff Diversification Campus Crime Regulatory Requirements Student Judicial Process	Experiential Learning Partners Unrestricted Fund Balance Management Excessive Use of Force Student of Concern Student Sex Discrimination, Harassment or Violence
	1–Rare Has occurred in higher ed, but is rare		Hiring of Non-Qualified Employees Pandemic Incident		Health Center Medical Error	Loss of Accreditation
		1–Insignificant No measurable impact on the organization	2–Minor Impact on the organization will last only for days	3–Moderate Impact on the organization may last for weeks	4–Significant Impact on the organization may last for months	5–Critical Impact on the organization may last for years

ORGANIZATIONAL IMPACT



Annual Risk Review

- First Annual Reviews January 2021
 - Planned for January each year, 1-1.5 hours per meeting (some one-on-one, but mostly by department)
- Risk Management will meet with risk owners in each risk category to:
 - Review institutional risks we've already identified (scoring, risk descriptions)
 - Identify new risks, or remove risks
 - This year's meetings include time to work on completion
- In advance of budget prep
 - Updated scoring, risk treatment plans
 - Institutional Risk considerations part of budget process

Summary of Changes (as of 2/10/21)

	2020 Q4	2021 Q1	Change
Institutional Risks	111	109	-2
Controls	200	341	+141
Completion Rate	51%	85%	+34%
ERCM Review	37% (11/30)	42% (13/31)	+5%
Scores Increased		14*	
Scores Decreased		8*	

** Annual Review still in progress, will complete in February*

2020/2021 ERCM Committee Review

August 2020	November 2020	February 10, 2021	May 12, 2021
<i>Campus Emer. Prep – S&EP</i> <i>Workplace Violence – S&EP</i> <i>Viol by Intrud or Terrst – S&EP</i>	<i>Maint. Full BOT – GC</i> <i>Unfunded Mandates - GC</i> <i>Failure of IT to Cont Serv – IT</i>	<i>Employee Discrim & Harassmnt – TC</i> <i>Inapp Relations Fac/Stu – TC</i>	- - - -

Require Initial Committee Review (score 15+)

Student Attrition – AA
Equitable Acad Experien – AA
Experiential Learning Env – AA
Door Sec/Access Control – FAC

Protection of Minors – SS
Recruiting Diverse Stu Popul – SS
Retirement Program Mngmt – TC
eDiscovery Response – IT
Federal & State Funding - GC

Federal Fin. Aid Compl – FIN
Improp. Use of Gifts – ER
Fundraising Goals – ER
Environ. Incident – EH&S
Inaccessibility of Academic Programs - IT



What will ERCM review?

- ERCM to review:
 - Controls
 - Risk Treatment Plan
- ERCM review a venue to discuss individual risks with risk owners
- ERCM to consider facilitation of risk owner's risk treatment plan.



Potential Questions for Risk Owner

- Have we captured all existing Controls?
- Does Current Control Effectiveness feel right in light of Risk Rating and existing Controls?
- Does the Risk Treatment Plan have clear action items?
- Can ERCM committee offer support to Risk Owner on Risk Treatment Plan?

ERM at Broward College



BROWARD COLLEGE
Powered by Gallagher ERM | Hi, Alan Hansen

My Apps | ERM- Broward College | New App

Home | Users | ERM Management Team | Submit A Risk | **Manage Risks** | Manage Controls | Manage Actions | Manage Obligations | Manage Compliance E... | Document Templates | Document Subtables | Attachments | KRI | Risk Rankings | Calculations | New Table

Manage Risks > Vehicle Accident Involving Institution Driver | + New Risk | Edit | Email | More | Customize this Form

Risk | Controls | < Prev | Return | Next >

Enterprise Risk Management

Complete all fields on this form.

Risk Identification

Risk Identification is the process of finding, recognizing, and recording risks.

- Risk Name**
Vehicle Accident Involving Institution Driver
- Risk Description**
Lack of training and policy enforcement leading to vehicle accident caused by employee or student, resulting in legal liability, property damage, or reputational harm.
- Risk Owner**
Alan Hansen
- Other Team Members (Optional)**
Marileidy Campusano

Risk Analysis

Risk Owners are asked to complete both the Risk Type and Impacted Organizational Objectives fields. These two fields are drop down fields, please select all that apply. Some fields are locked, to change a score for Likelihood or Impact a Risk Owner will need to contact Risk Management.

Risk Likelihood 4	Risk Impact 3	Risk Rating 12
-----------------------------	-------------------------	--------------------------

See Ranking History

Risk Category Risk Management | **Risk Type** Financial | Operational | Reputational | Safety | **Impacted Organizational Objectives**

Insurability Insurable

Risk Evaluation

Risk Owners are asked to complete this section after they are finished entering Controls. Below Risk Owners will evaluate the overall control effectiveness.

- Current Control Effectiveness** Adequate Controls
- Communication Plan** Present revised policy to committee, connect with CTEL to evaluate training delivery through new MyLearning site, consult with ERCM committee on whether to make driver training mandatory and revisions to driver eligibility criteria.

Risk Treatment Plan (What we plan to do)

Risk Owners are asked to develop a Risk Treatment Plan to address any planned or future mitigation efforts (new/revised policy, procedure, training, etc.) The Risk Treatment Plan is where we document what we plan to do beyond the Current Controls we have in place now. BULLET POINT FORMAT PREFERRED

- Current Risk Treatment Plan**
 - Revise policy/procedure 6Hx2-7.07 to reflect administrative changes, geographical restrictions for college vehicle use, and driver eligibility criteria.
 - Review driver eligibility criteria and revise as needed to increase focus on high risk indicators in driver history, as opposed to catch all criteria.
 - Work with CTEL to deliver driver training through MyLearning platform and consider making training mandatory.

ERCM Review

This section for ERCM Committee Chair use

Date of last ERCM review 02-12-2020

ERM at Broward College



BROWARD COLLEGE Powered by Gallagher ERM | Hi, Alan Hansen

My Apps | ERM- Broward College | New App

Home | Users | ERM Management Team | Submit A Risk | Manage Risks | Manage Controls | Manage Actions | Manage Obligations | Manage Compliance E... | Document Templates | Document Subtables | Attachments | KRI | Risk Rankings | Calculations | New Table

Manage Risks > **Vehicle Accident Involving Institution Driver** + New Risk | Edit | Email | More | Customize this Form

Risk | **Controls** < Prev | Return | Next >

▼ **Current Controls (What we're doing now)**

This is where Risk Owners are asked to list the things we are doing now to mitigate this risk. Please add any controls that help mitigate the risk. i.e. Policy/Procedure, Training, Insurance...

Add Control # of Controls: 4

Full Report | Grid Edit | Email | More ▼ 4 Controls

	Risk Name	Control Type	Control Name	Control Owner	Control Description
Vehicle Accident Involving Institution Driver (4 Controls)					
<input type="checkbox"/>	Vehicle Accident Involving Institution Driver	Insurance	Insurance	Alan Hansen	The college is insured through a combination General & Auto liability policy as part of the Florida College System Risk Management Consortium (FCSRMC) self-insurance pool with a \$0 deductible with limits up to \$200,000/\$300,000 to match the protections afforded by FS 768.28 (Sovereign Immunity). In addition, the college has excess insurance with limits of \$800,000/\$3,200,000 that would be available should the protections afforded by FS 768.28 are unavailable.
<input type="checkbox"/>	Vehicle Accident Involving Institution Driver	Policy/Procedure	Policy & Procedure - Use of College Vehicles	Alan Hansen	College policy 6Hx2-7.07.pdf and Procedure A6Hx2-7.07 outline the permissible use of college vehicles and the set driver eligibility criteria. http://www.broward.edu/legal/policies/Section%20Template/6Hx2-7.07.pdf http://www.broward.edu/legal/policies/Section%20Template/A6Hx2-7.07.pdf
<input type="checkbox"/>	Vehicle Accident Involving Institution Driver	Training	Training	Alan Hansen	There are two voluntary driver trainings available. Both the Defensive Driving Course and the Utility Vehicle/Golf Cart Operator Safety Course are available through the Environmental Health & Safety (EH&S) Department.
<input type="checkbox"/>	Vehicle Accident Involving Institution Driver	Other	Background Checks	Alan Hansen	Authorized drivers' history as per Florida Dept. Highway Safety & Motor Vehicles reviewed prior to authorization and periodically (annually at minimum). Eligibility criteria established per procedure A6Hx2-7.07. http://www.broward.edu/legal/policies/Section%20Template/A6Hx2-7.07.pdf

Generate Heat Map Document

Where We Are Now & What's Next



- Where we Are Now:
 - In 3rd annual cycle
 - Annual ERM Review Cadence
 - Integrated with Budget Cycle
 - Managed Risk Owner reassignments
- What's Next:
 - Maturing the program
 - Compliance using the ERM model
 - Key Risk Indicators (KRI)
 - Consider opportunity in addition to threat



What Went Well

- Standardization of risk language/understanding
 - Likelihood/Impact, Controls
 - Risk Owners, ERCM Committee Members, and Executive Team associating risks with a Risk Owner
 - Sharing ideas, knowledge of existing controls
- Acceptance
 - Champion
 - Luck
 - Presentation
 - Simplicity
- Industry Specific Sample Risk Register

Challenges



- Have we captured all existing Controls?

Thank You!