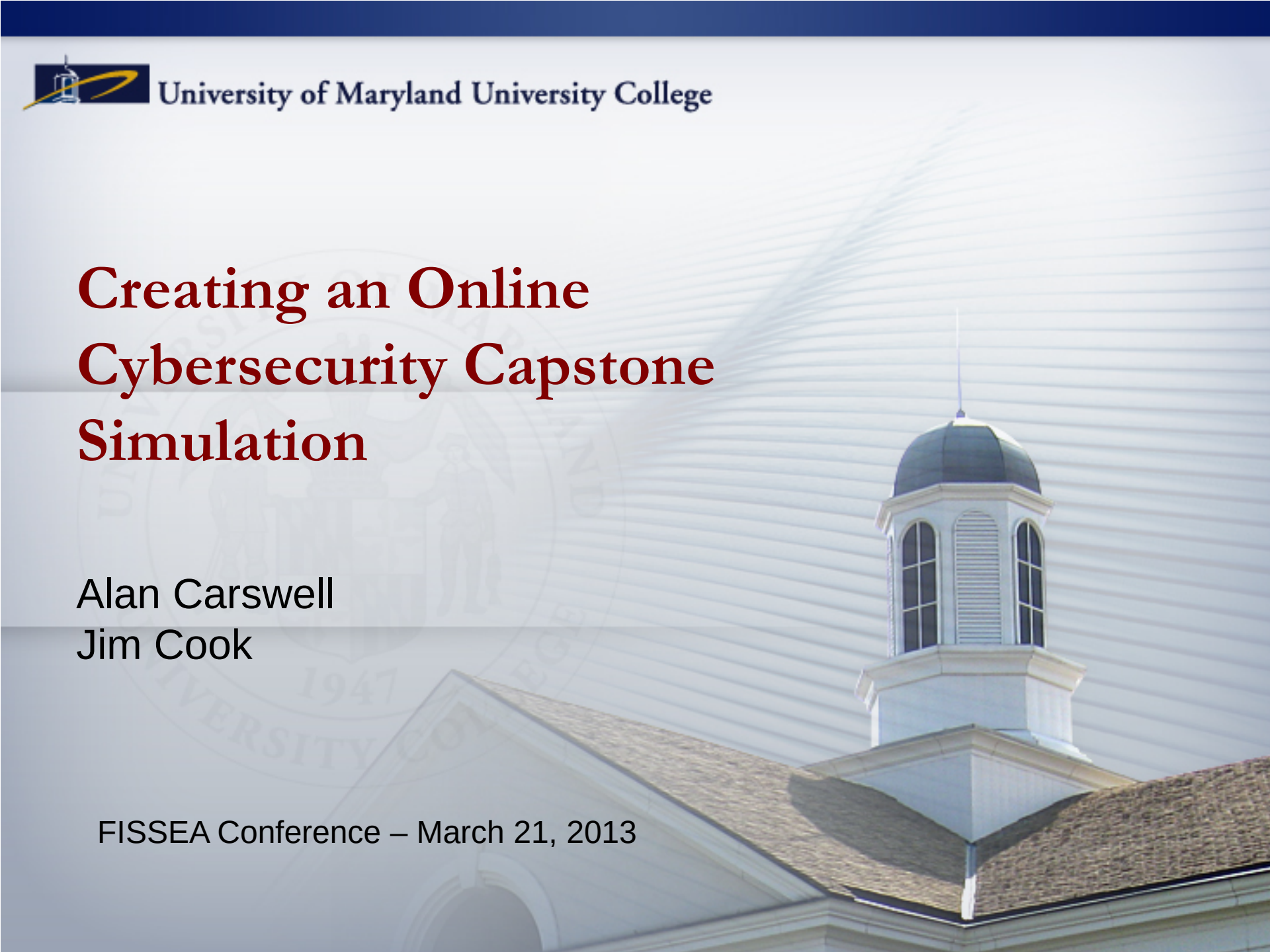
University of Maryland University College

Creating an Online Cybersecurity Capstone Simulation

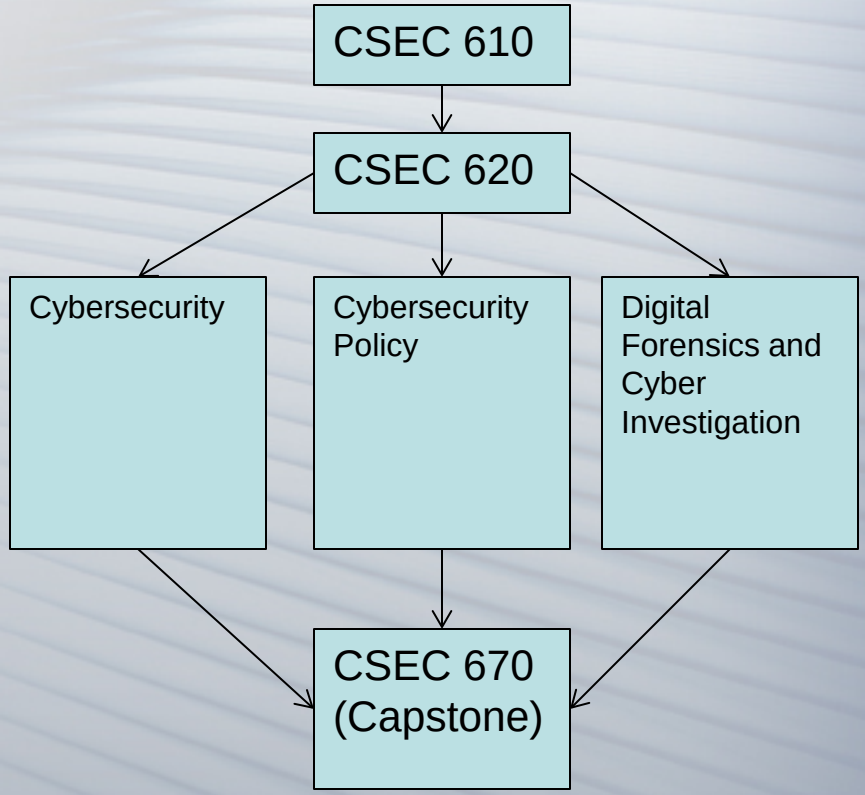
Alan Carswell
Jim Cook



FISSEA Conference – March 21, 2013

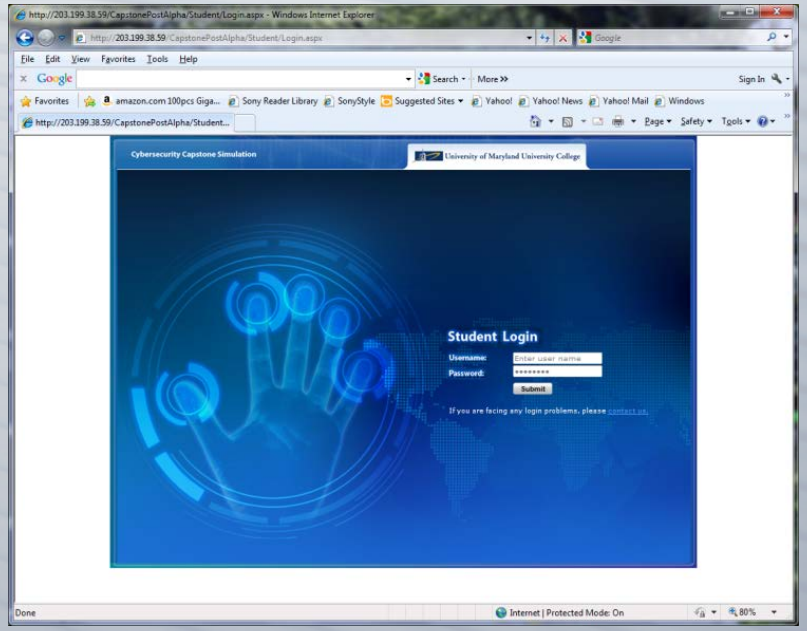
Overview

- Cybersecurity Programs
  - MS in Cybersecurity
  - MS in Cybersecurity Policy
  - MS in Digital Forensics and Cyber Investigation
- Six-credit courses
- 100% online
- Interdisciplinary
- Simulation a part of CSEC 670

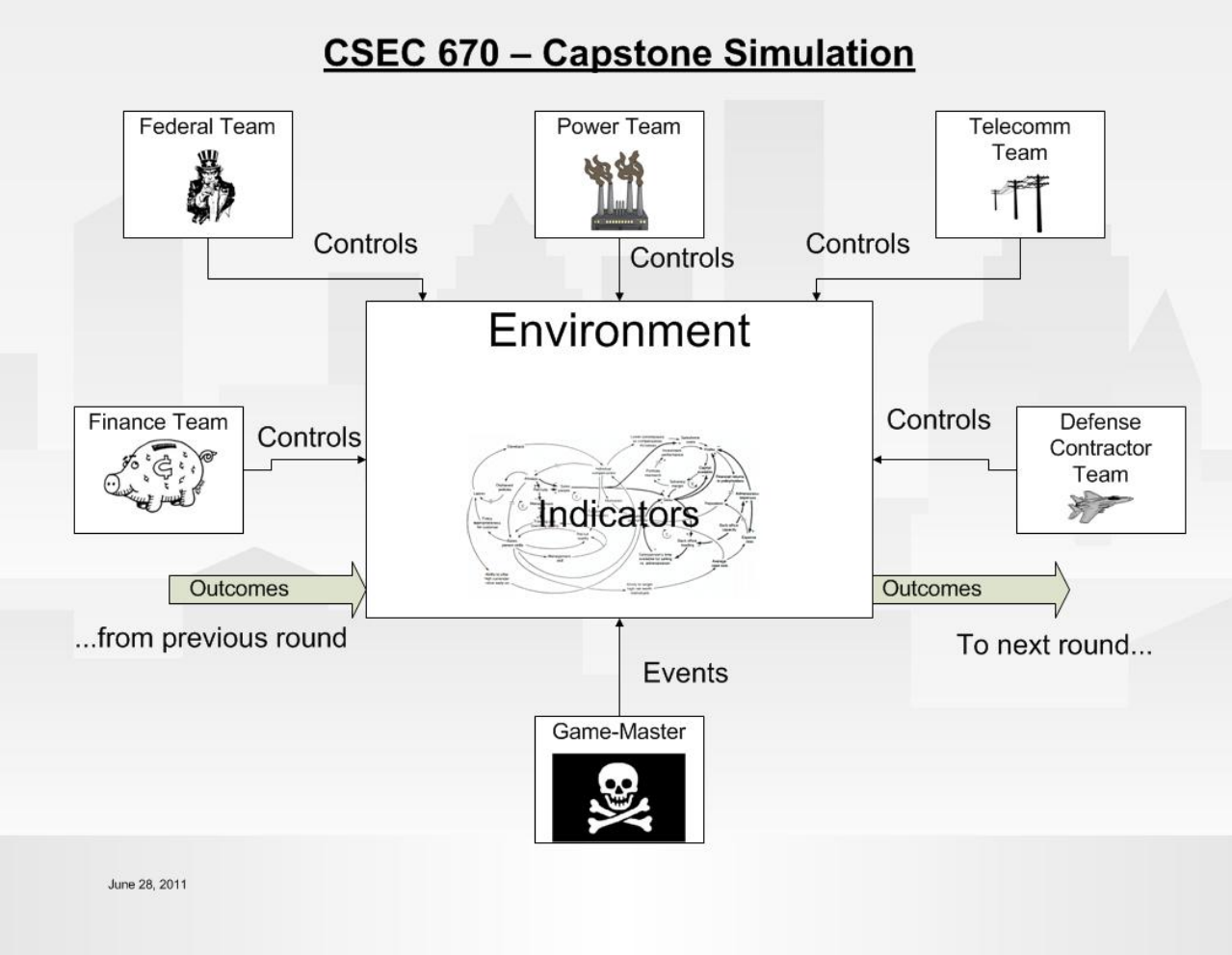


Overview – Simulation Objectives

- Multi-player collaborative online “game”
- Simulation of a national environment
- Technical and Policy Issues
- Synthesis of prior learning
- Bridge to career



Overview – Simulation Organization



UMUC Cybersecurity Capstone Simulation Mission – Protect the US Critical Information Infrastructure against cyberattack

UMUC Capstone Simulation Combines Technical and Policy Skills

- **RedTeam** vs **BlueTeam**
  - Technical insight
- **Tabletop exercises**
  - Policy insight

- Objectives are to protect -
  - system security
  - profitability
  - popular sentiment
  - national security
  - minimize system downtime

- Maintain Business & Infrastructure Budgets

Roles

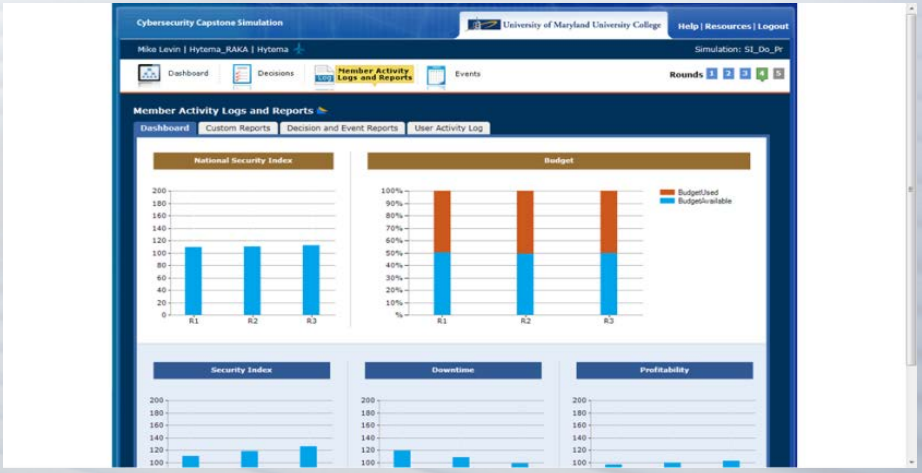
- **Game Master**
- **Instructor**
- **Student Teams**
  - represent Critical Infrastructure businesses
- **Individual Students take on Roles for managing cybersecurity**
  - CIO
  - Net Admin
  - Cyber Sec Officer
  - Cyber Policy Coord
  - Etc.

Operation

- Weekly Cycle
- Game Master
  - introduces Attacks
- Students Teams ➔
  - Receive Alerts About Attacks
  - Select controls to counter
  - Cooperate to stay within budget
  - Adjust cost and strength of controls
  - Finalize selections

Outputs and Evaluation

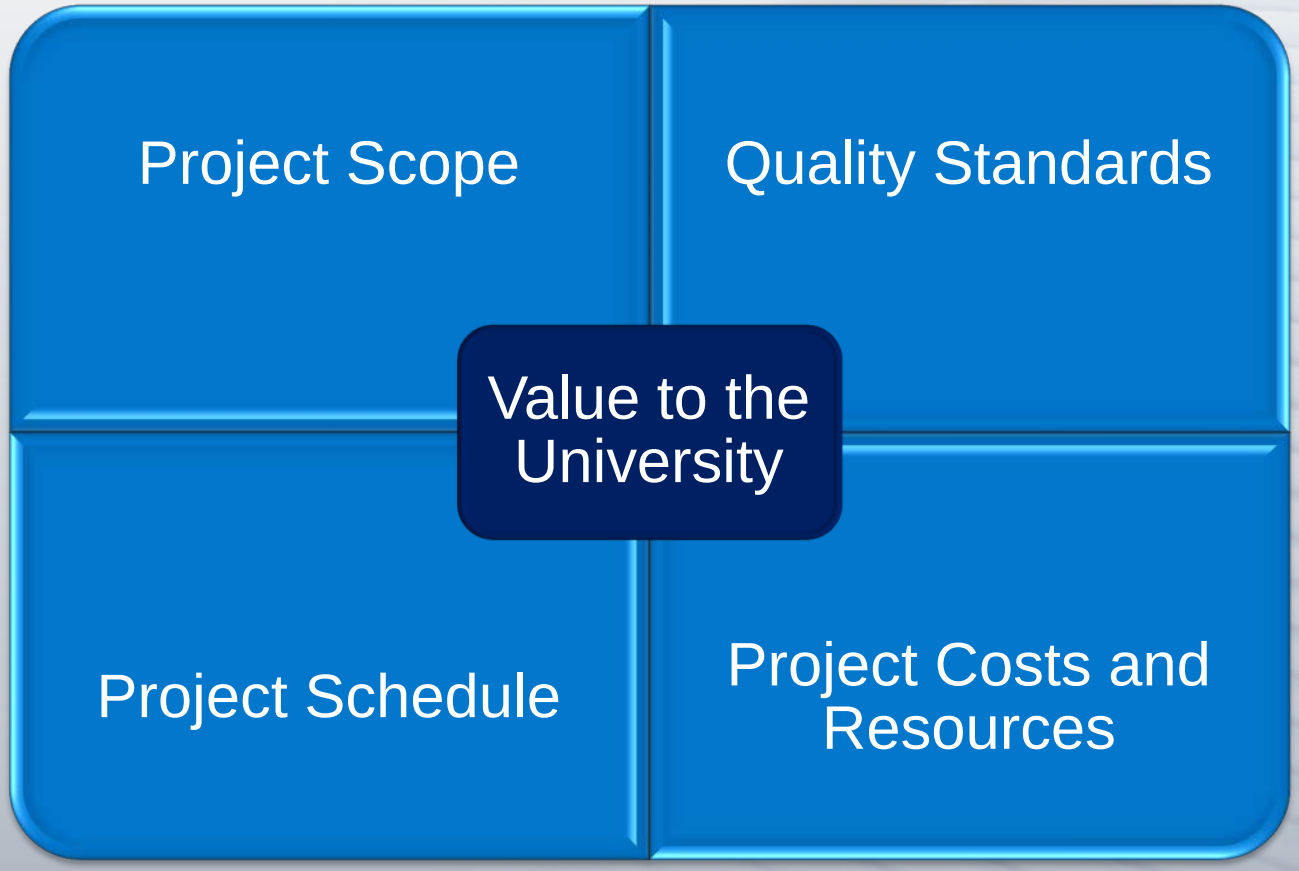
- **Student Teams**
  - choose controls
  - write rationale for control selections
- **Model** runs in background
- **Output Indexes** rise or fall for Security and Business Health
- **Charts** show effects of student choices on Output Indexes
- **Instructor**
  - uses special tools for analysis
  - evaluates indexes and rationale
  - comments on effectiveness of choices made by each team.



Grading Rubric

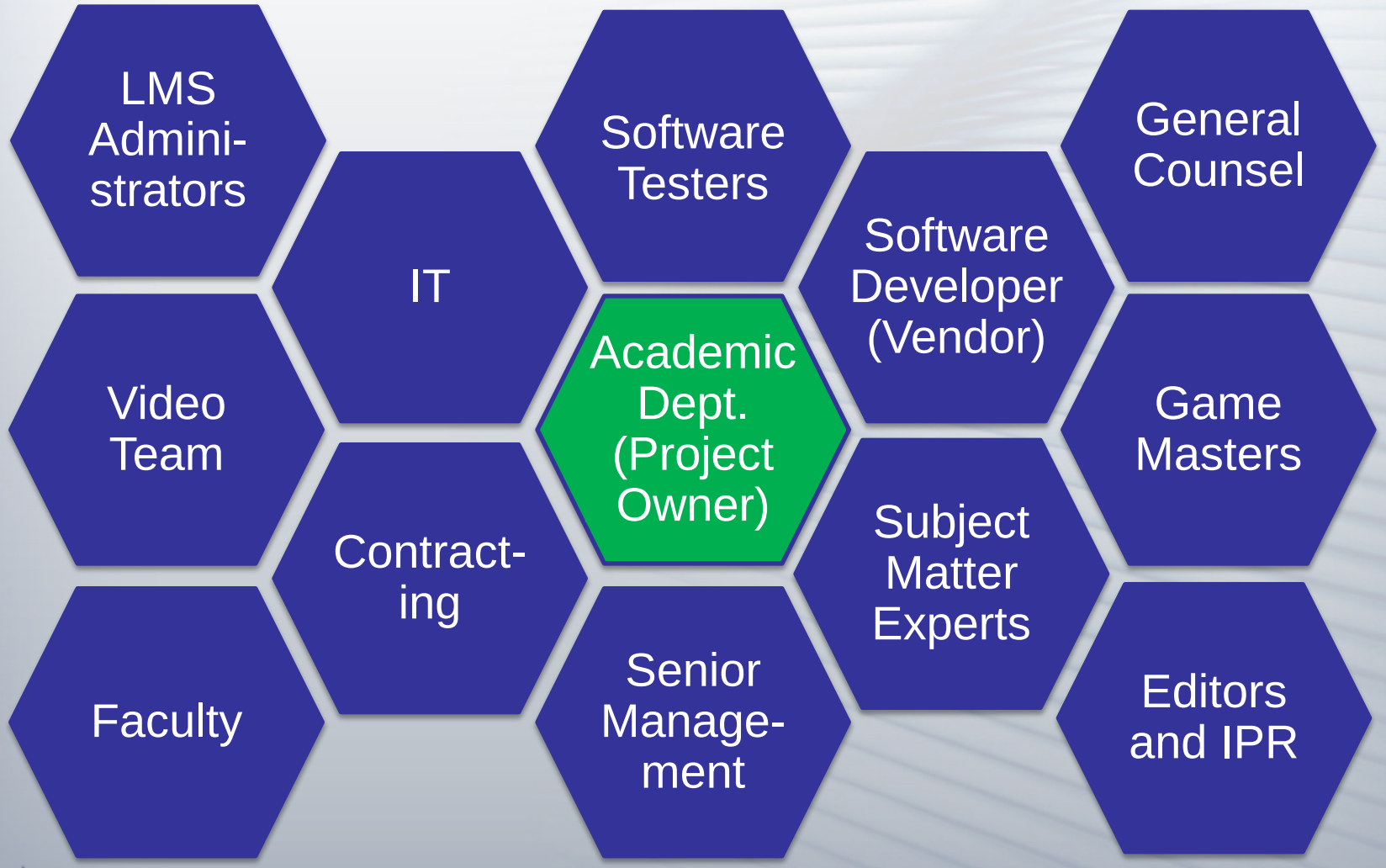
	Excellent	Satisfactory	Needs Improvement	Comments
Changes in key indices from previous round (not applicable for Round 1)				
Consideration of environmental effects such as events and previous rounds' outcomes.				
Demonstration of understanding of controls' effects on security.				
Demonstration of knowledge of the sector's contribution to national security				
Acknowledgement of trade-offs between conflicting objectives.				
Demonstration of team coordination.				
Proper writing, including grammar, punctuation, sentence structure, and typography. Compliance with APA format.				

Managing the Project

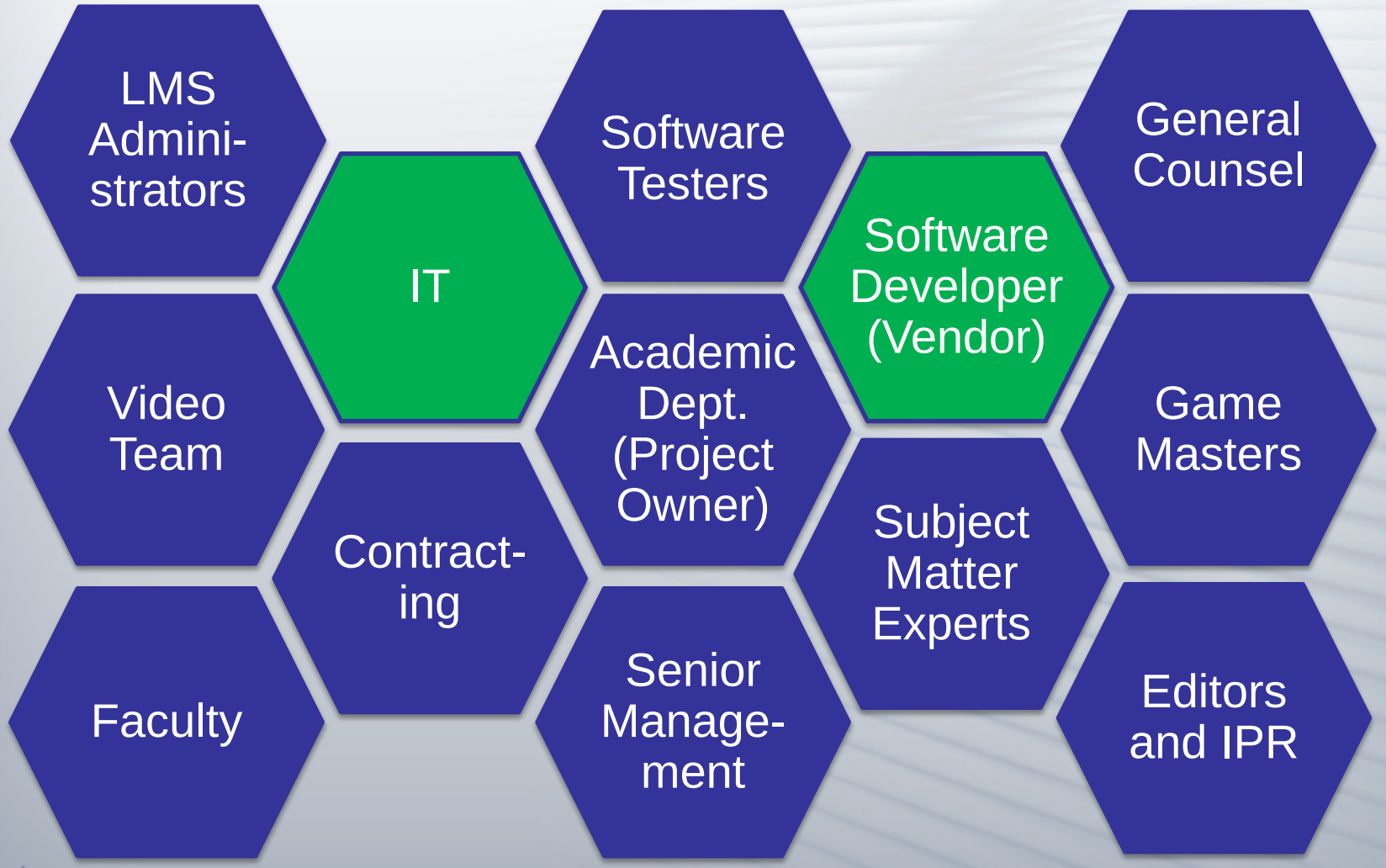


Coordination

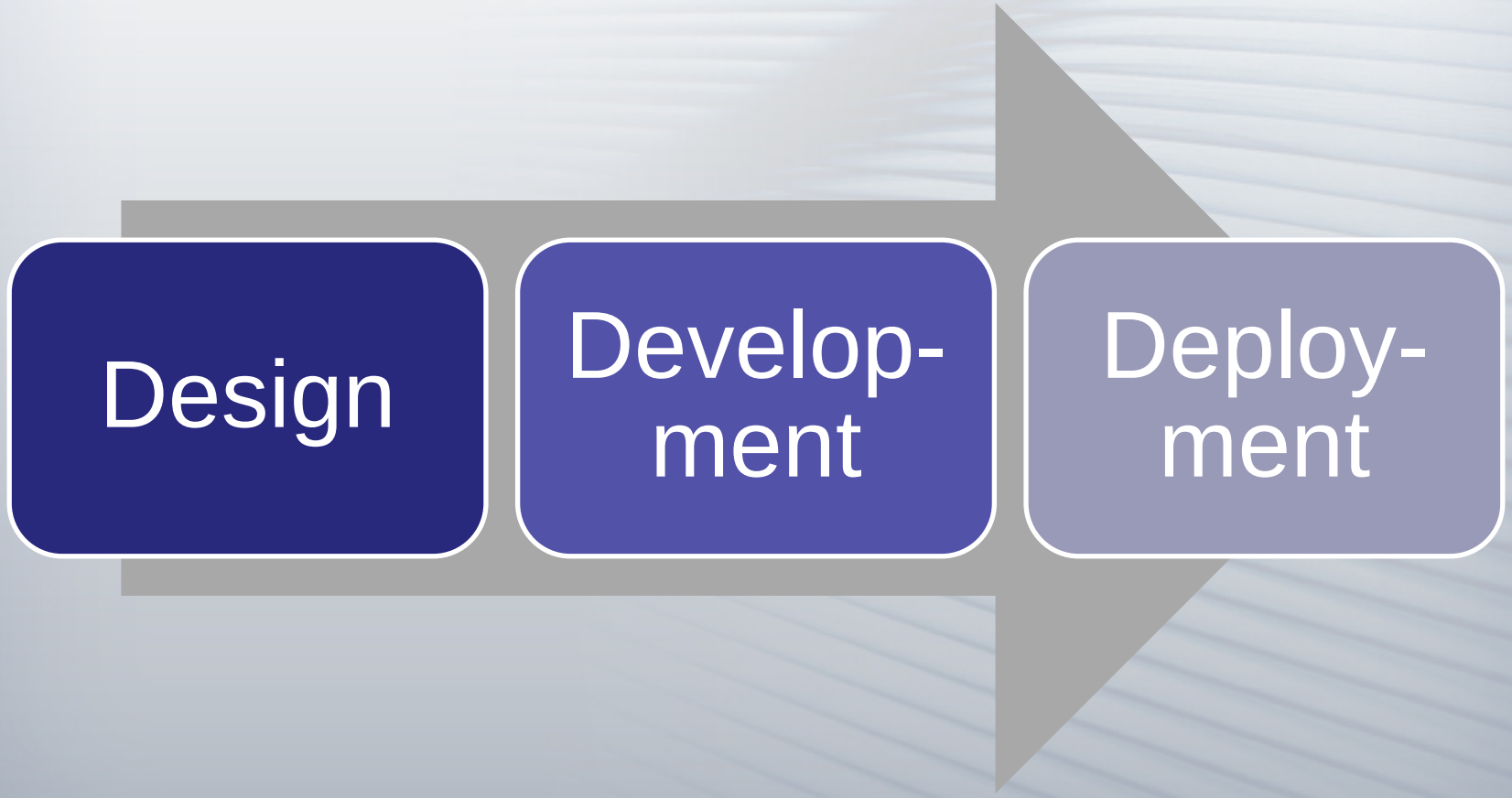
Coordination



Coordination



Project Phases



Design Phase

- SMEs and software designers conceptualize product
- Functional specifications document

Development Phase

- Prototypes and components
- Alpha, Beta, and Gold subphases--delivery and testing of software
- User manuals
- Technical architecture design
- Server hosting
- Load testing

Deployment Phase

- Training of faculty
- Additional documentation for students and faculty
- Facilitating deployment in semester

Results and Plans

- Student reaction – generally positive
  - Using what they learned in their previous courses
  - Simulation visually interesting, easy to use
- But…
  - a steep learning curve
  - Unclear relationship between decisions and outcomes (maybe a virtue?)
- Future plans – cross-team effects

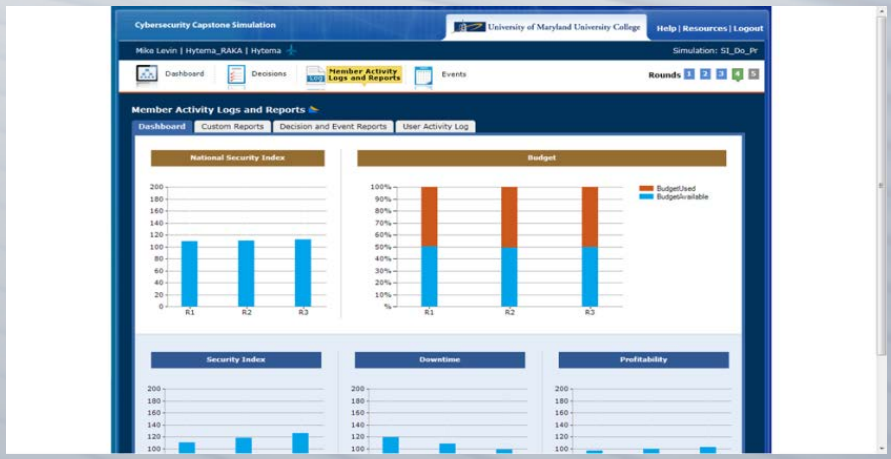
Questions?

Controls

- Decisions on technical and policy measures like:
  - Frequency of software updates
  - RAID levels implemented
  - Level of encryption
  - Investment in training
- Optimization

Events

- Injected by Game Master
- Examples
  - DDoS attack
  - Phishing expedition
  - Economic downturn
  - Natural disaster

Outcomes

- Indicators measuring the performance of each team. Examples:
  - Profitability (Surplus for the Federal Government team)
  - Employee Morale
  - Security Index
  - Budget