# IT Security For Research Data UMBC

jack@umbc.edu

VP of IT, UMBC

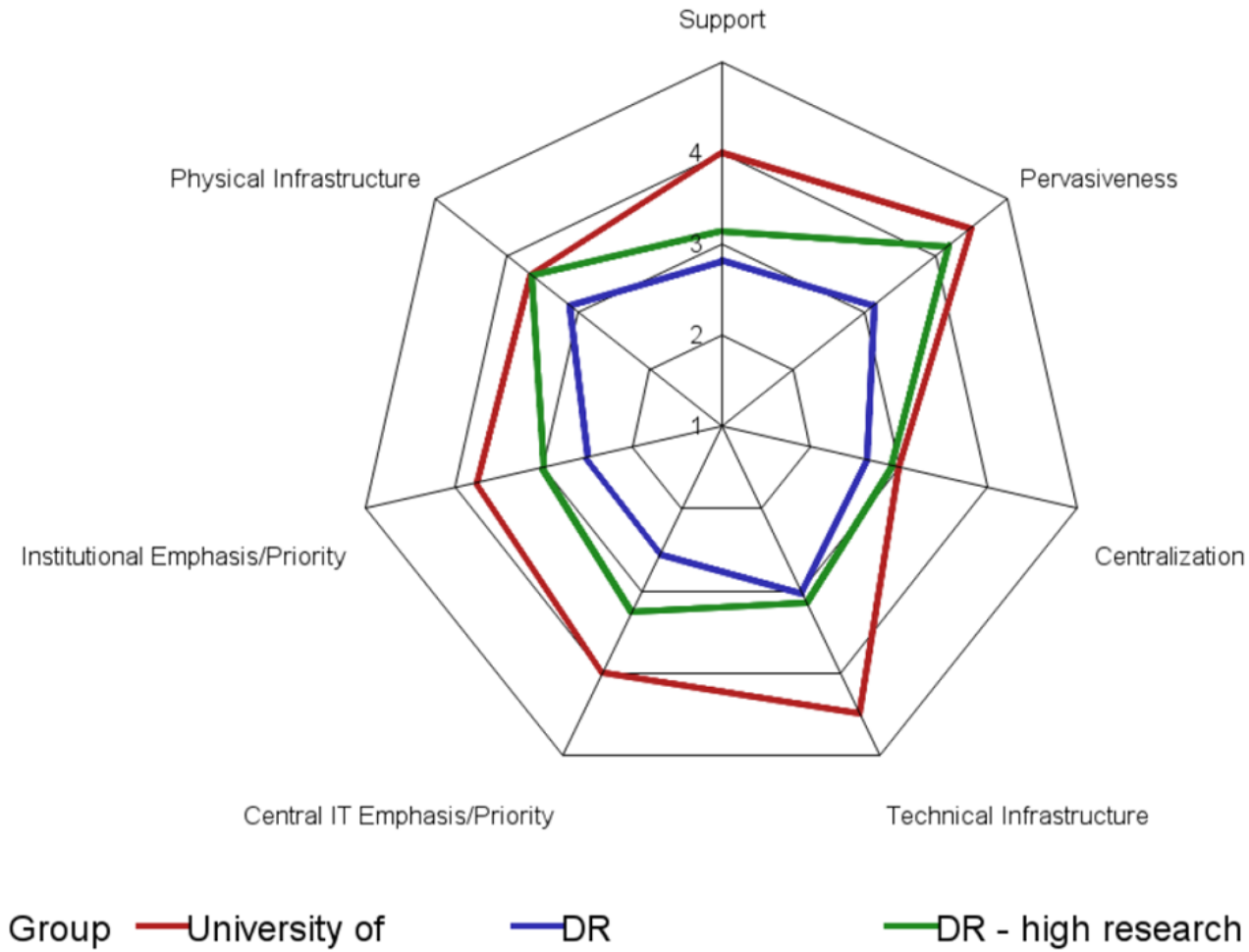
# EDUCAUSE Benchmarking

- Annually, EDUCAUSE collects data from about 750 institutions as part of the core data service.
- Through a grant from the Lumina foundation and EDUCAUSE internal resources, EDUCAUSE is building out a set of benchmarks to look at institutional technology maturity and deployment for some key areas.
- I will show you two that are pertinent to this discussion today.
  - Research Computing Benchmarks (2016 version)
  - Information Security Benchmarks (2017 version)

EDUCAUSE

## 2B. Research Computing Maturity Dimension Scores

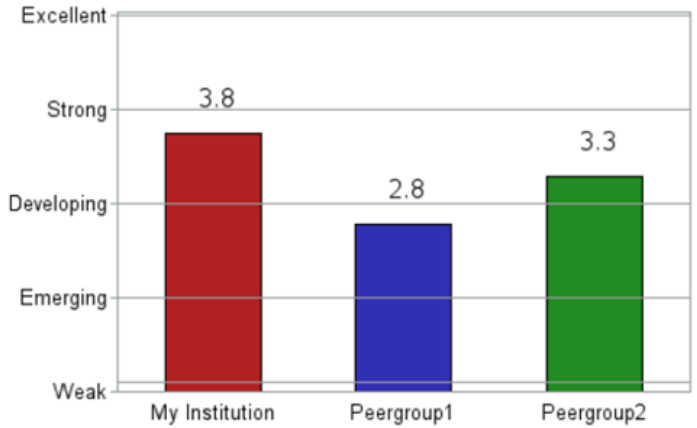
An research computing maturity index dimension score represents the mean response for all items within that dimension. The dimension scores allow you to examine your institution's maturity within a specific area of research computing. The graphic below depicts how University of Maryland Baltimore County's dimension scores compare to dimension scores for peer institutions.



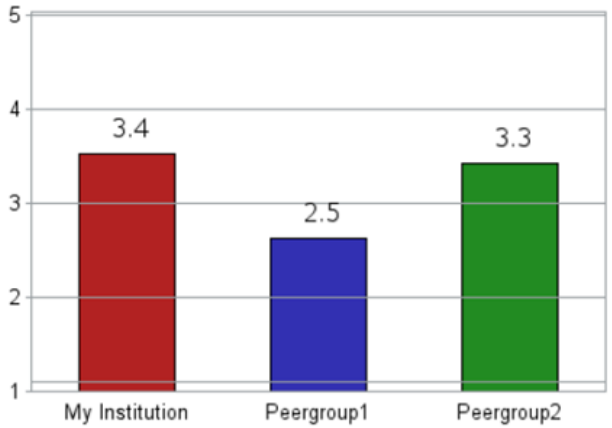
EDUCAUSE

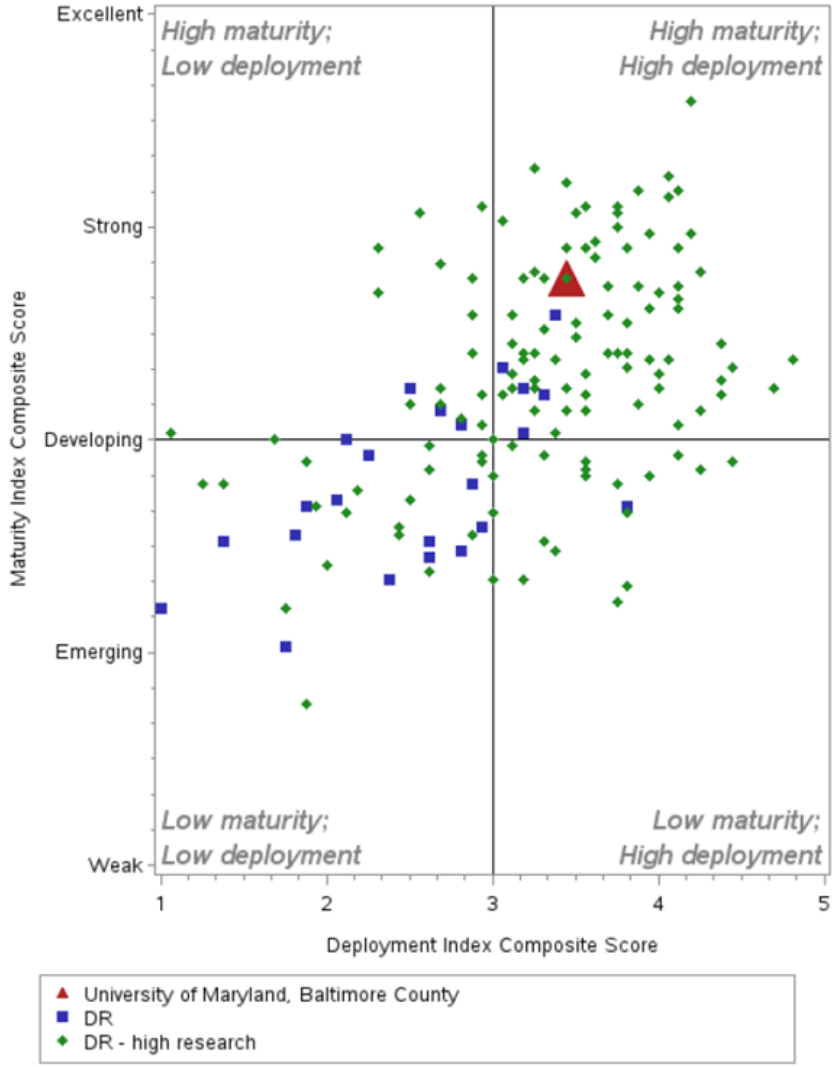
# 1. Maturity and Deployment Index Results Overview

## Maturity Index Composite Score




## Deployment Index Composite Score



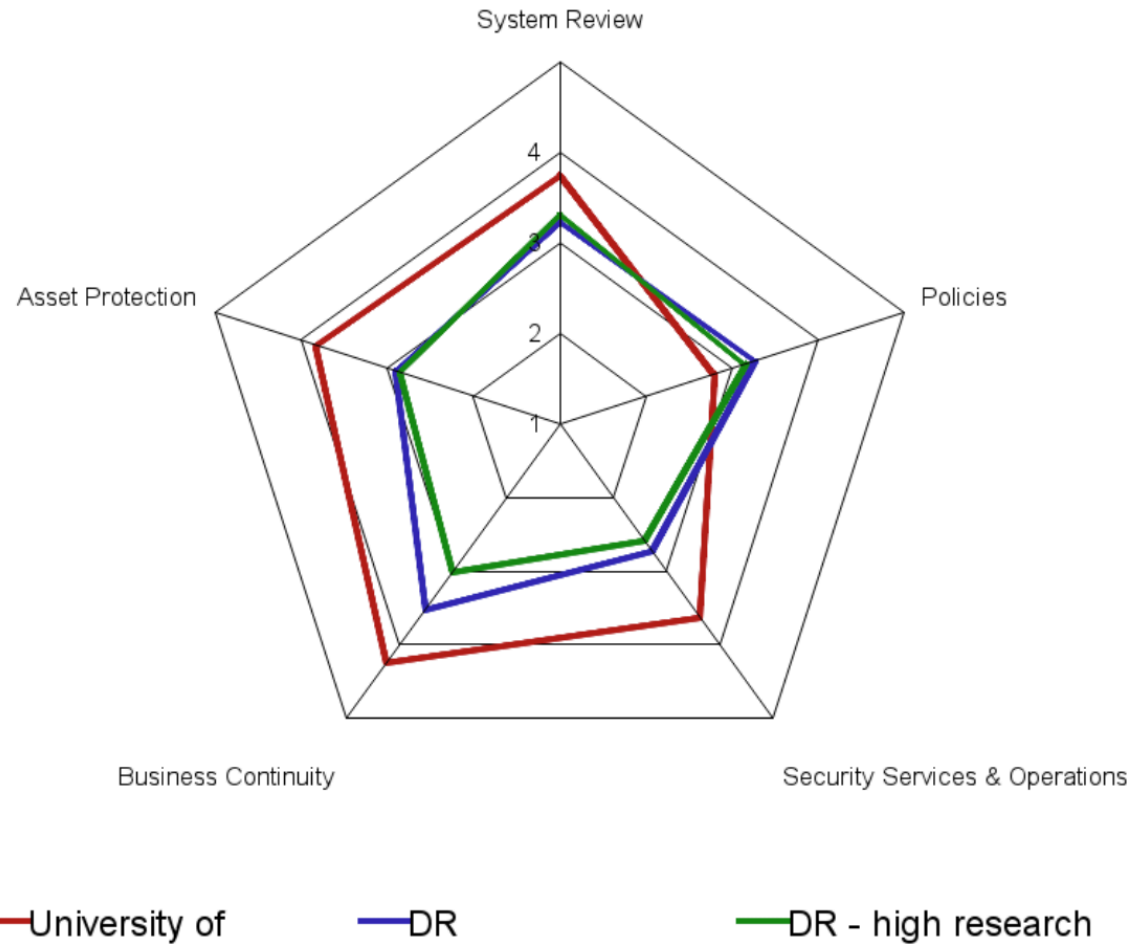
# Research Computing Results

- DR High and Very High have higher maturity and deployment scores that DR when it comes to research computing.
- Pervasiveness and physical infrastructure score the highest, centralization and institutional priority score slightly lower.

EDUCAUSE

## 2B. Information Security Maturity Dimension Scores

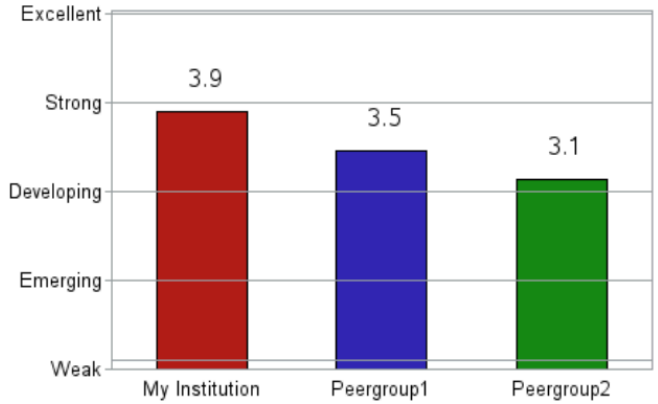
An information security maturity index dimension score represents the mean response for all items within that dimension. The dimension scores allow you to examine your institution's maturity within a specific area of information security. The graphic below depicts how University of Maryland Baltimore County's dimension scores compare to dimension scores for peer institutions.



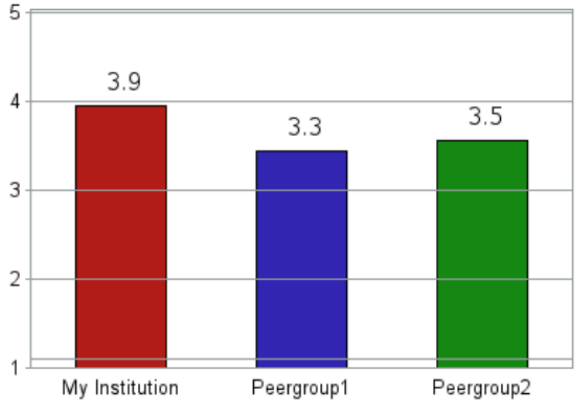
EDUCAUSE

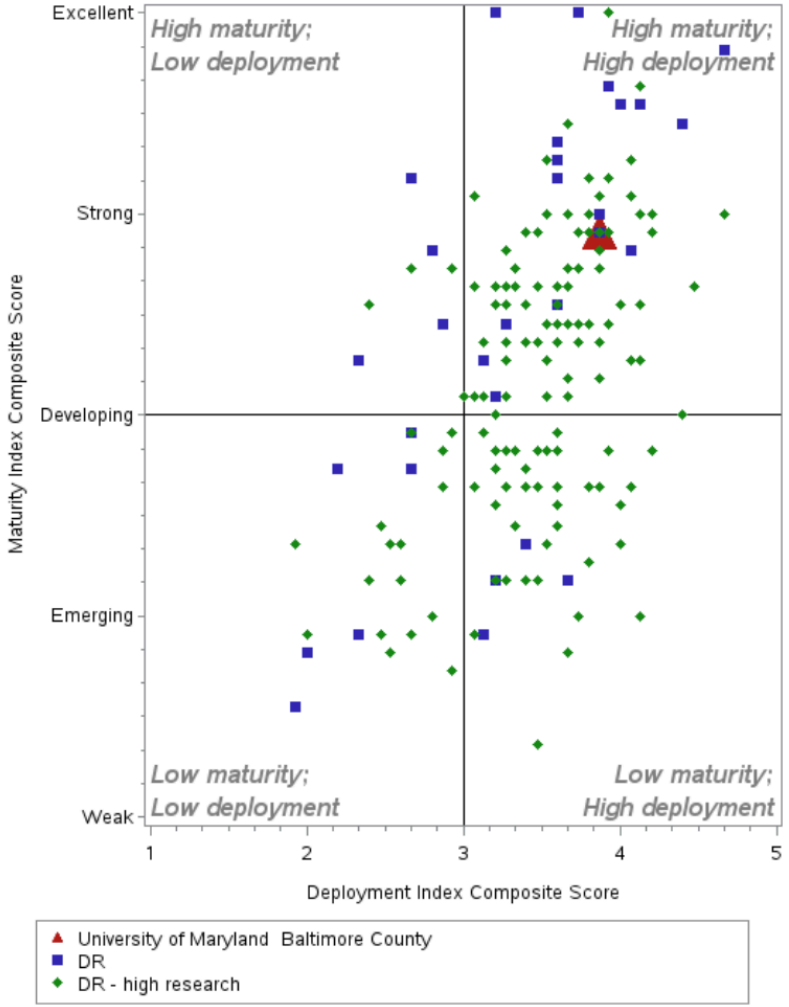
# 1. Maturity and Deployment Index Results Overview

## Maturity Index Composite Score




## Deployment Index Composite Score



# Information Security Results

- Larger universities, DR-High and above have lower maturity of processes and procedures.
  - All five dimensions have similar scores, but security services and operations is generally the lowest of the five.
- Collectively, institutions are doing better in deployment of technologies than in process and procedure development.
- My personal opinion, most higher education institutions will need a few years to move to NIST 171 moderate. If Financial aid data is categorized as FISMA moderate, that will require all institutions to move towards this over time.

# UMBC Plan for Research Data

“Data can be as toxic as chemicals to the institution and we need processes for identifying “toxic data” similar to what we use for identifying toxic chemicals” -- Dr. Karl Steiner, UMBC VP of Research.

- OSP established a Research Data Management Council (RDMC)
- DoIT Chief Information Security Officer participates on the RDMC
- DoIT CISO meets regularly with the OSP team to review data use agreements.

# DoIT Efforts to Support Research Data

- **Unprotected Data**
- High Performance Cluster/ Science DMZ for data-intensive research
- Creating research data environment for NIH genomic data.
- Exploring cloud vendors for supporting data science.
- Documenting procedures for security.

- **Protected Data**
- DoIT is responsible for HIPPA data in research.
- Consult with faculty on data use agreements
- Exploring how we can best stand up environments supporting FISMA – looking at U. Florida and other models.
- Add BAA to Microsoft, Box and AWS Internet2 NET+ agreements.

# What We Still Need to Do

- Educating PI's on the cost of securing their data – these regulations will drive up costs and make it harder for faculty to operate systems. Also, teaching faculty to help us push back when data is being protected beyond its inherent risk.
- Working with VPR to get base funding in place to treat "protected data computation" as CORE research facility on campus.
- Mapping our current University System of Maryland security requirements against NIST 171 to know exactly what we need to do.
- Continued and ongoing training of our central infrastructure teams. We view security as we do business continuity, FISMA moderate should ultimately be our default for institution data at risk.