CERIAS

The Center for Education and Research in Information Assurance and Security

Modeling Impact Relationships for Software-as-a-Service Public Cloud Systems

Students: Lloyd Jones, Sarah Isaacs

Advisors: Dr. Melissa Dark, Filipo Sharevski, Courtney Falk

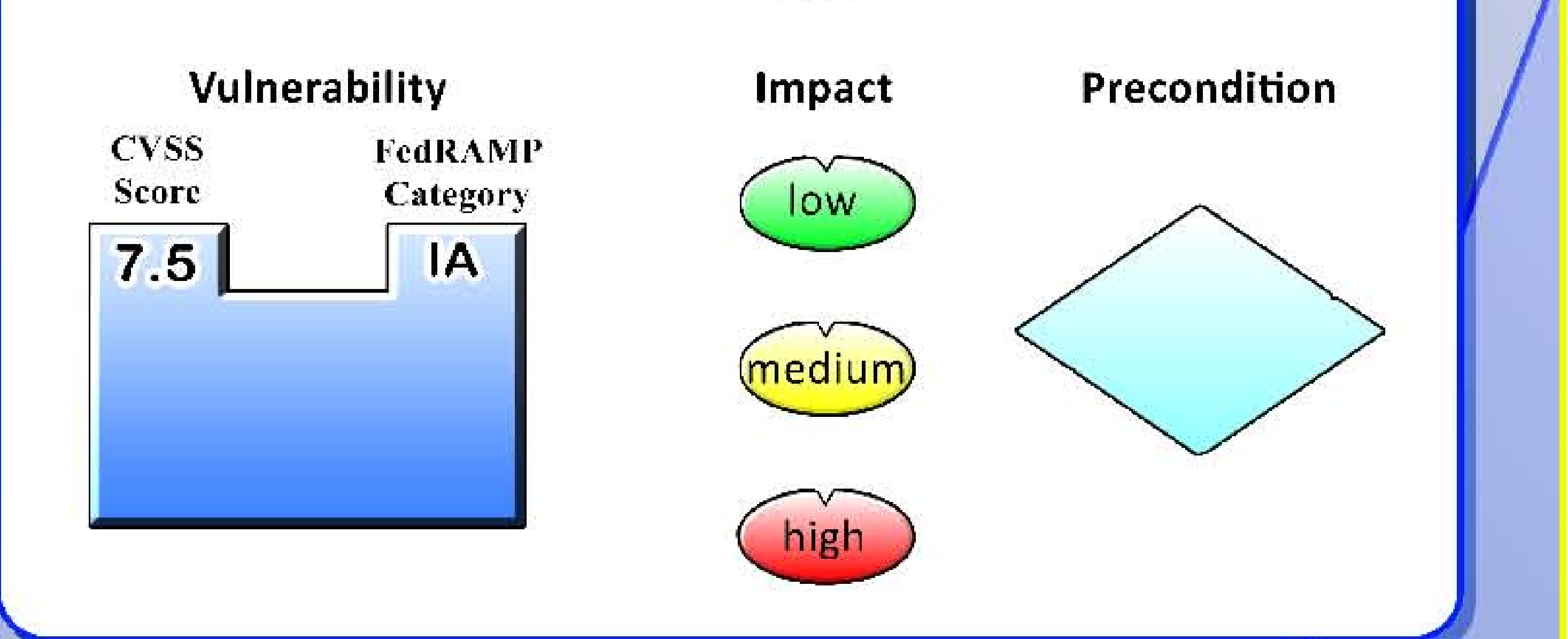
Problem Statement

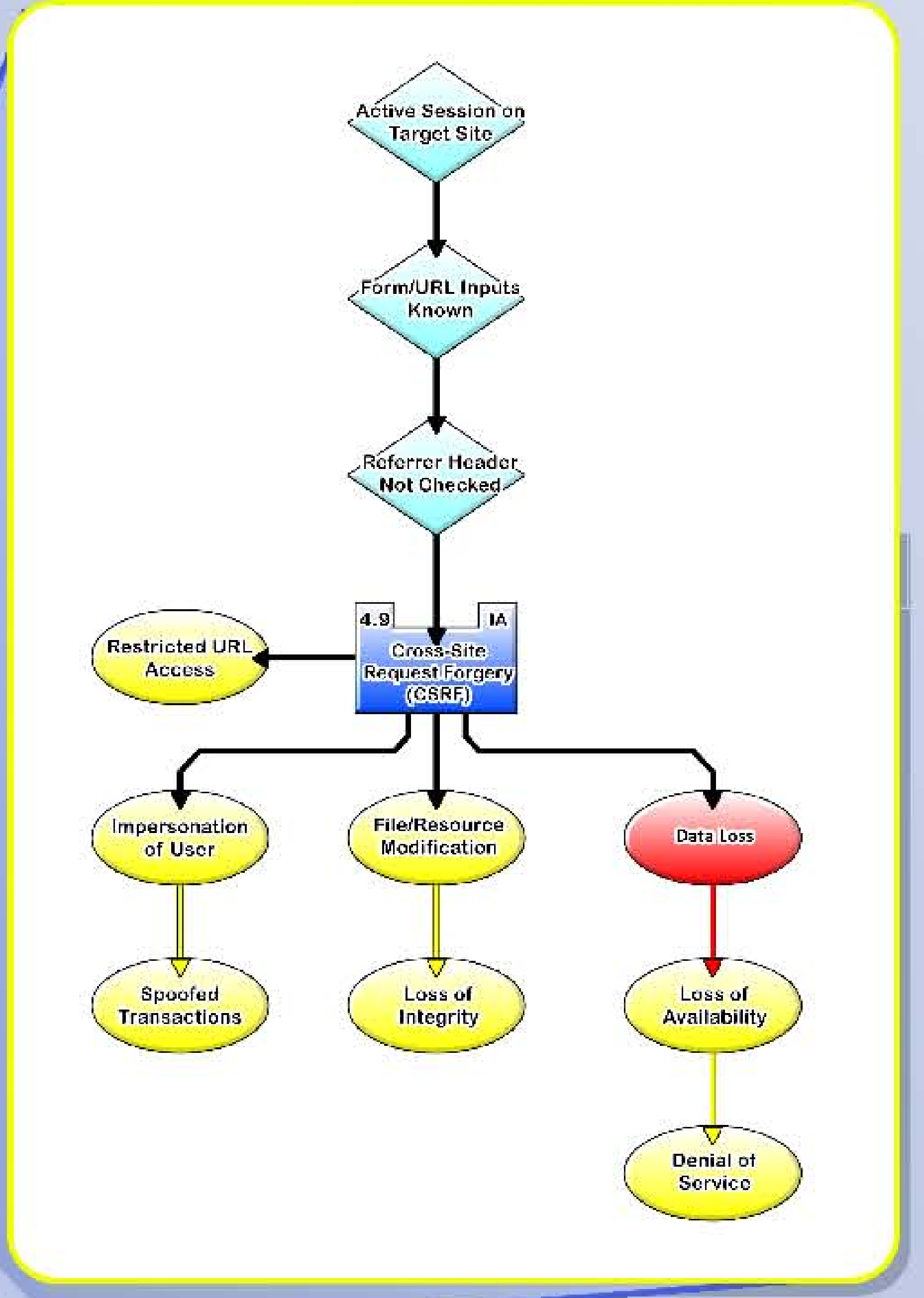
This project creates a visual model of the relationships among known vulnerabilities, impacts, and controls using FedRAMP's Identification and Authentication category as the prescribed control set.

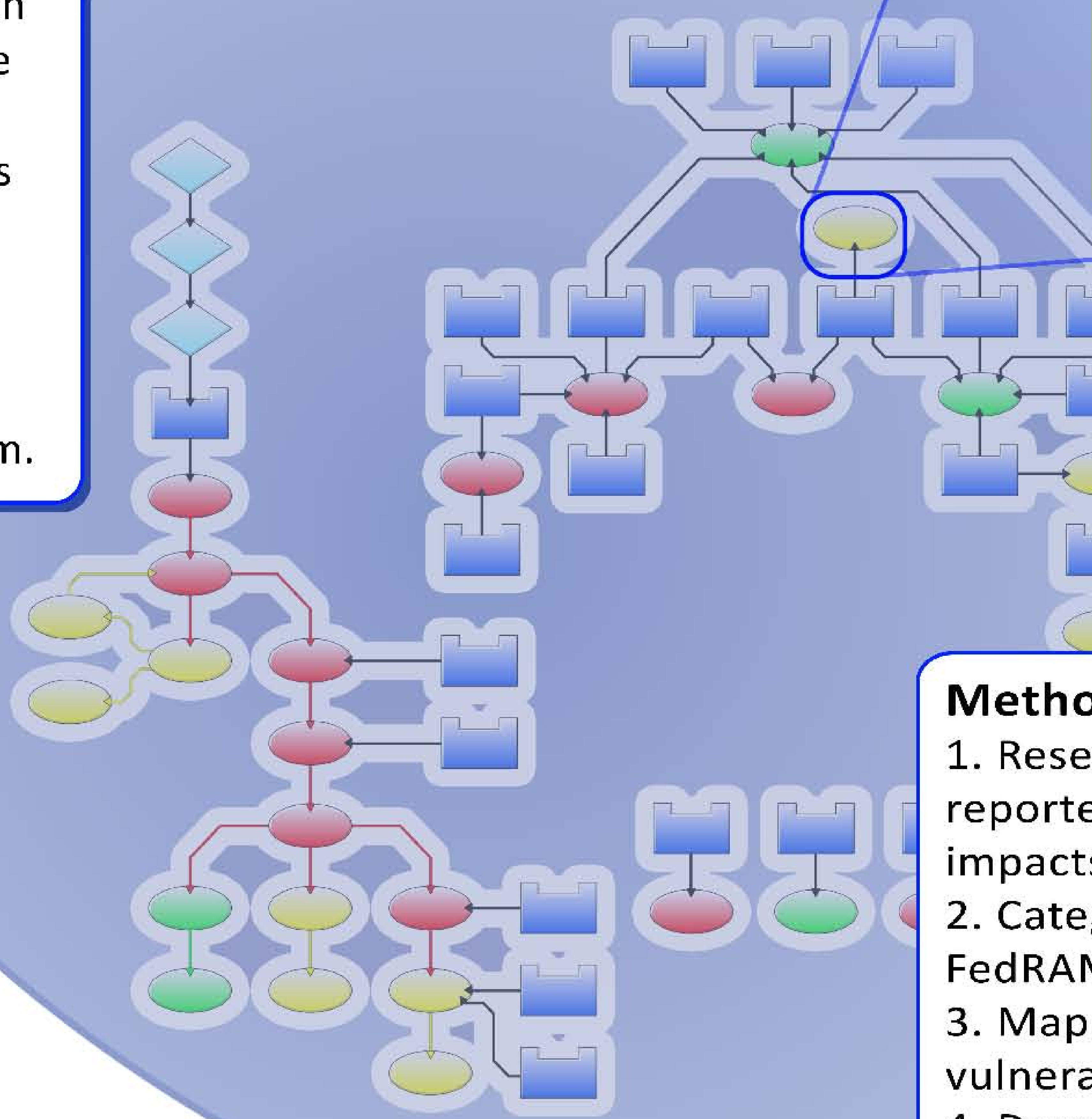
Significance

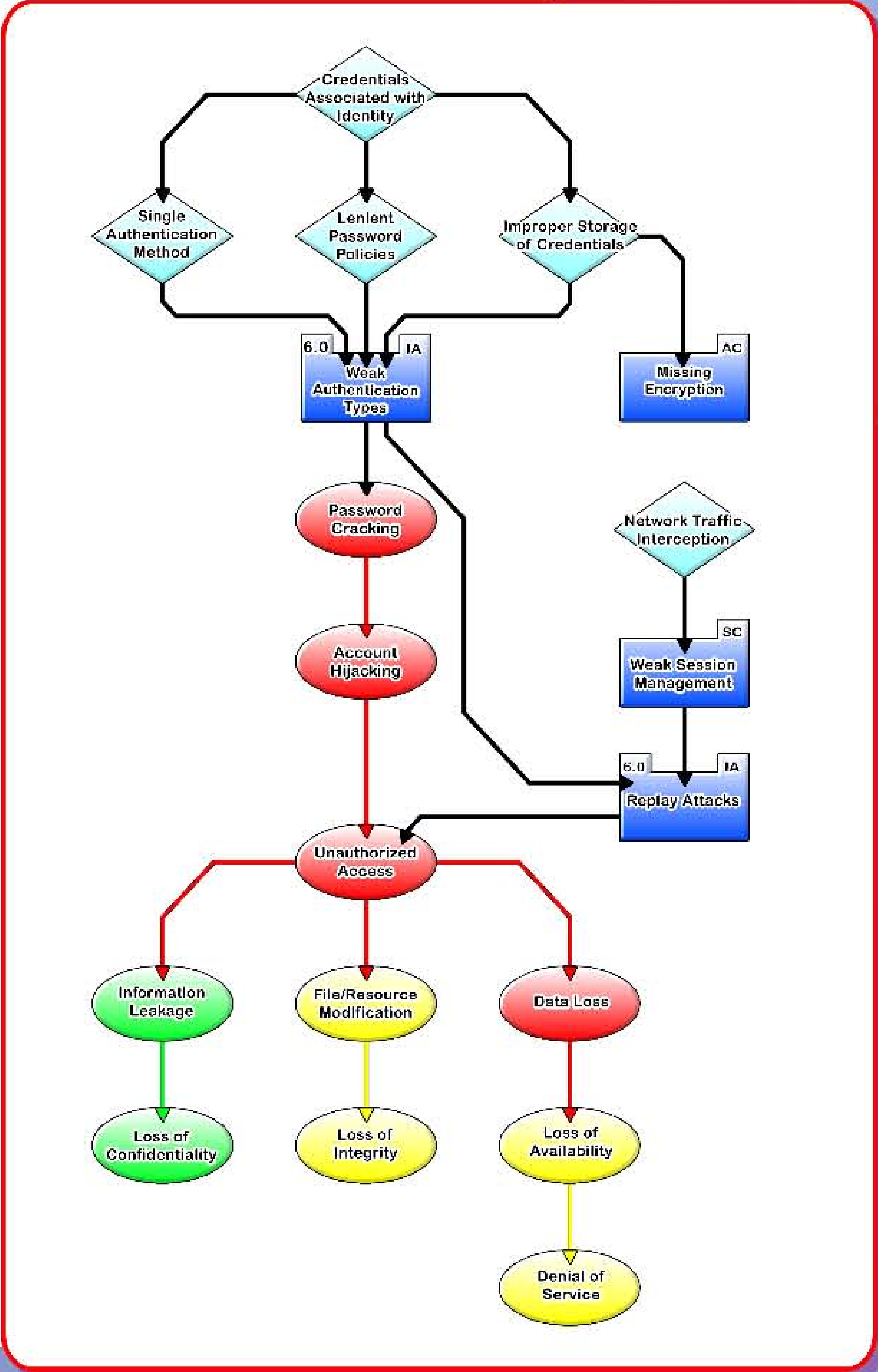
By visualizing these relationships, the overall severity of a vulnerability can be easily assessed and the audience can make otherwise unknown connections between vulnerabilities and impacts. This type of analysis also allows for customization based on newly reported attacks, the sensitivity of stored data, and the specific use case of the cloud system.

Shape Legend









Methods

1. Research known and publicly reported SaaS vulnerabilities and impacts
2. Categorize vulnerabilities using FedRAMP guidelines
3. Map and assign scores to vulnerabilities and impacts
4. Develop algorithm to calculate total impact score

Future Work

- Extend vulnerability relationship map and score every known vulnerability
- Develop interactive web application that allows for customization of all variables
- Present findings to FedRAMP for review and possible implementation

Algorithm and Findings

Total Impact Score = (Sum of all normalized OWASP Impact Scores * Vulnerability CVSS Score) + Child Vulnerability Total Impact Score(s)

Rank	Vulnerability	FedRAMP Category	Total Impact Score
1	Cross-Site Scripting	System and Information Integrity (SI)	69.75
2	Weak Authentication Types	Identification and Authentication (IA)	53.33
3	Cookie Manipulation	System and Communications Protection (SC)	36.38
4	Unauthenticated Use of a System	Identification and Authentication (IA)	29.63
5	Weak Session Management	System and Communications Protection (SC)	27.90
6	Replay Attacks	Identification and Authentication (IA)	23.70
7	Insecure Configurations	Configuration Management (CM)	22.50
8	Inactive User Accounts	Access Control (AC)	22.08
9	Cross-site Request Forgery	Identification and Authentication (IA)	19.85
10	Hardware Failure	Contingency Planning (CP)	13.86
11	Unknown Data Ownership	Media Protection (MP)	6.75
12	Insecure Multi-tenancy	System and Communications Protection (SC)	1.82

OWASP Risk Rating Methodology. (2014). Retrieved July 3rd, 2014, from https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Mell, P. A., & Romanosky, S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0. (2014). Retrieved July 2nd, 2014, from http://www.first.org/cvss/cvss-guide.html

FedRAMP Rev 4. Baseline Workbook. (2014). Retrieved June 7th, 2014, from http://cloud.cio.gov/document/fedramp-security-controls

This material is based upon work supported by the National Science Foundation under grant #1062970. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

INSuRE is training students in information security research. Sponsored by the National Science Foundation with problems provided by the National Security Agency.

PURDUE UNIVERSITY