netSPI
RISK COMPLIANCE SECURITY

App Security? There is a metric for that!

by Yan Kravchenko

About Me

Yan Kravchenko, QSA, CISSP, CISA, CISM, PCIP
Compliance Advisory Practice Lead

yan.kravchenko@netspi.com
612-455-8485

Twitter: @yanfosec
Contributor: https://www.netspi.com/blog/

netSPI
RISK COMPLIANCE SECURITY

Agenda

- Background – Why is this necessary?
- Defining Risk:
  - Value / Potential Impact
  - Maturity / Susceptibility
- Why Open SAMM?
- Dashboards – Decision Support Systems
- Demo

netSPI
RISK COMPLIANCE SECURITY

Risk Measurement Challenges

- Applications can be developed with different SDLC methodologies
- Inconsistent maturity of the design and embedded security mechanisms
- Applications range in size, complexity, and perception of risk
- Application security / maturity is difficult to normalize, contrast, and compare

netSPI

RISK COMPLIANCE SECURITY

Defining Application Risks

Defining Risk

- Significance / Impact
  - What an application is
  - Does not change without significant changes to the nature of the application
- Maturity / Susceptibility
  - Maturity of the application
  - Can be changed by implementing additional security controls
  - Based on OWASP Software Assurance Maturity Model (SAMM)

Static Risk

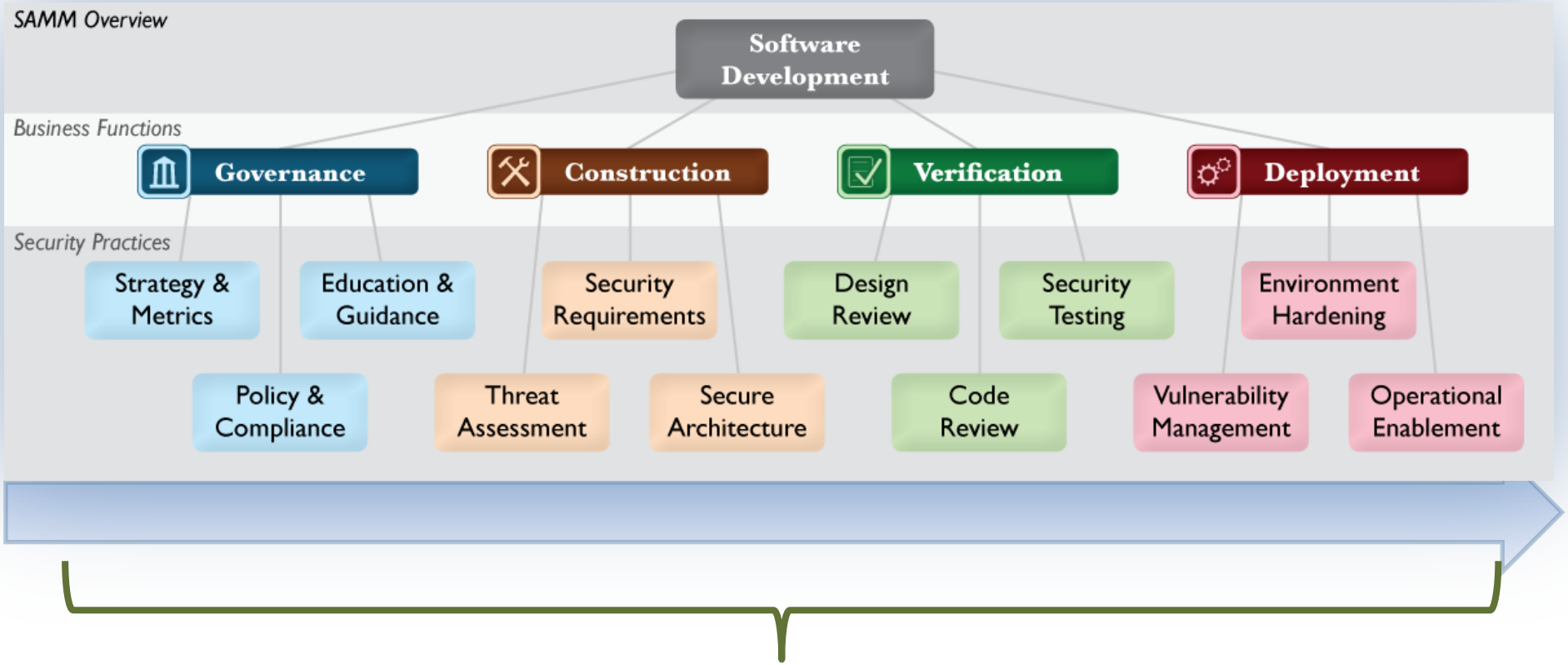
- Customized for each organization
- Should not change unless the application or the organization undergoes big changes
- Focuses on application risk categories and attributes that are significant and meaningful
- Static risks can be used for risk calculation or presenting correlated risk scores as they relate to each static risk
- Static risks can be used to pivot data, highlighting internal initiatives

Dynamic Risk

- Based on OWASP Software Assurance Maturity Model (SAMM)
- Uses SAMM's questionnaire for determining the maturity model
- Answers to questions help calculate numeric dynamic risk score as well as determine control maturity levels
- In addition to establishing the maturity level, SAMM provides detailed control implementation requirements

Why they Open SAMM?

SAMM



Secure Development Lifecycle (SAMM)

Sample Dashboards – SAMM Scores

	Application 1	Application 2	Application 3	Application 4	Application 5	Application 6
Governance: Strategy & Metrics	0+	2+	0+	0+	0+	0+
Governance: Policy & Compliance	0+	1+	0+	0+	0+	0+
Governance: Education & Guidance	0+	2	2+	2+	2+	2+
Construction: Threat Assessment	0+	1+	1+	0+	1+	1+
Construction: Security Requirements	0	2+	0+	0+	1+	0+
Construction: Security Architecture	1+	2	1+	1+	1+	1+
Verification: Design Review	1+	0+	1+	0+	1	0+
Verification: Code Review	1	2	3	1+	0+	3
Verification: Security Testing	1+	1+	1+	0+	1+	0+
Deployment: Vulnerability Management	1+	2+	1+	1+	1+	1+
Deployment: Environment Hardening	0	2	0+	0	0	0+
Deployment: Operational Enablement	0	2	0+	0+	0+	0+

Correlated Risk Analysis / Dashboards

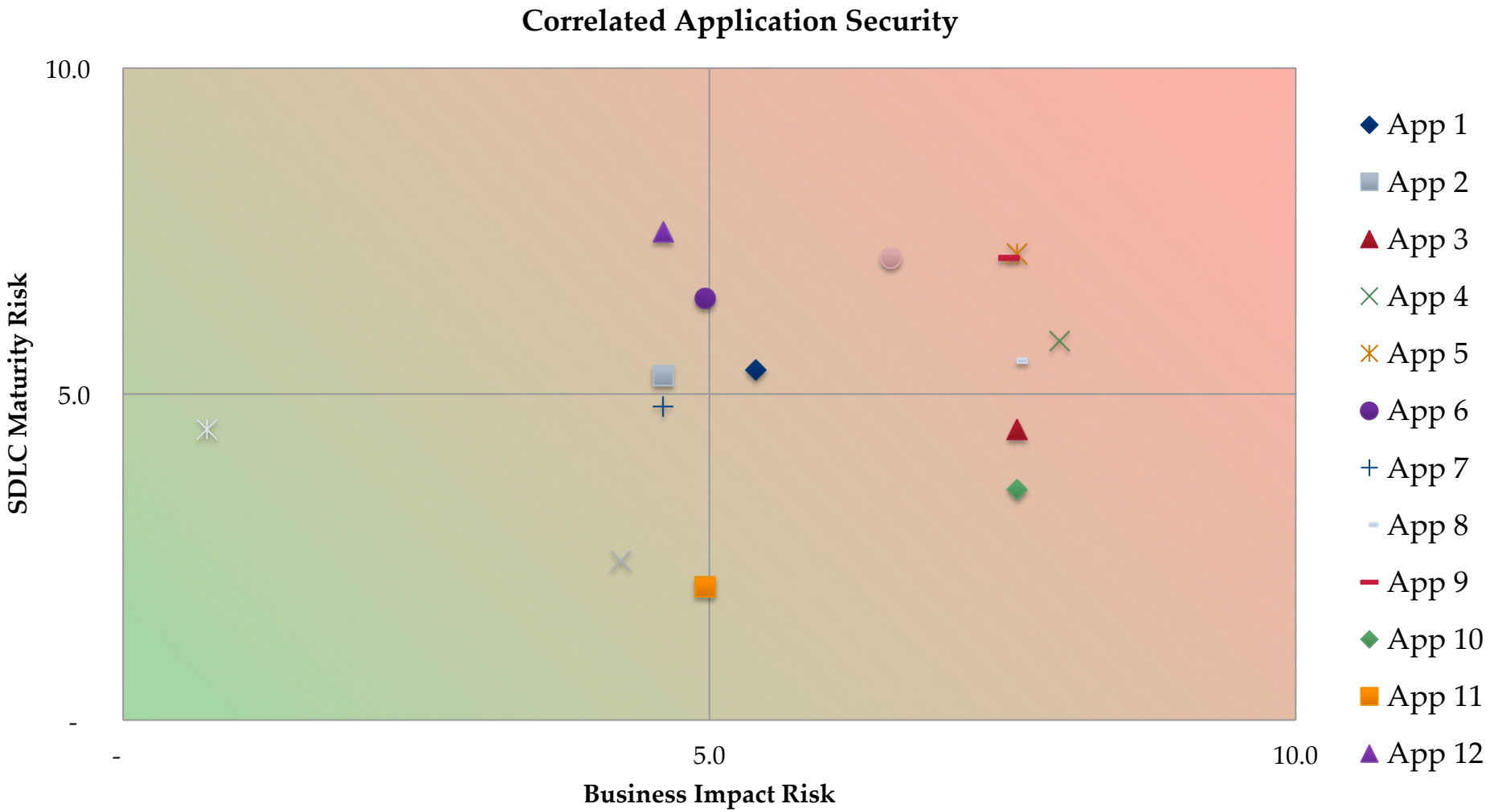
Risk Correlation

Value * Maturity = Correlated Risk

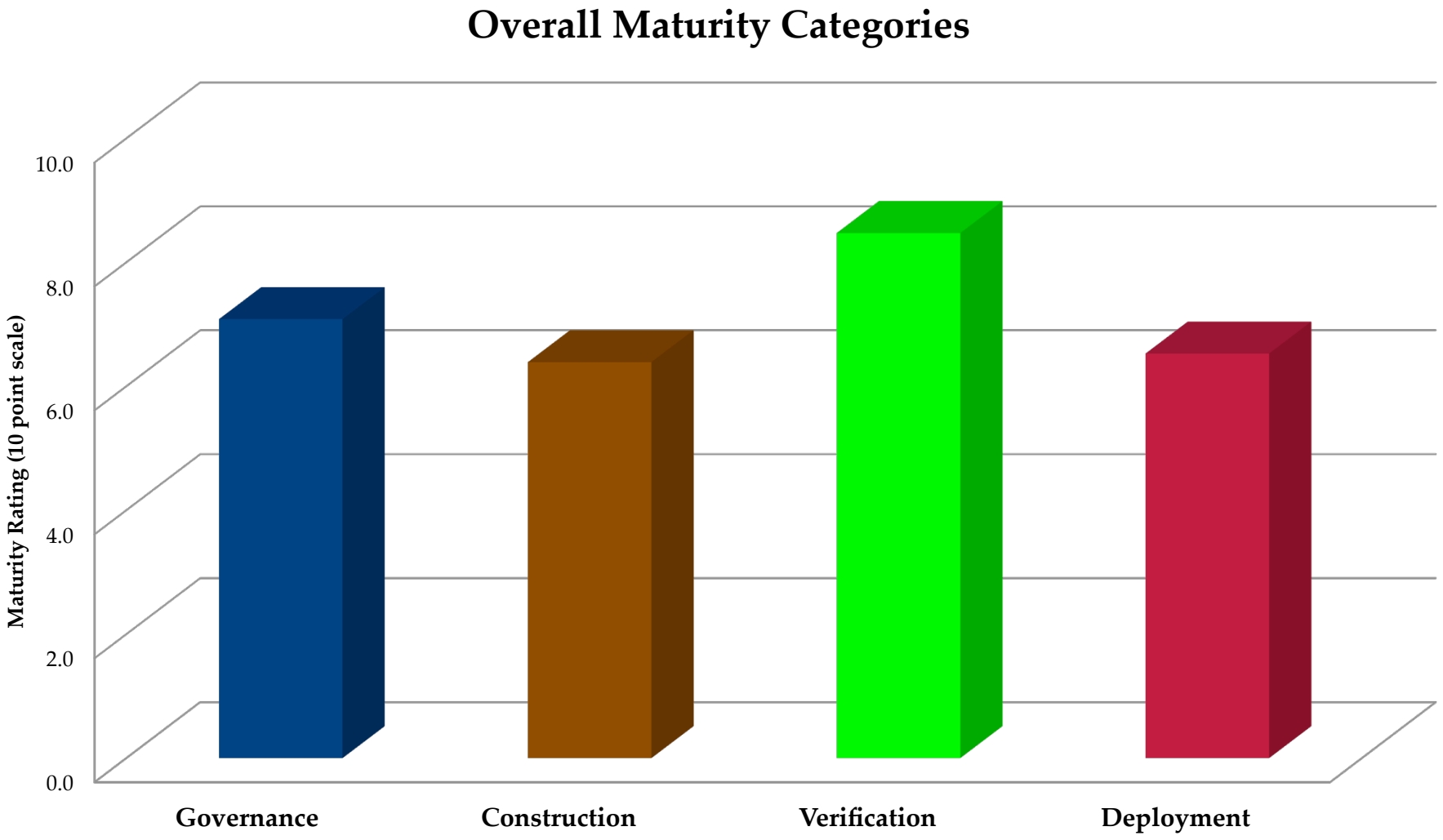
- Value / Impact factors generate a numeric score, normalized against all applications
- SAMM activities generates a numeric score, based on answers provided as part of the SAMM assessment
- Provides a single measure of security for each application
- Can be applied uniformly across all applications
- Provides a “true” value, allowing a side-by-side comparison of all applications

netSPI
RISK COMPLIANCE SECURITY

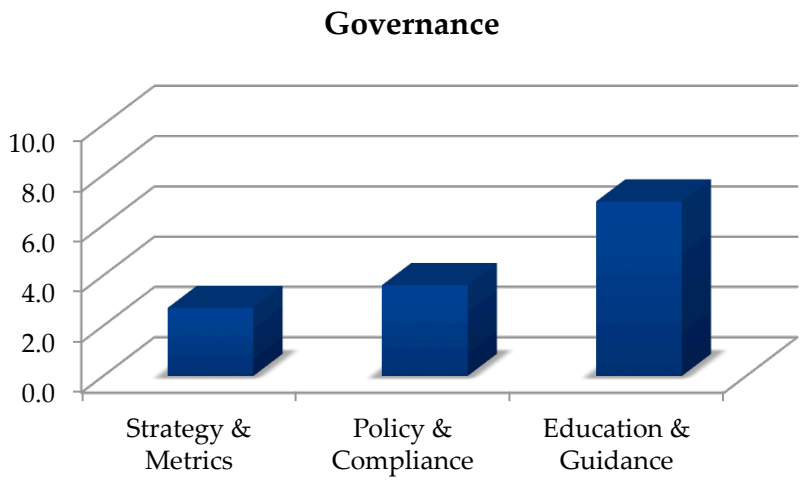
Sample Dashboards

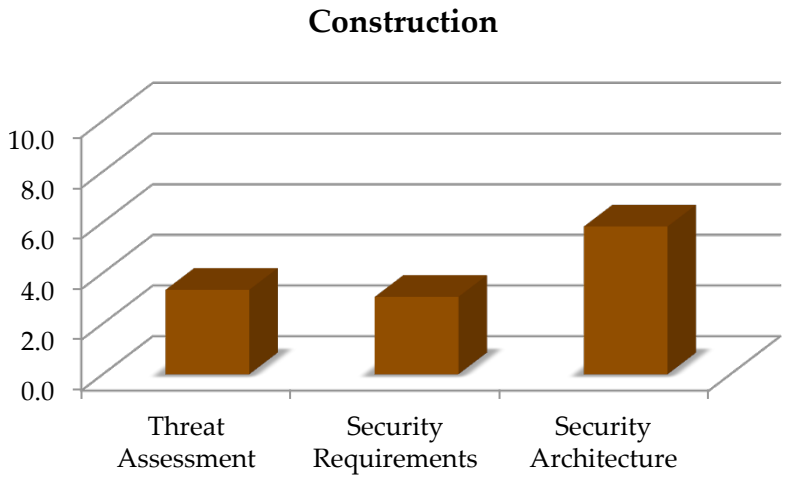


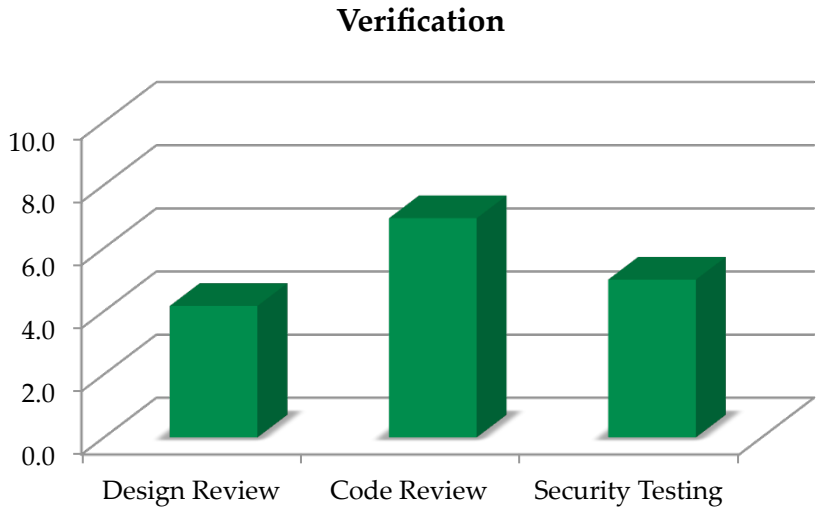
Sample Dashboards

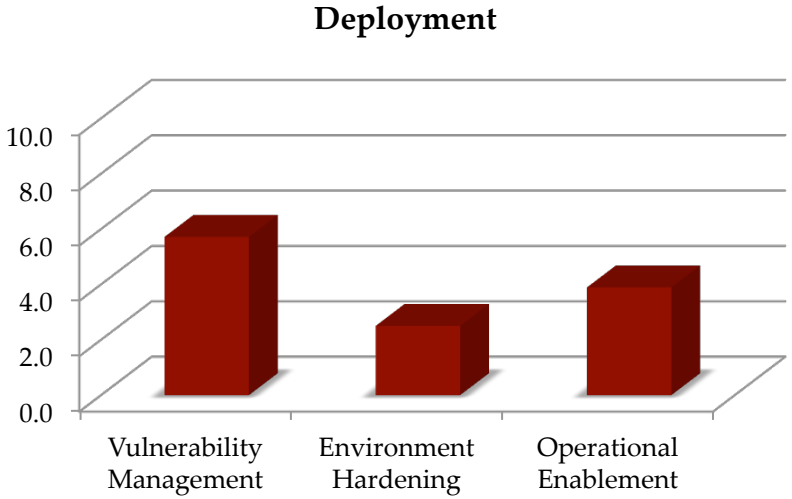


Sample Dashboards

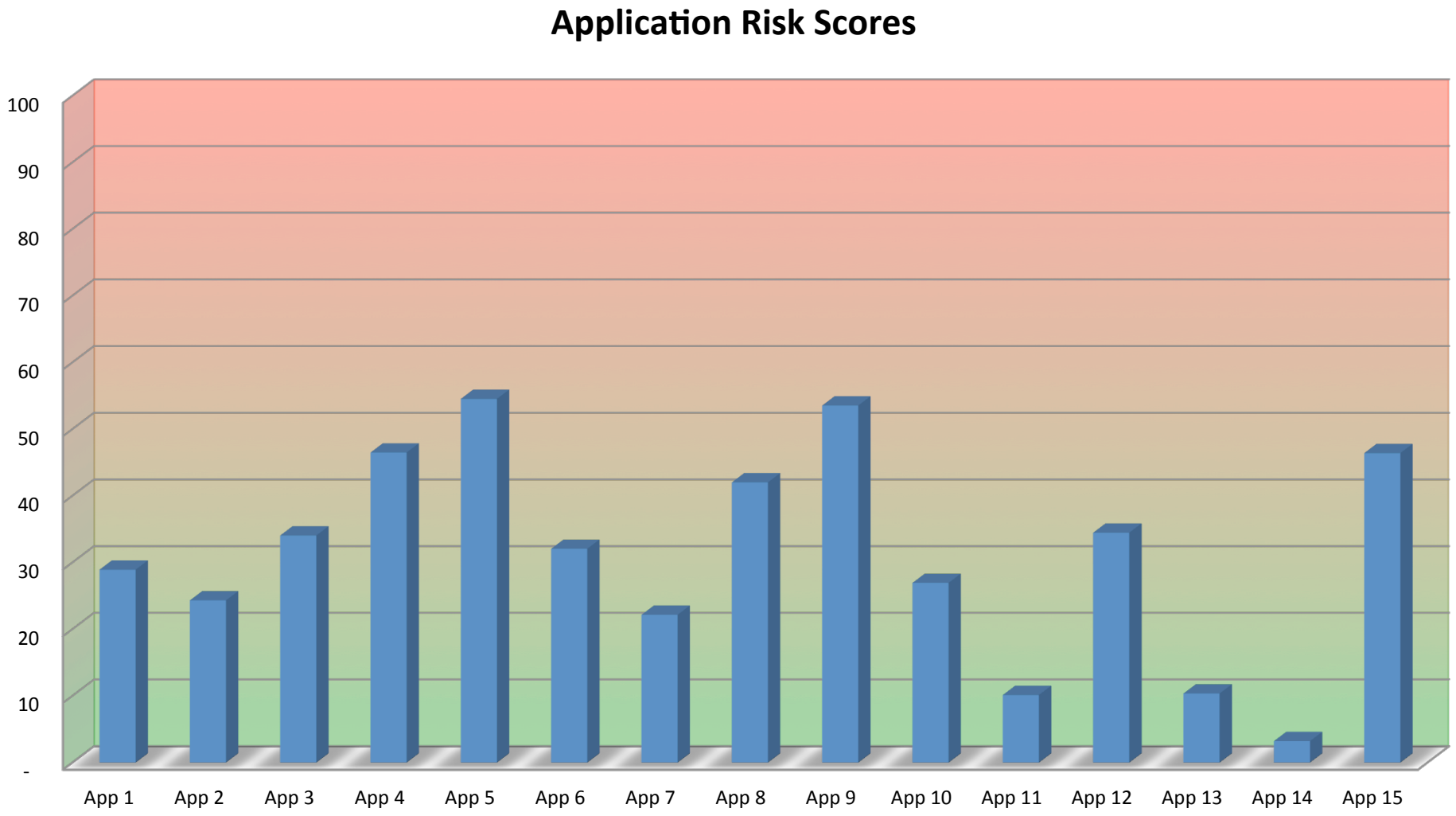




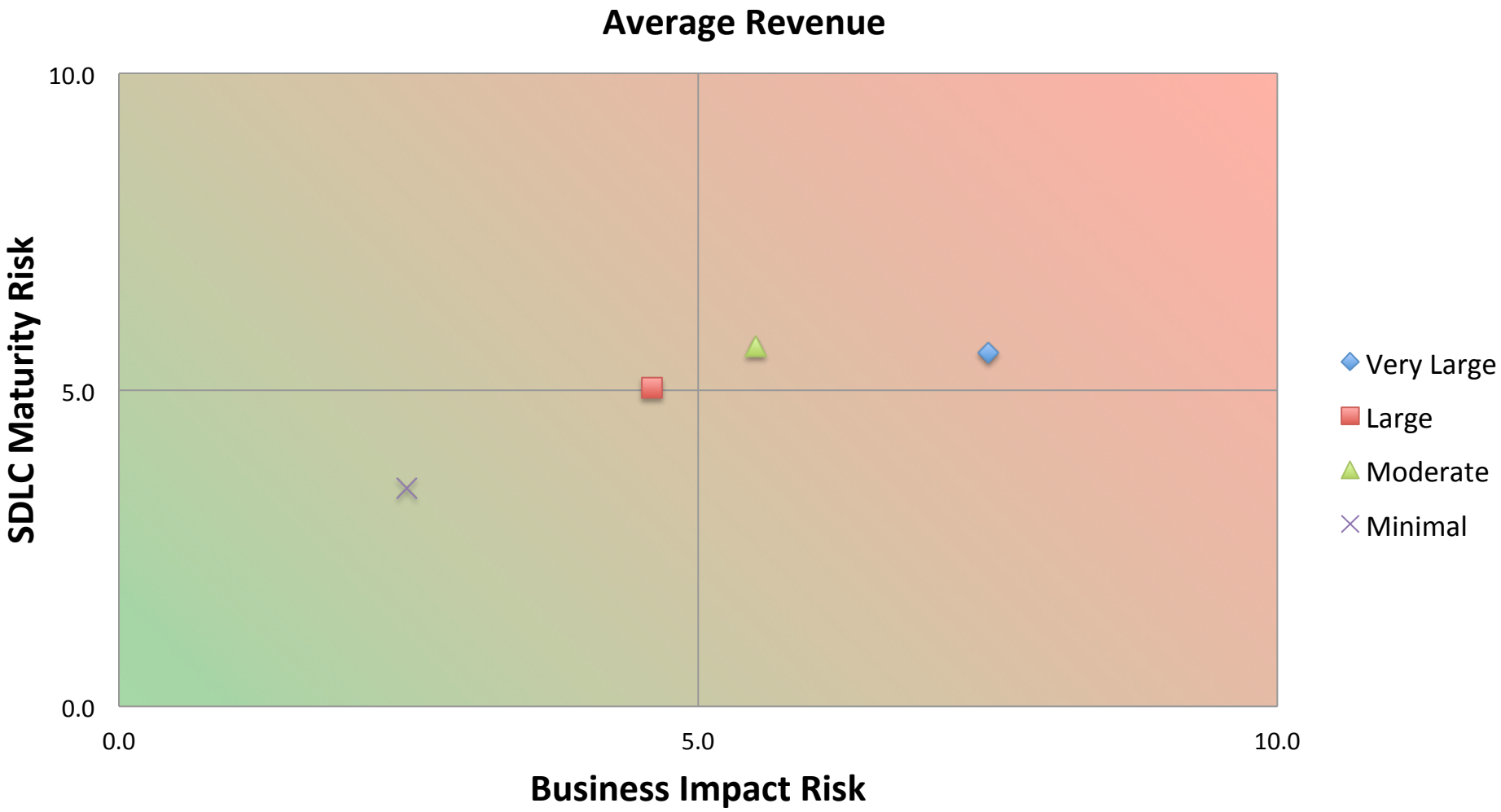




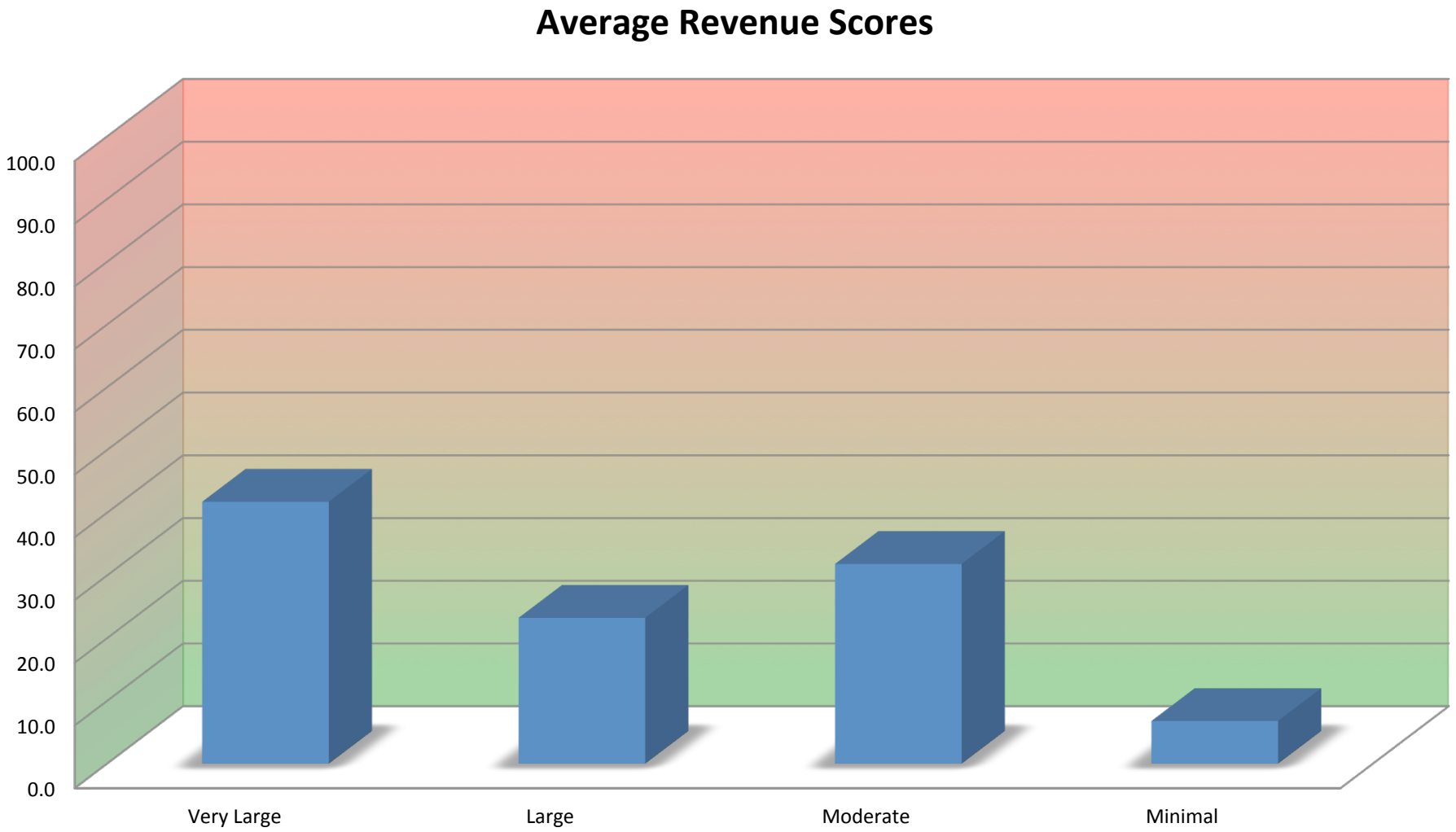
Sample Dashboards



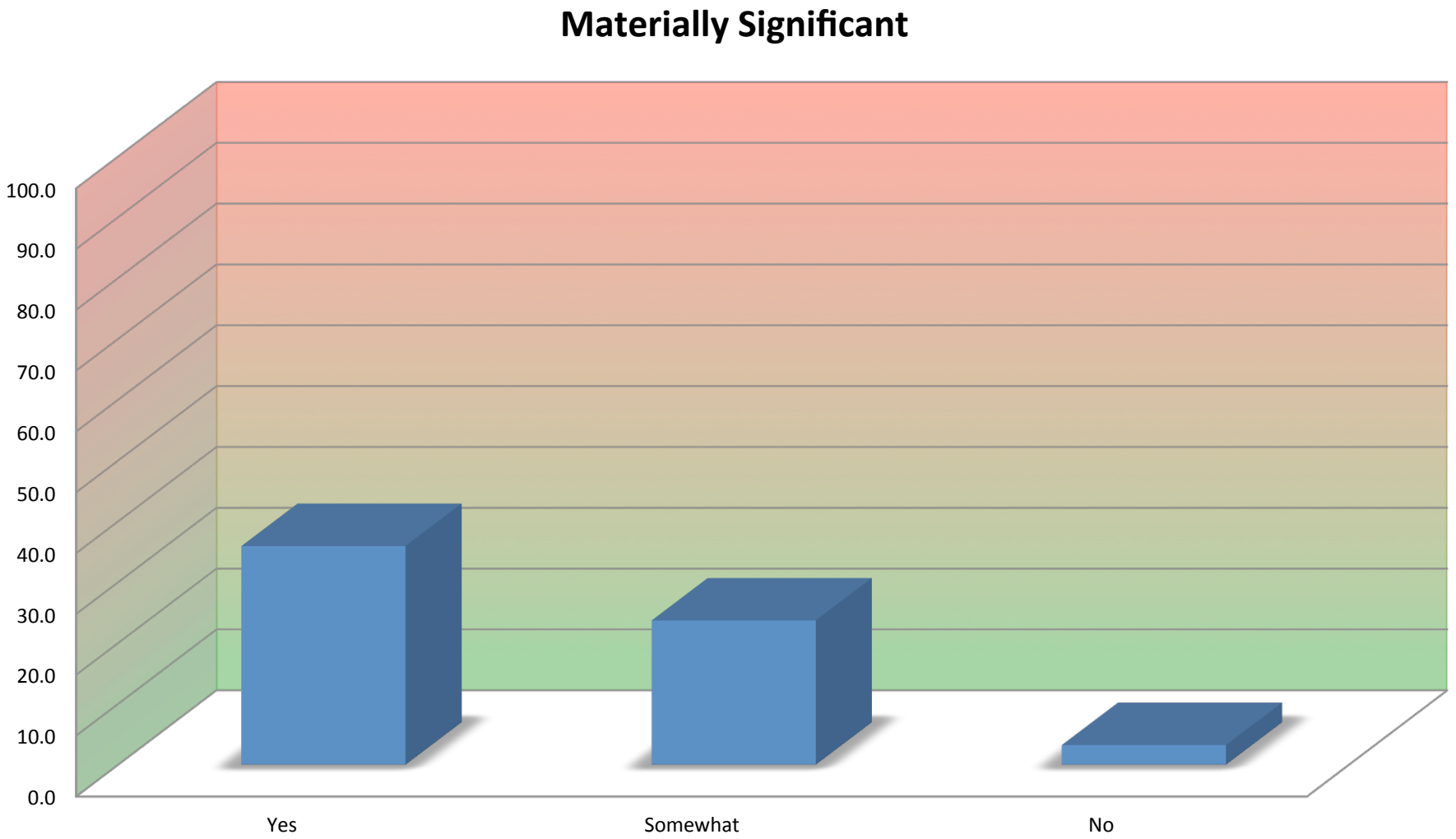
Sample Dashboards



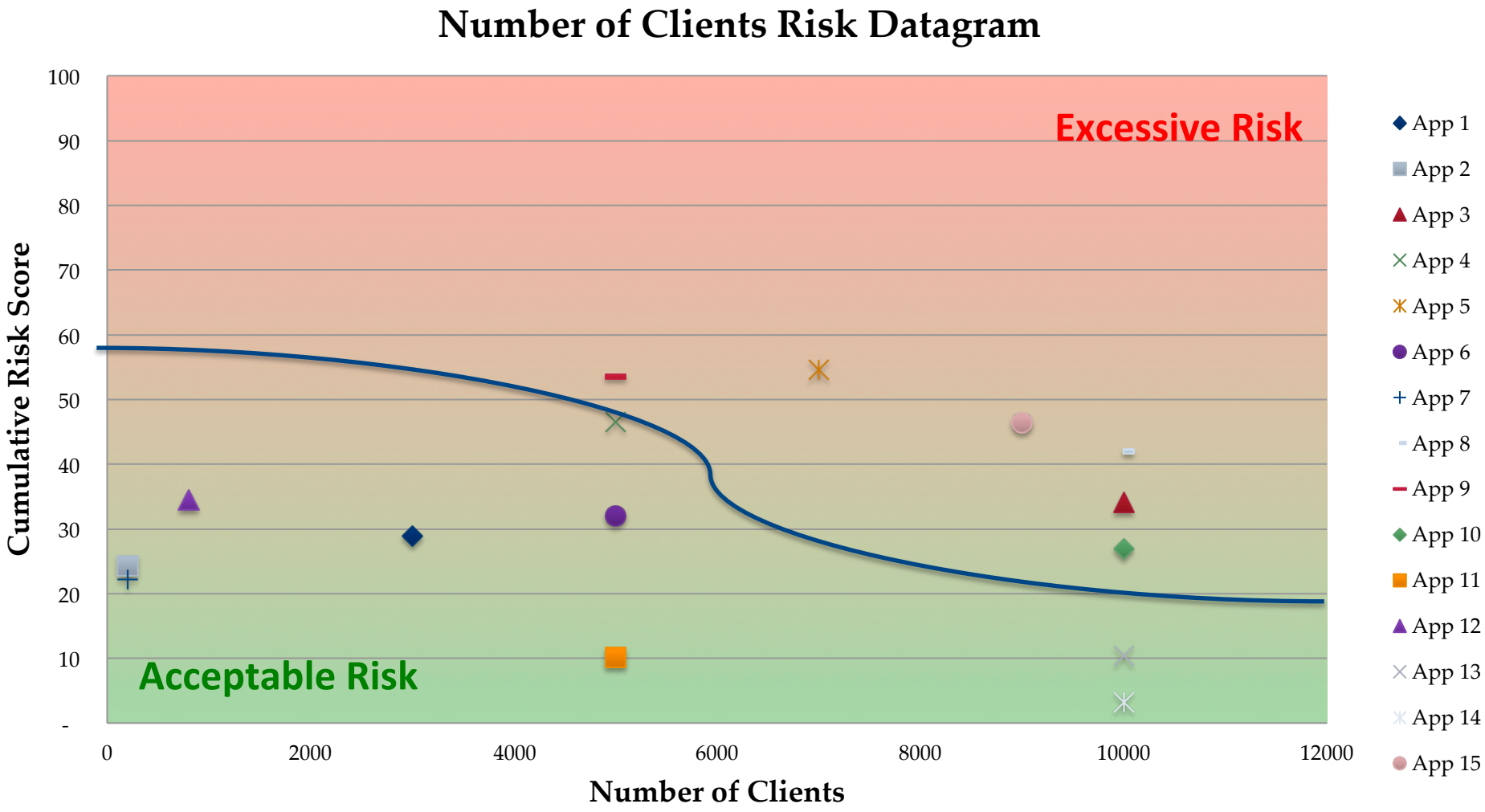
Sample Dashboards



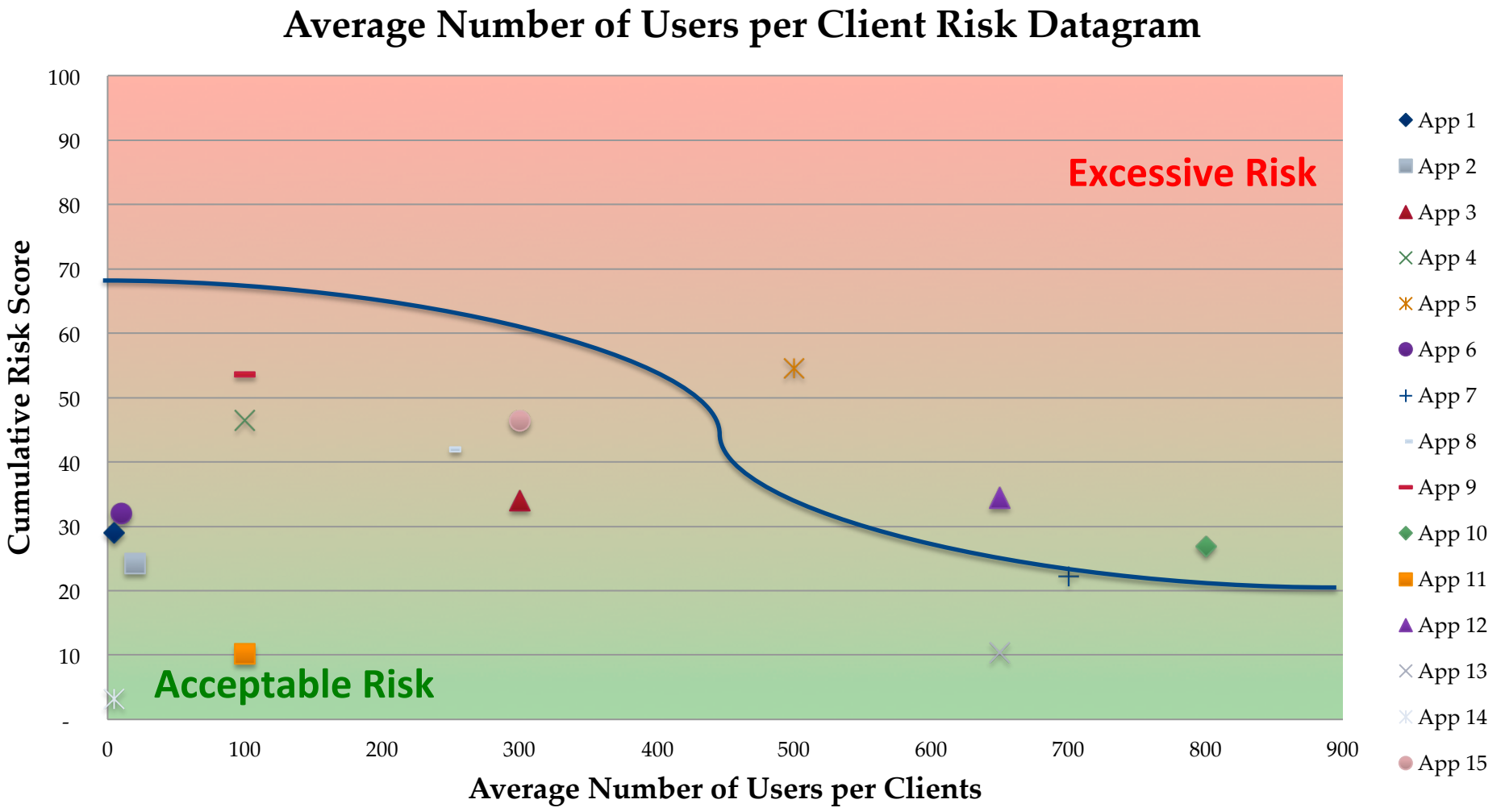
Sample Dashboards



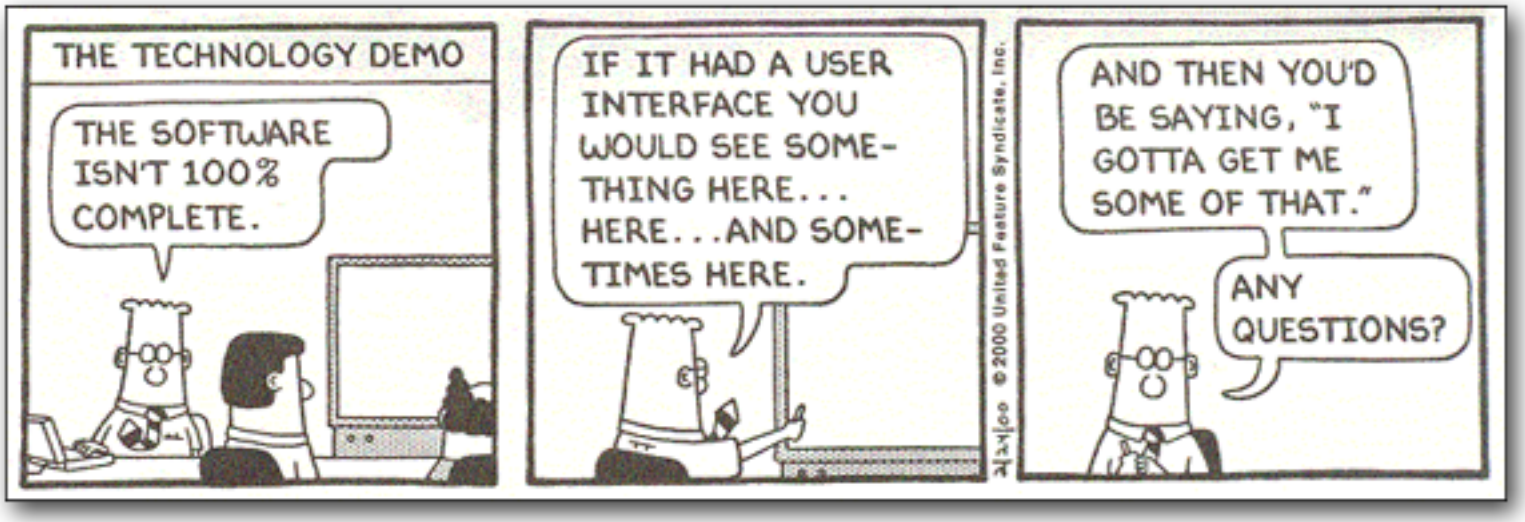
Sample Dashboards



Sample Dashboards



Time for a quick demo…



Summary

- Enhanced ability to manage the entire application security portfolio
- Normalizes risk scoring between different applications
- Allows application security optimization through efficient "what-if" calculations
- Helps identify insecure applications
- Metrics support ability to make application security decisions
- Measures accomplishments and highlights application risk reduction activities

Questions?

- Application Value / Potential Impact
- Maturity / Susceptibility
- Open SAMM
- Risk Correlation
- Dashboards

Yan Kravchenko – 612-455-8485
yan.kravchenko@netspi.com

netSPI

RISK COMPLIANCE SECURITY

Thank you!