Building a Corporate Application Security Assessment Program

Rob Jerdonek and Topher Chung
Corporate Information Security
Intuit Inc.

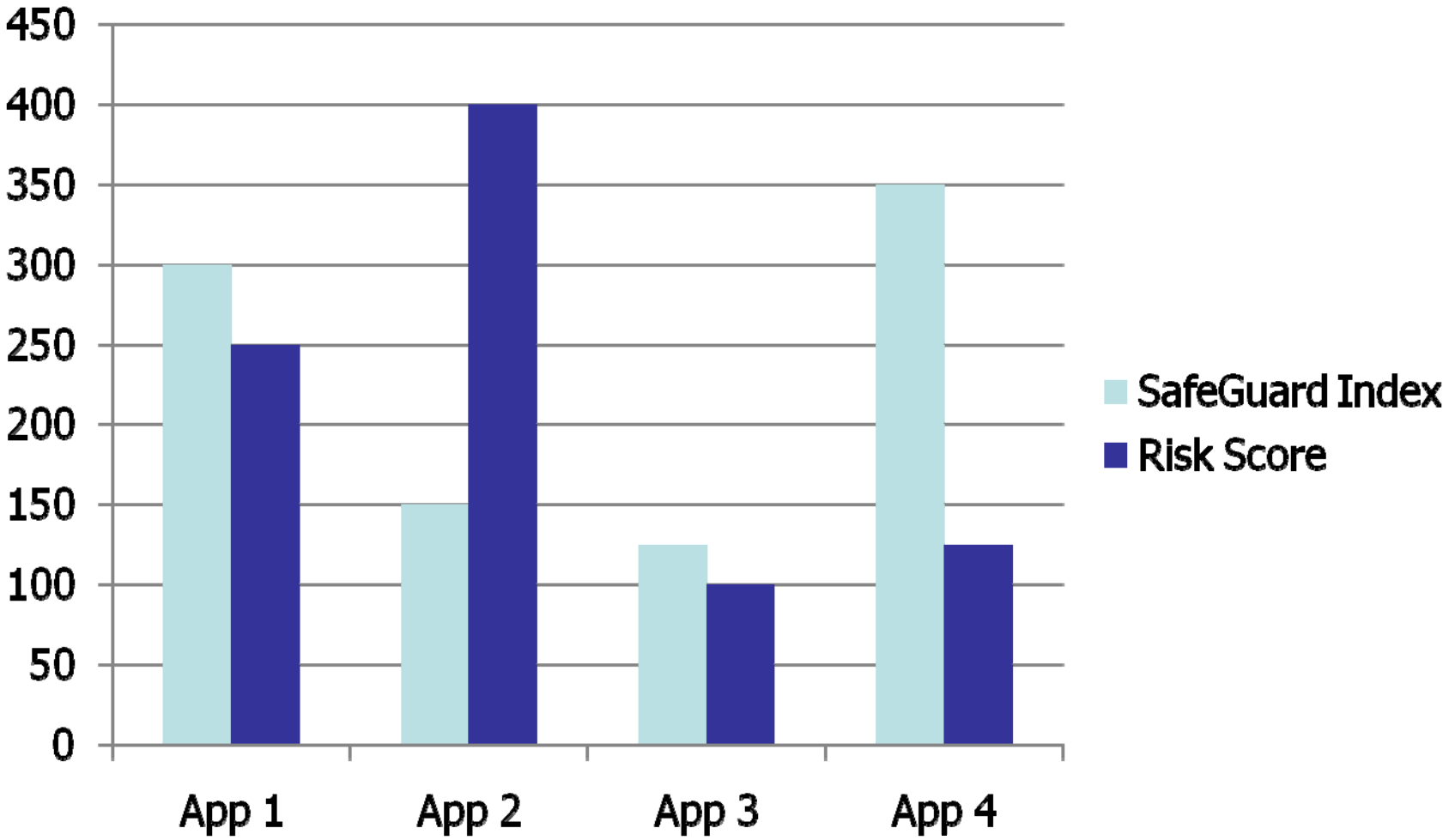
OWASP

July 23, 2009

Steps to Building a Corporate Application Security Assessment Program

- Identify goals and objectives of the program
- Define process and methodology
- Record and track quantitative results.
- Use results to drive process and technology improvements.

Comparing Risk Across Applications



Identify Goals of Assessment Program

- **Scale**: Provide high value assessment services across the entire company in a timely manner.
- **Consistency**: Unified approach to remove variability among different apps and business units.
- **Results:** Record and track quantitative results. Monitor trends over time.
- **Improvements:** Use results to drive technology and process improvements.

Note: Maps to Six Sigma methods (DMAIC and DMADV)

Examples of other goals and objectives

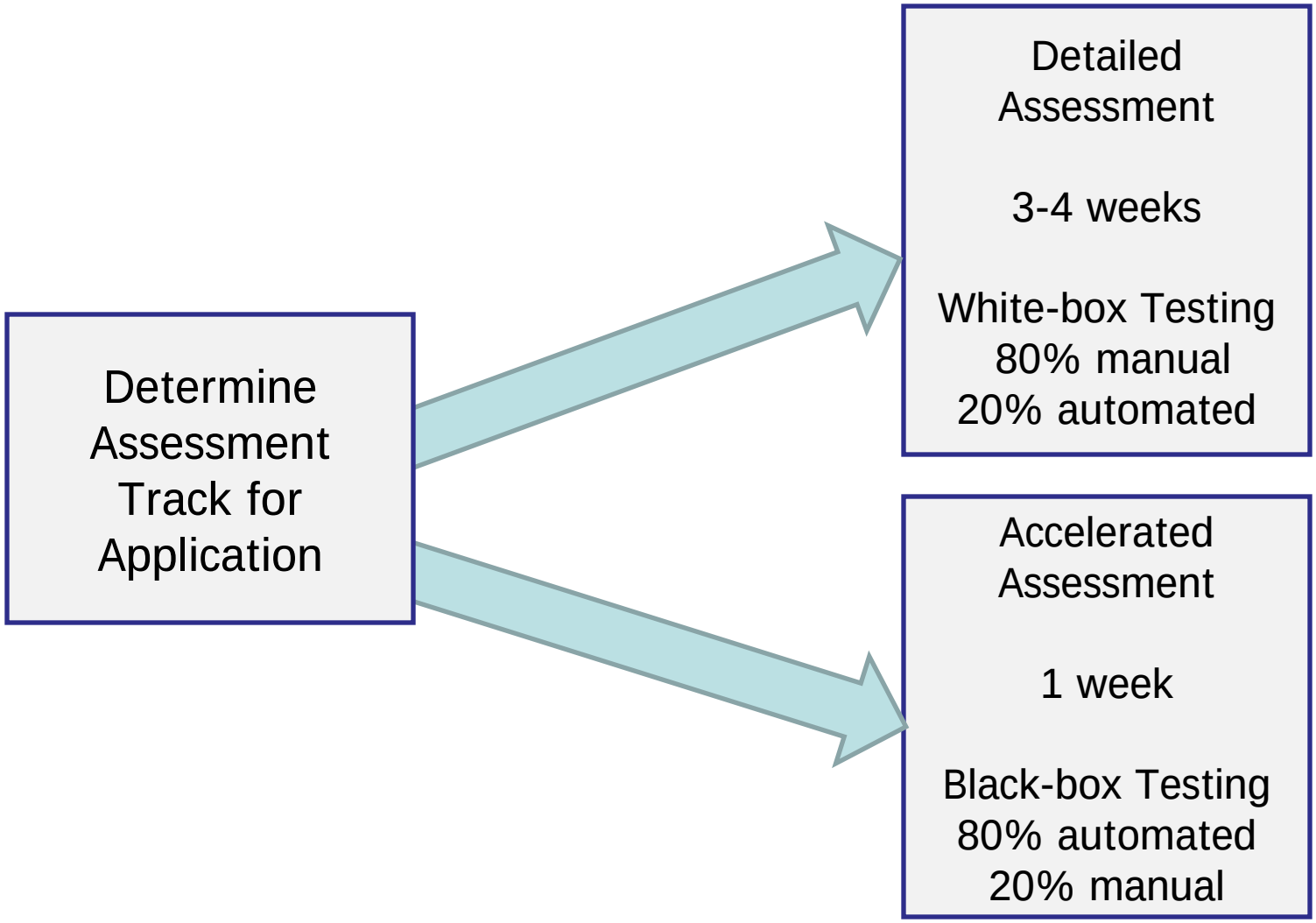
- Continuously improve the security posture of applications.
- Provide qualitative and quantitative risk analysis for applications.
- Help justify strategic investments to improve security
- Keep applications in line with evolving industry best practices and regulatory landscape.
- Embed security into the SDLC.

Define Process and Methodology

Assessment Process requirements:

- Consistent process among all applications.
- Adaptable to uniqueness of each application (small, large, etc..)
- Not dependent on any particular tool or technology.

Assessment Process – Two tracks



Assessment Process - Results

Risk Metrics

How much risk is carried by the application? What is the business impact?

Benchmarking relative to other corporate apps

Vulnerability List

Vulnerabilities found and/or exploited during penetration testing

Threat List

Threat control deficiencies found from Architecture Interviews and Threat Analysis.

Recommendations

Actionable recommendations for any all threats & vulnerabilities

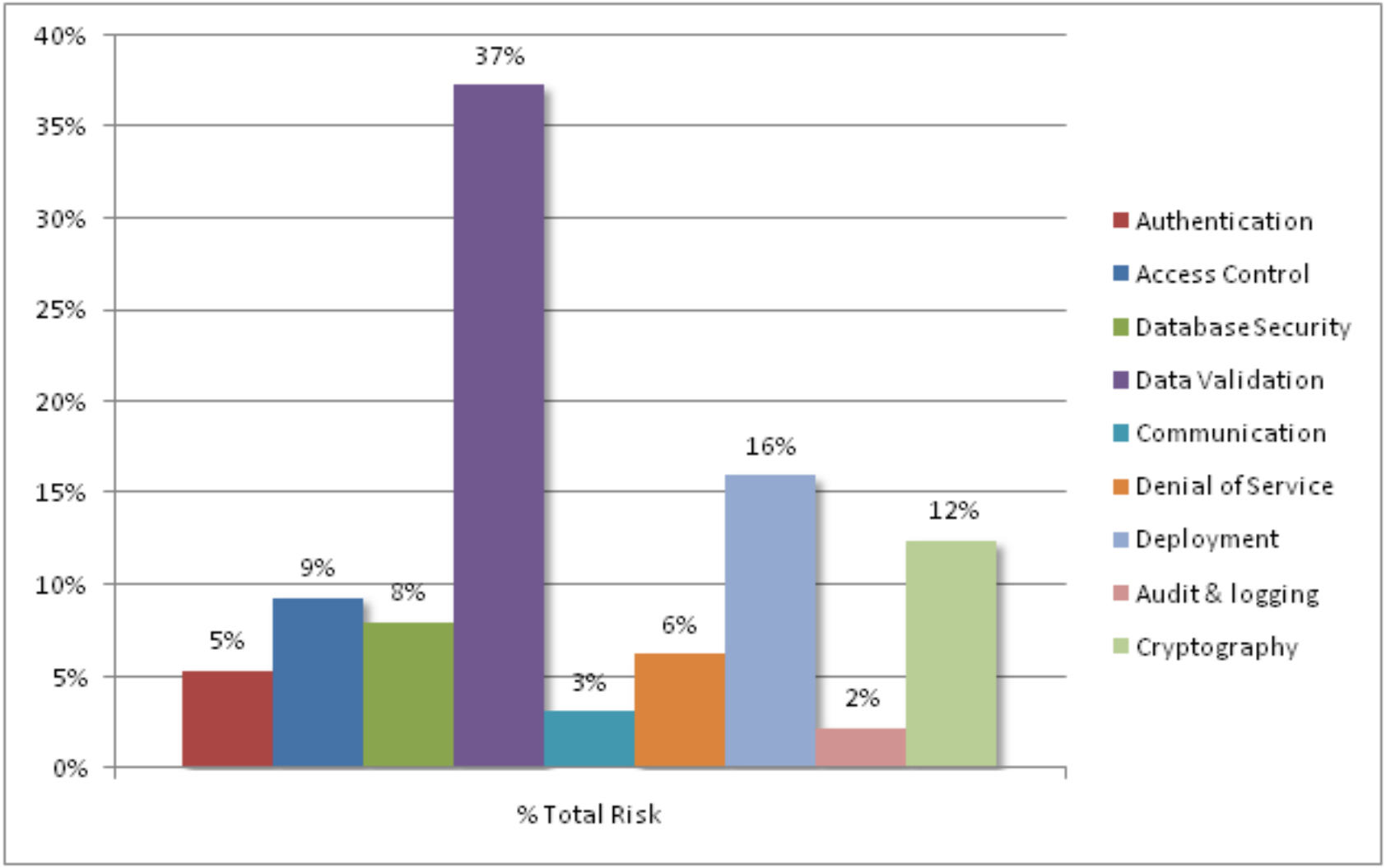
Risk Metrics- Categories

9 Risk Categories

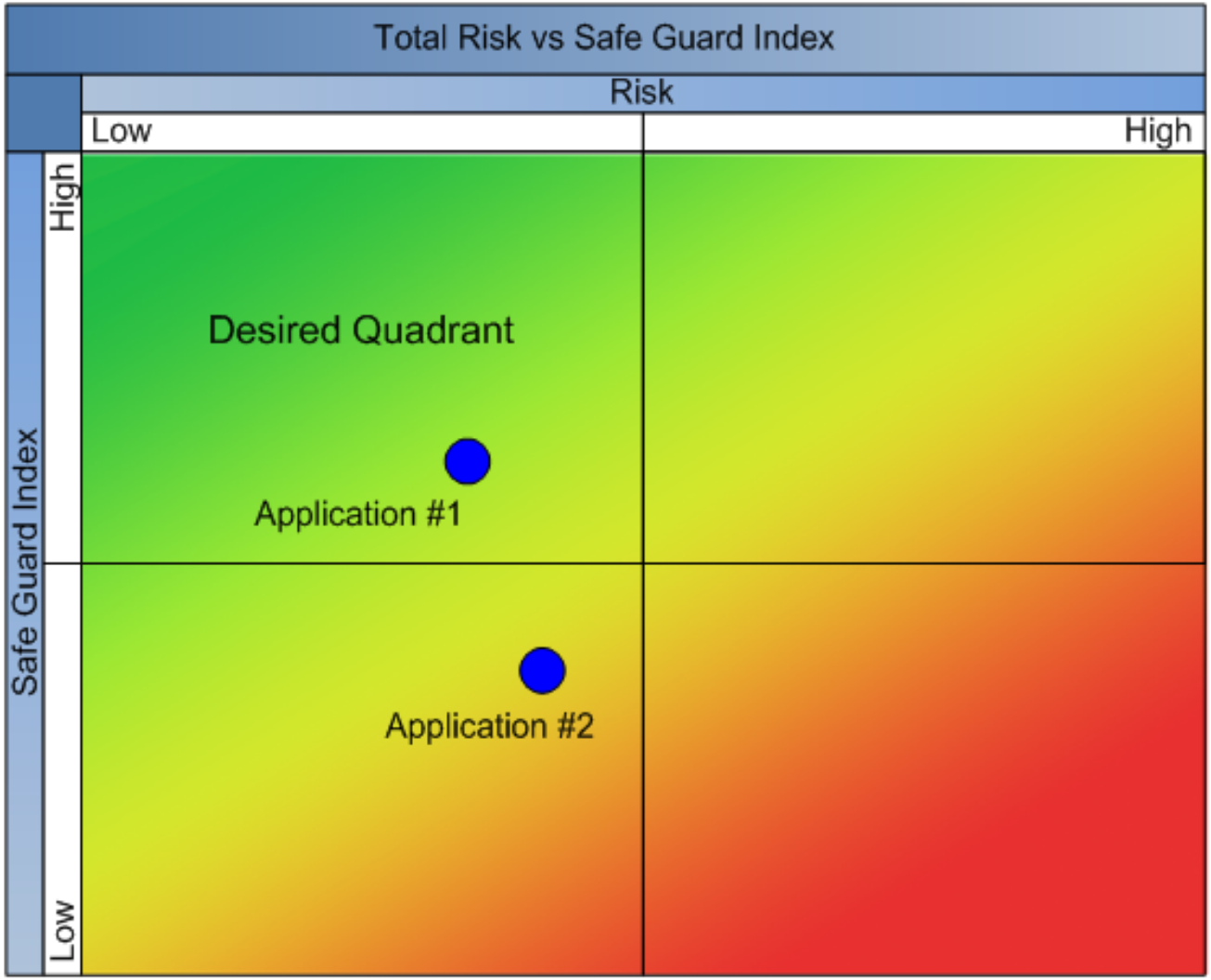
- Authentication
- Access Control
- Database Security
- Data Validation
- Communication
- Denial of Service
- Deployment
- Audit & Logging
- Cryptography

- All threats & vulnerabilities are put into the above categories.
- Risk scores are distributed among these categories

Allocation of Risk



Application Assessment “Heat Map”



Risk Metrics- Calculations

Threat Risk is architectural risk.

Total Risk Score = Risk $_{(Threats)}$ + Risk (Vulnerabilities)

Vulnerability Risk comes from vulnerabilities found during penetration testing.

Lower is better.

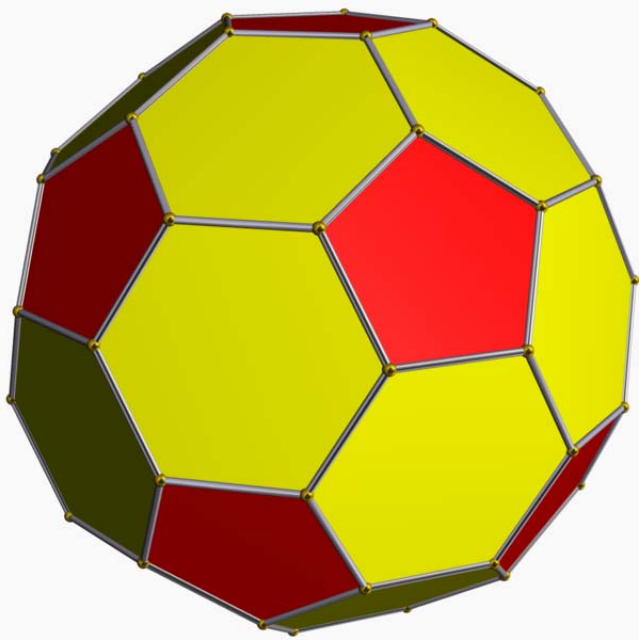
Safe Guard Index =

(Actual Control Rating / Perfect Control Rating) * 100%

Higher is better.

Threat analysis

Application looks like a soccer ball.



- Each patch on the ball is a threat surface.
- Each patch is examined for threat potential.
- How well does an application control the threat?
- Each patch is tested for security weaknesses.
- Currently 28 threat categories are examined.

Threat Analysis - DREAD

Damage potential: How great is the damage if the vulnerability is exploited?

Reproducibility: How easy is it to reproduce the attack?

Exploitability: How easy is it to successfully exploit this condition?

Affected users: As a rough percentage, how many users are affected?

Discoverability: How easy is it to find the vulnerability?

DREAD Rating Criteria - Examples

Rating Scale	8-10 (High)	4-7 (Medium)	1-3 (Low)
Damage Potential	Subvert security system, run as Admin, upload content	Leakage of sensitive information.	Leaking trivial information
Reproducibility	No timing window required.	Only within timing window.	Difficult to reproduce.
Exploitability	Easily exploitable by novice .	Takes repeated steps by skilled attacker.	Requires extremely skilled attacker w/ indepth knowledge.
Affected Users	Impacts large user base.	Impacts only a small group of users.	Impacts very small group of users.
Discoverability	Found in most common features and very noticeable	Likely noticed by only a few users.	Obscure bug. Very unlikely to be discovered.

Threat Analysis – Control Rating

0	1-2	3-4	5
No security control implementation in place to mitigate the threat.	No security control implementation in place to mitigate the threat.	Security control implementation in place is in compliance with the information security policies. Scoring of 3 and 4 provides the degree to which it is policy compliant.	High degree of security control implementation in place to mitigate the threat. Complies with the industry standard best practices.

Threat Analysis- Residual Risk

DREAD score if no control implemented						
Control Rating: Degree to which security control is implemented		**1-2**	**3-4**	**5-6**	**7-8**	**9-10**
	0	5	7	8	9	10
	1	5	6	7	8	9
	2	4	5	6	7	8
	3	2	4	5	6	7
	4	1	1	1	2	3
	5	0	0	0	0	0

Residual Risk = Remaining risk after accounting for control rating

Using Results to Drive Improvements

- Compare overall risk between BU's.
- Compare risk among Applications in a single BU.
- Identify areas for application security improvements.
- Monitor performance over time.

Using Results to Drive Improvements (cont.)

- Use assessment results to target strategic investments in security:
  - Shared Security Components
  - Security Testing tools
  - Identity Management Infrastructure, etc…