Risk Management Standards in Practice

Robert A. Martin
20 March 2018
One element of Risk Management is Identifying Quality Gaps in Capabilities Critical to Mission/Business Functions.
One element of Risk Management is Identifying Quality Gaps in Capabilities Critical to Mission/Business Functions
Quality Gaps can occur in any of the capabilities that make up our mission/business functions.
Risk Management is about addressing the Hazards & Attacks that can impact Mission/Business Functions.

“Counter Measures - Actions” include:
- choices about architecture, design, physical decomposition, and operational approaches;
- adding/changing security/safety functions, protection schemes, activities & processes;
- use of static & dynamic code assessments, dynamic testing, physical testing, and pen testing;
- attack surface & fault-tree analysis, architecture and design reviews.

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 17-3226-30
CWSS & the Common Weakness Risk Analysis Framework (CWRAF) in a Nutshell

<table>
<thead>
<tr>
<th>CWSS Score</th>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>97</td>
<td>CWE-79</td>
</tr>
<tr>
<td>95</td>
<td>CWE-78</td>
</tr>
<tr>
<td>94</td>
<td>CWE-22</td>
</tr>
<tr>
<td>94</td>
<td>CWE-434</td>
</tr>
<tr>
<td>94</td>
<td>CWE-798</td>
</tr>
<tr>
<td>93</td>
<td>CWE-120</td>
</tr>
<tr>
<td>93</td>
<td>CWE-250</td>
</tr>
<tr>
<td>92</td>
<td>CWE-770</td>
</tr>
<tr>
<td>91</td>
<td>CWE-829</td>
</tr>
<tr>
<td>91</td>
<td>CWE-190</td>
</tr>
<tr>
<td>91</td>
<td>CWE-494</td>
</tr>
<tr>
<td>90</td>
<td>CWE-134</td>
</tr>
<tr>
<td>90</td>
<td>CWE-772</td>
</tr>
<tr>
<td>90</td>
<td>CWE-476</td>
</tr>
<tr>
<td>90</td>
<td>CWE-131</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>

CWSS Scoring Engine

User-defined cutoff

W is all possible weaknesses

Wd is all known weaknesses (CWE)

Most Important Weakness/Quality Gaps

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 17-3226-30
Common Weakness Scoring System (5 Sep 2014)

Base Finding Group
- Technical Impact
- Acquired Privilege
- Acquired Privilege Layer
- Internal Control Effectiveness
- Finding Confidence

Attack Surface Group
- Required Privilege
- Required Privilege Layer
- Access Vector
- Authentication Strength
- Level of Interaction
- Deployment Scope

Environmental Group
- Business Impact
- Likelihood of Discovery
- Likelihood of Exploit
- External Control Effectiveness
- Prevalence

Common Weakness Risk Analysis Framework (CWRAF)
- Vignettes
- Technical Impact Scorecard
Common Vulnerability Scoring System

- NVD provides CVSS scores for all CVE identifiers
- Payment Card Industry (PCI) using CVSS to determine compliance

www.first.org/cvss/
Standards for Inputs and Calculating Risks...
Cyber Risk is Expanding into Physical Risk

IT Risk

Operational Risk

Loss of information or service

Loss of reliability or safety

Loss of life or property

“Back office”

Production

© 2017 Gartner. All rights reserved.

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 17-3328-30
Who’s risk is being managed?