TRUSTWORTHINESS & SECURITY MATURITY MODEL

FREDERICK HIRSCH

FUJITSU

SYDNEY INDUSTRY DAY
THE WORLD IS CHANGING

Frederick Hirsch

Deliver

Software

Hardware

OEM

Solution Provider

Software Integrator

Transaction

Services

SeaS

Trust

ODM

Development Tools

Software Stack

Container

Guest OS

IaaS

Hyervisor

Firmware

Modules

Chips

Frederick Hirsch

FUSU
RISK

• Risk - “A state of uncertainty where some of the possibilities involve a loss, catastrophe, or some other undesirable outcome.”*
  • Uncertainty → Probability
  • Outcome → Quantified Loss

* Hubbard, Seiersen; How to Measure Anything in Cybersecurity Risk
UNCERTAINTY

- Risk - “A state of uncertainty where some of the possibilities involve a loss, catastrophe, or some other undesirable outcome.”
  - Uncertainty → Probability
  - Outcome → Quantified Loss
CONSEQUENCES

- Risk - “A state of uncertainty where some of the possibilities involve a loss, catastrophe, or some other undesirable outcome.”
  - Uncertainty → Probability
  - Outcome → Quantified Loss
APPROACH

• Risk - “A state of uncertainty where some of the possibilities involve a loss, catastrophe, or some other undesirable outcome.”
  • Uncertainty → Probability
  • Outcome → Quantified Loss
BUILDING ON PREVIOUS WORK

Reference Architecture (IIRA)

Security Framework (IISF)

Connectivity Framework (IICF)

Vocabulary
RECENT PUBLICATIONS

Dec 2017
Safety Challenges
Frederick Hirsch
Fujitsu

Sept 2018
Journal of Innovation: Trustworthiness

June 2019
AI

July 2019
Managing & Assessing

https://www.iiconsortium.org/white-papers.htm
ASSURANCE AND EVIDENCE
SECURITY MATURITY MODEL (SMM)

https://www.iiconsortium.org/smm.htm

https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_FINAL_Updated_V1.1.pdf

Security maturity is a measure of the understanding of the current security level, its necessity, benefits and cost of its support.

Security level is a measure of confidence that system vulnerabilities are addressed appropriately and that the system functions in an intended manner.

- **Security maturity** is a measure of the understanding of the current security level, its necessity, benefits and cost of its support.
- **Security level** is a measure of confidence that system vulnerabilities are addressed appropriately and that the system functions in an intended manner.
MANY FRAMEWORKS BUT NO SINGLE STANDARD

Common Criteria

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAL 1</td>
<td>Functionally tested</td>
</tr>
<tr>
<td>EAL 2</td>
<td>Structurally tested</td>
</tr>
<tr>
<td>EAL 3</td>
<td>Methodically tested and checked</td>
</tr>
<tr>
<td>EAL 4</td>
<td>Methodically designed, tested, and reviewed</td>
</tr>
<tr>
<td>EAL 5</td>
<td>Semiformally designed and tested</td>
</tr>
<tr>
<td>EAL 6</td>
<td>Semiformally verified design and tested</td>
</tr>
<tr>
<td>EAL 7</td>
<td>Formally verified design and tested</td>
</tr>
</tbody>
</table>

NIST Cyber Security Framework

C2M2

Optimized Organizational strategy

Processes managed, based on measures

Processes defined, performance managed

Managed Activities are managed

Unpredictable, reactively managed

Defined

Work done according processes

Initial

Project success depends on individual performance

- Focus on improvement
- Quantitatively Managed
- Processes and activities are managed based on measures
- Defined
- Work done according processes
- Managed
- Activities are managed
- Unpredictable
- Reactively managed
SMM Structure and Tables

Frederick Hirsch
<table>
<thead>
<tr>
<th>Objective</th>
<th>Comprehensiveness Level 1</th>
<th>Comprehensiveness Level 2</th>
<th>Comprehensiveness Level 3</th>
<th>Comprehensiveness Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective Description</td>
<td>Objective Description</td>
<td>Objective Description</td>
<td>Objective Description</td>
<td>Objective Description</td>
</tr>
<tr>
<td>General considerations</td>
<td>Level Description</td>
<td>Level Description</td>
<td>Level Description</td>
<td>Level Description</td>
</tr>
<tr>
<td>What needs to be done to achieve this level</td>
<td>What needs to be done to achieve this level</td>
<td>What needs to be done to achieve this level</td>
<td>What needs to be done to achieve this level</td>
<td></td>
</tr>
<tr>
<td>Considerations</td>
<td>Considerations</td>
<td>Considerations</td>
<td>Considerations</td>
<td>Considerations</td>
</tr>
<tr>
<td>Indicators of accomplishment</td>
<td>Indicators of accomplishment</td>
<td>Indicators of accomplishment</td>
<td>Indicators of accomplishment</td>
<td></td>
</tr>
<tr>
<td>Considerations</td>
<td>Considerations</td>
<td>Considerations</td>
<td>Considerations</td>
<td>Considerations</td>
</tr>
</tbody>
</table>

Levels include all the considerations of the lower levels
ACTIONABLE

• Practitioner’s Guide
• Profiles
• Mappings
• Training
THANK YOU

Frederick Hirsch, Fujitsu
@fjhirsch
fjhirsch.com

IIC Journal of Innovation, Trustworthiness:

Security Maturity Model Practitioner’s Guide:
https://www.iiconsortium.org/smm.htm