UST PrivacyProof

NIST Privacy Maturity Assessment – Using CMMI

October 27th, 2021
Mark Keelan - Director Privacy Practice
mark.Keelan@ust.com
Agenda

• Introductions
• State of the Privacy Market
• NIST PF & CMMI
• Hands on – Interactive Option
• Next Steps
Mark Keelan

UST
Director of Privacy Practice
mark.keelan@ust.com

• 36 Years in Information Technology
• Privacy, Cyber Security, Digital Analytics, Data Discovery and Classification, ERP, and more
• IBM, PeopleSoft, Blue Yonder
• ISSA LA Advisory Board
• IAPP LA Co-Chair
• ISACA Member
State of Privacy Today

• More and More Digital Information
  • Tracked and stored
  • Breached

• New legislation constantly being enacted
  • CPRA Passed in California – New Regulatory Enforcement Agency added
  • India looking to pass a new law
  • Brazil LGDP now in force
  • other US states and countries privacy laws are changing

• Immature Market
  • Product companies have fragmented offerings
  • Incomplete solutions require multi-product deployments
  • Largest product company VC funded and burning cash

• Covid-19 adversely impacted compliance projects
  • Projects delayed and placed on the back burner
  • This will likely create a panic to meet regulatory requirements in the end

Privacy is a Mess
But Most Critically

- **COMPANIES ARE NOT INVESTING IN PRIVACY**
  - Don’t want to invest in the platforms
  - Don’t want to invest in the talent
  - Don’t want to invest in operations

- Although...
  - EVERY company that deals with PII SAYS that Privacy is of critical importance
  - But very few put their money where their mouth is

- Results
  - Privacy platforms don’t mature
  - Privacy professionals don’t advance
  - Individuals don’t get their rights

- Why?
  - Because of the Risk Based Viewpoint of Modern Privacy Frameworks
  - Risk Based Frameworks Drive Businesses to
    - Spend the least amount of money on privacy
    - To achieve the maximum risk, will tolerate

\[
\text{MINIMUM COST} = \text{MAXIMUM RISK} + \text{MINIMAL CAPABILITIES}
\]
How Can We Change This?

• How Can We Change The Way We Measure Privacy To Encourage Investment?
  • Highest Value = Maximum Capability + Minimum Risk

• Make improvements in your ability to be:
  • “Measurable”
  • “Actionable”

• How to accomplish this?
  • NIST Privacy Framework Adoption
  • Capability Maturity Model Integration
  • Privacy Maturity Model
  • Qualitative & Quantitative Measurements
• NIST Cyber Security Framework is already the Gold Stand

• Important to consolidate support around one standard

• Free
  • https://www.nist.gov/privacy-framework/privacy-framework

• Acknowledge
  • Early in its life
  • Needs adoption

UST Supports the NIST Privacy Framework
Who we are

Impact unbound

Transforming the world's best companies through the power of technology.

Our history
Born digital in 1999
HQ, Orange County, CA
26,000* employees
140* global 1000 clients

Industry verticals
Financial Services
Healthcare
Retail & CPG
Manufacturing
Technology, Media & Telecom
Semiconductor
Public Sector

Global presence
25 countries
79 offices worldwide
USA, Canada, India, Malaysia, Singapore, Philippines, China,
Taiwan, Australia, Israel, England, Bulgaria, France, Germany,
Portugal, Poland, Spain, Mexico
Where you’ll find us

AMERICAS
Global HQ – Orange County, CA
Bentonville, AR
Chicago, IL
New York, NY
Toronto
Guadalajara
Leon

EMEA
London
Madrid
Tel Aviv
Berlin
Lisbon
Paris

INDIA
Trivandrum
Bangalore
Chennai
Hyderabad
Kochi

APAC
Singapore
Manila
Penang
Shanghai
Taiwan
Sydney

*To see a list of all offices, visit ust.com
The largest enterprises in the world across industries trust UST as their digital partner

<table>
<thead>
<tr>
<th>Manufacturing</th>
<th>Dana</th>
<th>GE</th>
<th>Rockwell Automation</th>
<th>Otis</th>
<th>Navistar</th>
<th>Liebherr</th>
<th>Bosch</th>
<th>UPS</th>
<th>BMW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail &amp; CPG</td>
<td>Albertsons</td>
<td>Walgreens Boots Alliance</td>
<td>Carrefour</td>
<td>Ahold Delhaize</td>
<td>H-E-B</td>
<td>Levi's</td>
<td>Nike</td>
<td>LEGO</td>
<td></td>
</tr>
<tr>
<td>Healthcare</td>
<td>Anthem</td>
<td>McKesson</td>
<td>Cigna</td>
<td>Independence</td>
<td>Cardinal Health</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Services</td>
<td>Equifax</td>
<td>Santander</td>
<td>Experian</td>
<td>Bank of America</td>
<td>Discover</td>
<td>Macquarie</td>
<td>BBVA</td>
<td>SunTrust</td>
<td>Schroders</td>
</tr>
<tr>
<td>Telecom, Media</td>
<td>Dell</td>
<td>Apple</td>
<td>Microsoft</td>
<td>Wolters Kluwer</td>
<td>Verizon</td>
<td>T-Mobile</td>
<td>Telefonica</td>
<td>Amazon</td>
<td></td>
</tr>
<tr>
<td>&amp; Technology</td>
<td>Adobe</td>
<td>Intel</td>
<td>NetApp</td>
<td>Hewlett Packard Enterprise</td>
<td>Comcast</td>
<td>Nokia</td>
<td>Sprint</td>
<td>VMware</td>
<td></td>
</tr>
</tbody>
</table>

UST
The Importance of NIST Continues to Grow

• Ohio has introduced new data privacy legislation
  • July 13, 2021 - Lieutenant Governor John Husted announced the introduction of OPPA - Ohio Personal Privacy Act

• The NIST Privacy Framework is at the core
  • “The Ohio Privacy Act also contains a notable deviation from privacy laws enacted in other states: Businesses can utilize an affirmative defense from an enforcement action by the Ohio Attorney General or a lawsuit filed by a consumer if the business creates, maintains, and complies with a written privacy program that reasonably conforms to the National Institute of Standards and Technology privacy framework.” —National Law Review

• In Ohio, following the NIST PF *directly* protects you from legal penalty
NIST Privacy Framework & CMMI

- Qualitative – NIST PF
  - Risk Focused
  - Described in words
  - Results
    - Narrative
    - Relative

- Quantitative - CMMI
  - Value Focused
  - Described in numbers
  - Results
    - Numeric Score
    - Normalized
# NIST Privacy Framework – “Qualitative”

## NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management

### Version 1.0 Core

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.</td>
<td>Inventory and Mapping (ID.IM-P): Data processing by systems, products, or services is understood and informs the management of privacy risk.</td>
<td>ID.IM-P1: Systems/products/services that process data are inventoried.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.IM-P4: Data actions of the systems/products/services, that process data are inventoried.</td>
</tr>
</tbody>
</table>
Capability Maturity Model - “Quantitative”

**Maturity Level 5**
- **Optimizing**
  - **Stable and flexible.** Organization is focused on continuous improvement and is built to pivot and respond to opportunity and change. The organization’s stability provides a platform for agility and innovation.

**Maturity Level 4**
- **Quantitatively Managed**
  - **Measured and controlled.** Organization is data-driven with quantitative performance improvement objectives that are predictable and align to meet the needs of internal and external stakeholders.

**Maturity Level 3**
- **Defined**
  - **Proactive, rather than reactive.** Organization-wide standards provide guidance across projects, programs and portfolios.

**Maturity Level 2**
- **Managed**
  - **Managed on the project level.** Projects are planned, performed, measured, and controlled.

**Maturity Level 1**
- **Initial**
  - **Unpredictable and reactive.** Work gets completed but is often delayed and over budget.
CMMC – Good Example of NIST and CMMI combined

Cybersecurity Maturity Model Certification
NIST Privacy Maturity Assessment: Creation

Adhere to the NIST Framework

| Identify-P | Develop the organizational understanding to manage privacy risk for individuals arising from data processing. |
| Govern-P   | Develop and implement the organizational governance structure to enable an ongoing understanding of the privacy risk. |
| Control-P  | Develop and implement appropriate activities to enable organizations or individuals to manage data with restrictions. |
| Communicate-P | Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding of privacy risks. |
| Protect-P  | Develop and implement appropriate data processing safeguards. |

Adhere down to the Subcategory Level

- **Systems / Products / Services that process data are inventoried** - ID.IM-P1 - NIST Privacy - Identify-P -
- **Owners / Operators / Roles that process data are inventoried** - ID.IM-P2 - NIST Privacy - Identify-P -
- **Categories of individuals whose data is processed is inventoried** - ID.IM-P3 - NIST Privacy - Identify-P -
- **Data actions of the systems / products / services are inventoried** - ID.IM-P4 - NIST Privacy - Identify-P -
### NIST Privacy Maturity Assessment: Creation

Expand by adding “Capabilities” and “Maturity Levels”

<table>
<thead>
<tr>
<th>Description</th>
<th>ID.IM-P5 C1</th>
<th>Maturity Level</th>
<th>NIST Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal data action purposes initially inventoried</td>
<td></td>
<td>1 - Initial</td>
<td></td>
</tr>
<tr>
<td>External data action purposes initially inventoried</td>
<td></td>
<td>1 - Initial</td>
<td></td>
</tr>
<tr>
<td>Projects managed using external data action purpose inventory</td>
<td></td>
<td>2 - Managed</td>
<td></td>
</tr>
<tr>
<td>Projects managed using internal data action purpose inventory</td>
<td></td>
<td>2 - Managed</td>
<td></td>
</tr>
<tr>
<td>Internal data action purpose inventoried with defined organizational ...</td>
<td></td>
<td>3 - Defined</td>
<td></td>
</tr>
<tr>
<td>External data action purpose inventoried with defined organizational ...</td>
<td></td>
<td>3 - Defined</td>
<td></td>
</tr>
<tr>
<td>Internal data action purpose inventories quantitatively measured</td>
<td></td>
<td>4 - Quantitativ...</td>
<td></td>
</tr>
<tr>
<td>External data action purpose inventories quantitatively measured</td>
<td></td>
<td>4 - Quantitativ...</td>
<td></td>
</tr>
<tr>
<td>All data action purpose inventorying optimized for continual improve...</td>
<td></td>
<td>5 - Optimizing</td>
<td></td>
</tr>
</tbody>
</table>
NIST Privacy

The NIST Privacy Framework is a voluntary tool developed in collaboration with stakeholders intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy.

Progress on Assessment-2020-Oct-13 @ 13:07

Identify-P 0 of 275
- Inventory and Mapping 0 of 145
- Business Environment 0 of 25
- Risk Assessment 0 of 70
- Data Processing Ecosystem Risk Management 0 of 35

Govern-P 0 of 160
- Governance Policies, Processes, and Procedures 0 of 60
- Risk Management Strategy 0 of 25
- Awareness and Training 0 of 20
- Monitoring and Review 0 of 55

Control-P 0 of 125
- Data Processing Policies, Processes, and Procedures 0 of 45
- Data Processing Management 0 of 55
- Disassociated Processing 0 of 25

Communicate-P 0 of 74
- Communication Policies, Processes, and Procedures 0 of 10
- Data Processing Awareness 0 of 64

Protect-P 0 of 205
- Data Protection Policies, Processes, and Procedures 0 of 50
- Identity Management, Authentication, and Access Control 0 of 45
- Data Security 0 of 80
- Maintenance 0 of 10
- Protective Technology 0 of 20

Identify-P > Inventory and Mapping > Systems / Products / Services that process data are inventoried > ID.8M-Pt.CI

Level
1 - Initial

Question #1
Have the internal systems which process data been initially inventoried?
An inventory of internal systems which process data will contribute to understanding, and informing management, of privacy risk.

Answer
Yes
In Progress
No
Privacy Maturity Assessment: Reports

Interactive reports are available
Plan – Other Assessments

• NIST Privacy Framework v1.0
• ISO 27701
• ISO 27001 v2013
• NIST CSF v1.1
• PCI DSS v3.2
• SOC 2
• NIST 800-53 US HIPAA
• EMEA EU GDPR

• Minimum Compliance Controls
  • Autofill overlapping requirements
FREE
NIST PF Maturity Assessment

(NIST Cyber Security Maturity Assessment coming in Q4)

SOMETHING NEW TODAY!

HANDS ON!

https://privacyassure.force.com/s/

OPTIONAL – NOT REQUIRED

I WILL DEMO ALSO.
My Assessments

Welcome to the future of privacy. While individual certifications are important, the world of privacy lacked a qualitative and quantitative "Industry standardized organizational assessment". Not anymore!

This solution combines the best of the best to provide qualitative and quantitative privacy maturity assessments using the NIST Privacy Framework with Capability Maturity Model Integration (CMMI).

Learn More  Start New Assessment

My Assessments

You have not started any assessments yet.
NIST Privacy

The NIST Privacy Framework is a voluntary tool developed in collaboration with stakeholders intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals’ privacy.

Instructions Feedback

Progress on Assessment - 2020-10-13 @ 13:07

Identify-P 0 of 275
- Inventory and Mapping 0 of 145
- Business Environment 0 of 25
- Risk Assessment 0 of 75
- Data Processing Ecosystem Risk Management 0 of 35

Govern-P 0 of 160
- Governance Policies, Processes, and Procedures 0 of 60
- Risk Management Strategy 0 of 25
- Awareness and Training 0 of 20
- Monitoring and Review 0 of 55

Control-P 0 of 125
- Data Processing Policies, Processes, and Procedures 0 of 45
- Data Processing Management 0 of 55
- Disassociated Processing 0 of 25

Communicate-P 0 of 74
- Communication Policies, Processes, and Procedures 0 of 10
- Data Processing Awareness 0 of 64

Protect-P 0 of 205
- Data Protection Policies, Processes, and Procedures 0 of 50
- Identity Management, Authentication, and Access Control 0 of 45
- Data Security 0 of 80
- Maintenance 0 of 10
- Protective Technology 0 of 20

Level 1 - Initial

Question #1
Have the internal systems which process data been initially inventoried?

An inventory of internal systems which process data will contribute to understanding, and informing management, of privacy risk.

Answer Yes In-Progress No
NIST PF Maturity Assessment

- Hand off to Mark
- Review structure which combines NIST and CMMI
- Explain feed into survey
- Live Demo,
  - ‘Mark Keelan LIVE!’
You can also email mark.keelan@ust.com
Copyright and confidentiality notice

Copyright © 2021 by UST Global Inc. All rights reserved.

This document is protected under the copyright laws of United States, India, and other countries as an unpublished work and contains information that shall not be reproduced, published, used in the preparation of derivative works, and/or distributed, in whole or in part, by the recipient for any purpose other than to evaluate this document. Further, all information contained herein is proprietary and confidential to UST Global Inc and may not be disclosed to any third party. Exceptions to this notice are permitted only with the express, written permission of UST Global Inc.

UST® is a registered service mark of UST Global Inc.