



CMMI[®] Institute

AN ISACA ENTERPRISE



Purpose

To make the world work better



Promise

To inspire cultures of continuous improvement that elevate performance and create sustainable competitive advantage



1987

1991

2010

2013

2014

2016

2017

2018



The Department of Defense (DoD) contacts Carnegie Mellon University to develop a capability maturity model (CMM) to assess the quality and capability of their software contractors

Carnegie Mellon's Software Engineering Institute releases the first version of the software development capability maturity model

CMMI[®]

The CMM model expands into other areas such as Services, Acquisition, and People and becomes integrated, now called **Capability Maturity Model Integration (CMMI)**[®]

Carnegie Mellon University founds the **CMMI Institute** in order to extend the benefits of CMMI beyond software and systems engineering to **any product or service company** regardless of size or industry

CMMI Institute introduces the **Data Management Maturity (DMM)**SM model to help companies build, improve, and measure their enterprise data management function and staff

CMMI Institute is **acquired by ISACA**[®], a global non-profit association specializing in information technology. Both companies **share a vision** for advancing organizational performance across a spectrum of functions and industries.

CMMI Institute introduces the first cybersecurity maturity management platform to help organizations improve cyber resilience.

CMMI Institute collaborates with the US government to release two **healthcare initiatives** that improve patient safety.

CMMI Development V2.0 is released with key enhancements to meet the challenges of the changing global business landscape



Software Engineering Institute
Carnegie Mellon



CMMI[®] Institute



CMMI[®] Institute
AN ISACA ENTERPRISE





CMMI DEV



CMMI SVC



CMMI ACQ



PCMM



DMM

CMMI CYBERMATURITY



CMMIDEV



CMMISVC



CMMIACQ



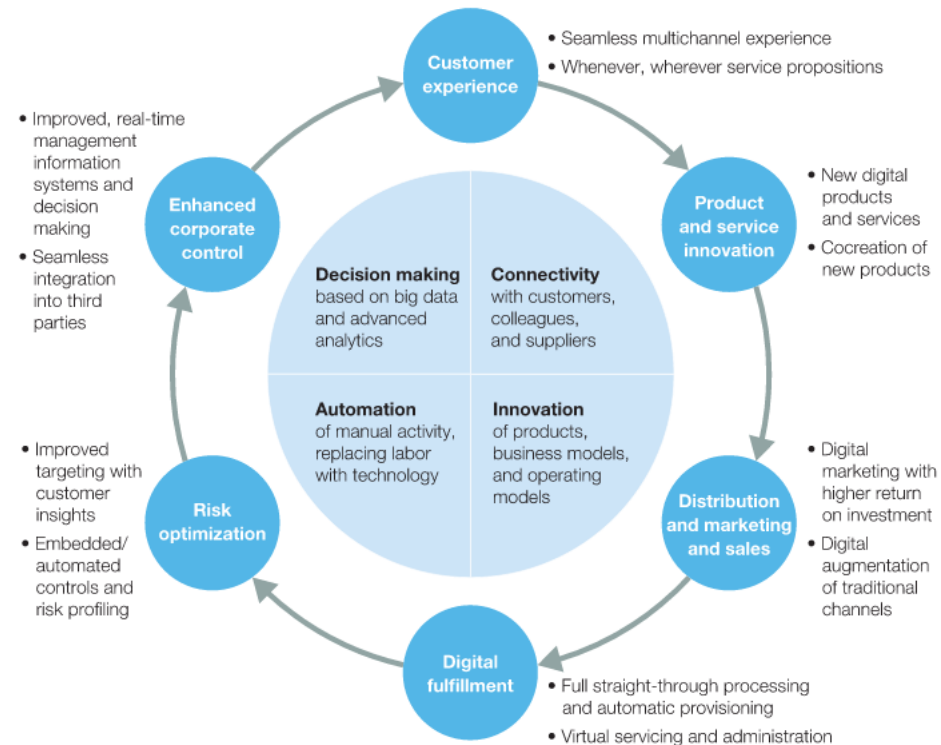
PCMM



DMM

CMMICYBERMATURITY

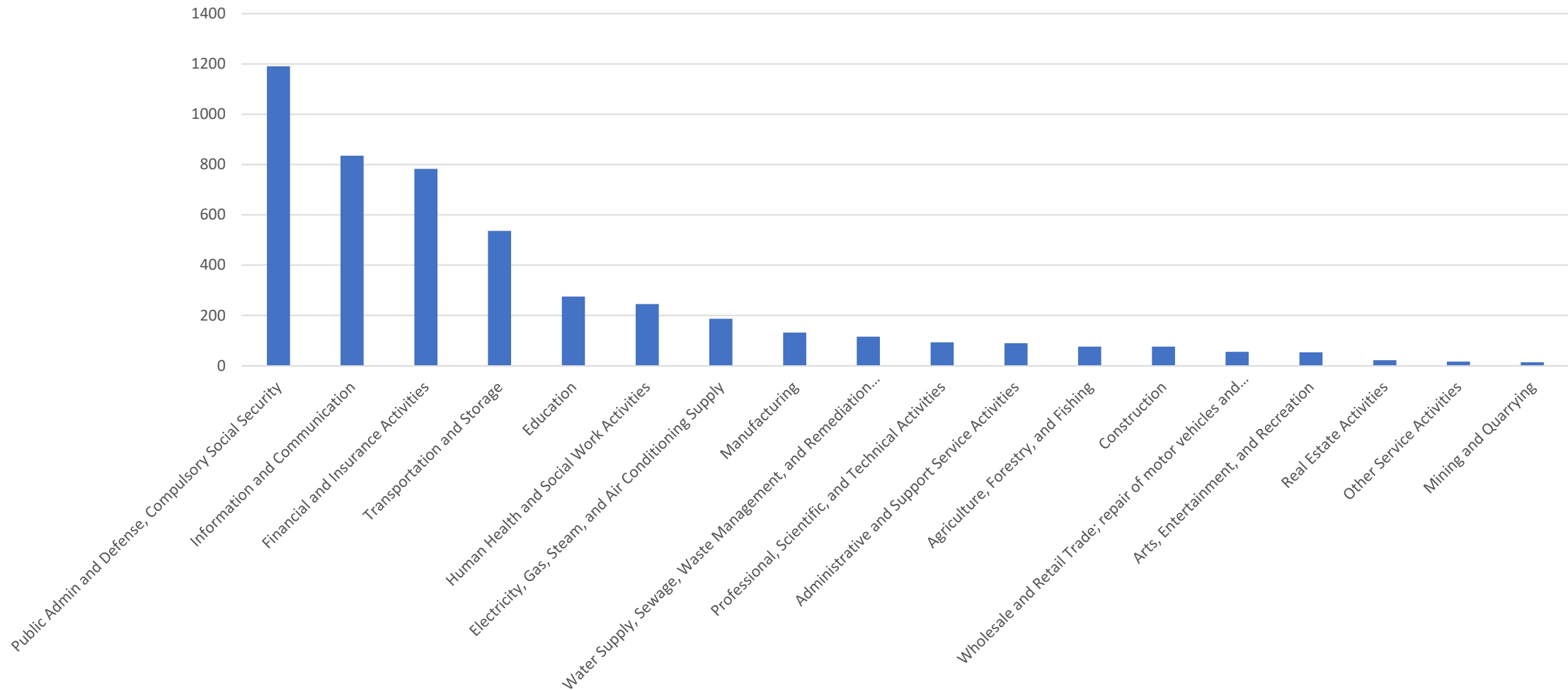
Digital can reshape every aspect of the modern enterprise.



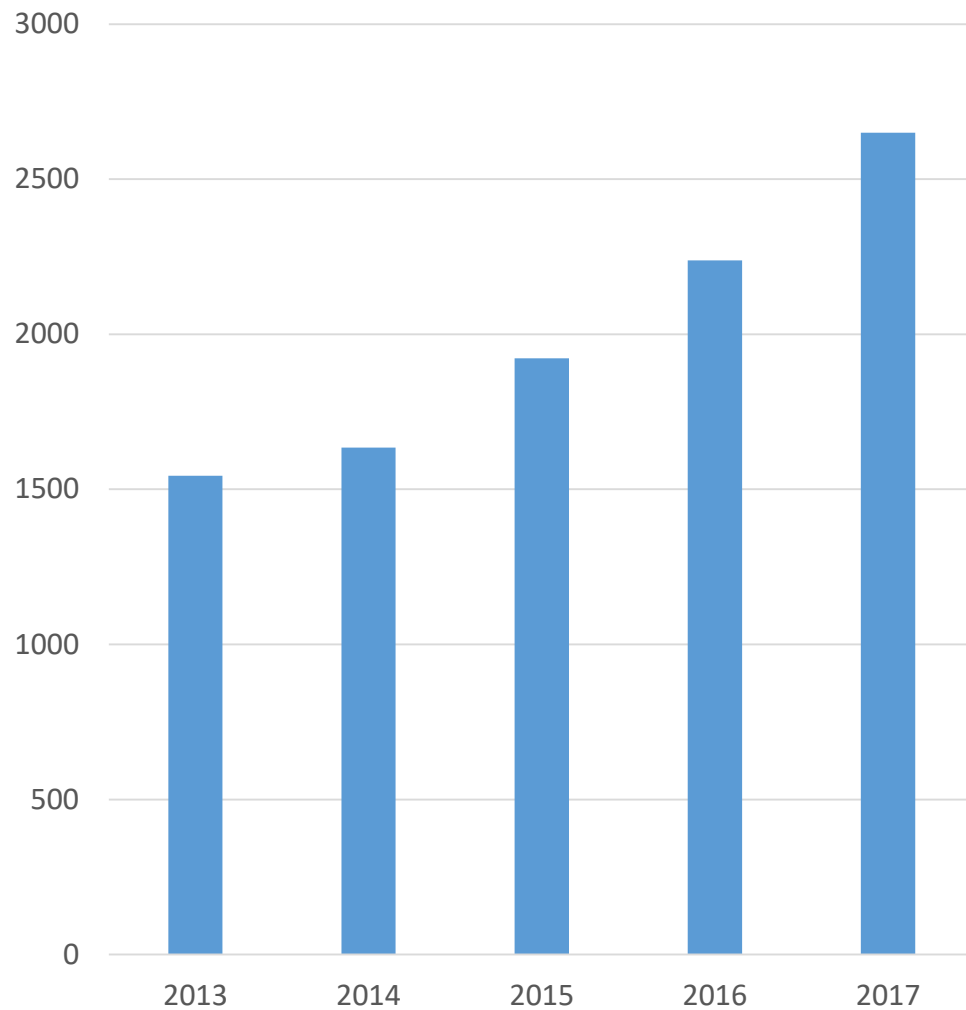
Source: Expert interviews; McKinsey analysis



Industry Mapping for 2016 and 2017



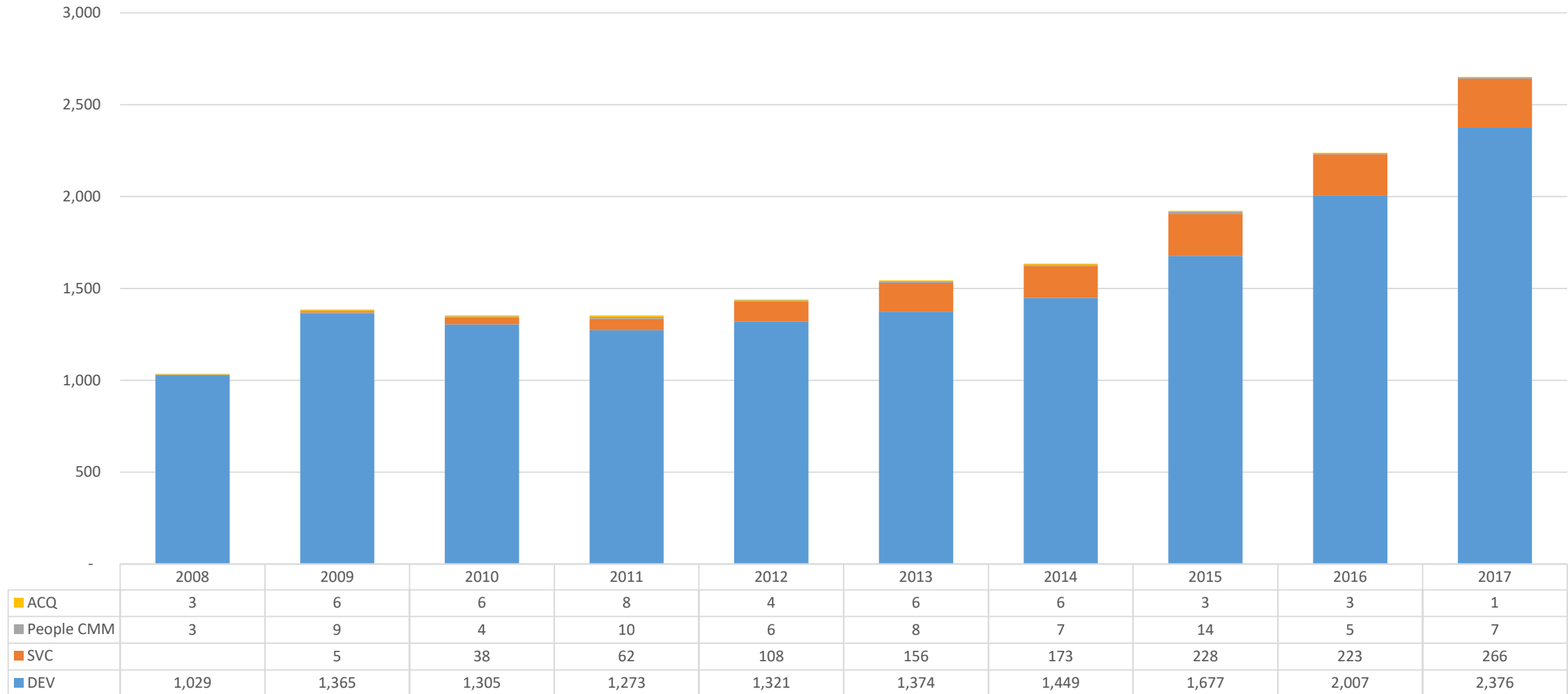
Appraisals



**18% Growth in
Adoption in 2017**



Appraisals by Constellation 2008–2017



80%



JALISCO

ES MÉXICO



Supporting Innovation
in Manufacturing
through

- CMMI- SVC
- Design Thinking
Training
- Technology
Consulting

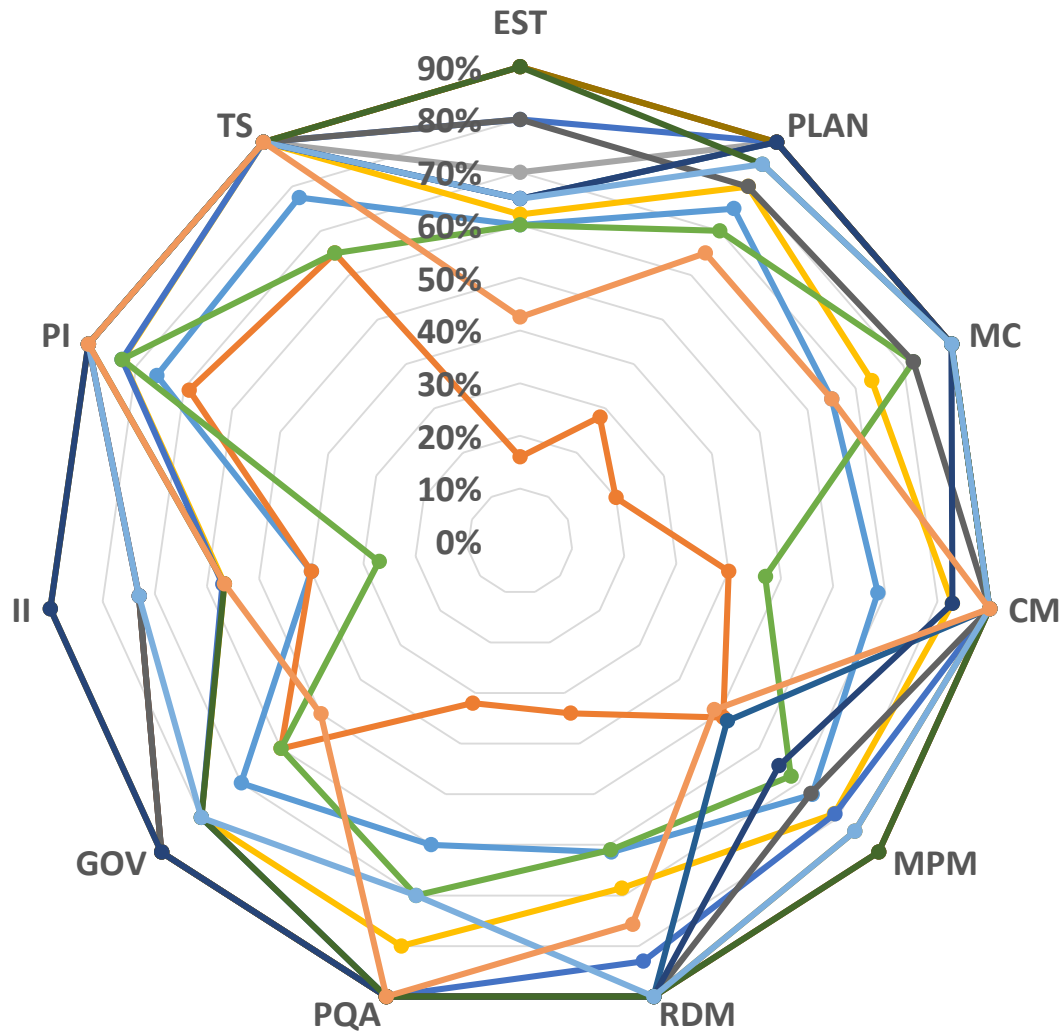






MDIC
MEDICAL DEVICE INNOVATION CONSORTIUM
ALIGN | ACHIEVE | ACCELERATE

What is FDA learning from the data?



Strengths

Strong emphasis on manufacturing and assembling product to address functionality and quality characteristics

Opportunities

Opportunity to improve how organizations ensure that the processes important to the organization are habitually and persistently improved

How are manufacturers perceiving the difference in the 2 processes?

Boston
Scientific

Mind-sets	
Discussion	
Interaction	
Time investment	

FDA inspection

- Only answer questions asked
- Do not discuss improvement opportunities or future plans
- Inspectors interrogate quality leaders, process experts, and record owners
- Inspectors look for evidence of noncompliance to regulations
- Large support team with backroom/ front room, streams, scribes, etc.
- **2-day inspection, 1,370 hours**

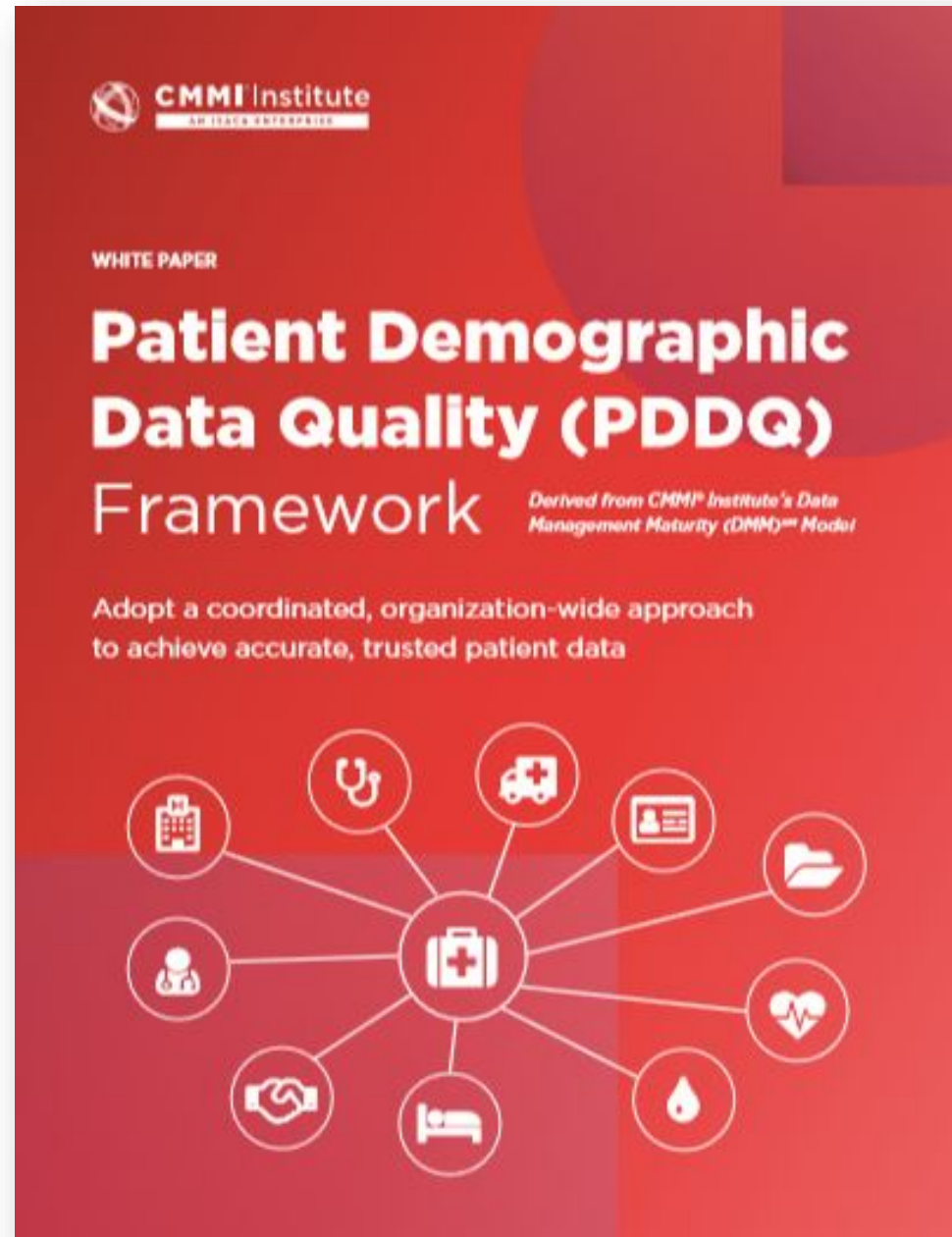


CMMI appraisal

- Be open in answering questions
- Weaknesses are opportunities to improve business processes
- Talk about improvements made over time and where we are going
- Appraisers conduct group interviews of “doers” responsible for work products
- Appraisers engage in discussions to truly understand how the business operates relative to best practices
- Minimal disruption to site resources and no need for backroom/front room
- **5-day appraisal, 340 hours**

Data Management Maturity Model

US Department
of Health and
Human Services



CMMI Cybermaturity Platform

	Risk Events										
	RE-1c	RE-1l	RE-1a	RE-2c	RE-2l	RE-2a	RE-5	RE-7	RE-6	RE-4	RE-3c
PV-1	VH	?	VL	?	VL	VL	H	-	L	-	-
PV-2	VH	?	VL	?	L	VL	L	-	H	-	-
PV-3	H	?	VL	?	L	VL	H	-	L	-	-
PV-4	VH	?	VL	?	L	VL	H	VL	H	-	-
PV-5	L	?	VL	?	VL	VL	L	-	H	-	-
PV-6	-	-	VL	-	-	VL	H	L	L	-	-
PV-7	VH	?	VL	?	L	VL	H	L	H	L	L
PV-8	VH	-	-	?	-	-	-	-	H	-	VL
PV-9	VH	?	VL	?	L	VL	L	-	H	-	-
PV-10	VH	?	VL	?	VL	VL	H	-	-	-	-
PV-11	VH	?	VL	?	L	VL	H	-	L	-	-
PV-12	VH	?	VL	?	VL	VL	H	VL	-	H	-
PV-13	-	-	VL	-	-	VL	H	L	H	-	-
PV-14	-	-	VL	-	-	VL	L	VL	-	-	-
PV-15	-	-	VL	-	-	VL	H	-	-	-	-
PV-6	-	-	VL	-	-	VL	H	L	L	-	-
PV-7	VH	?	VL	?	L	VL	H	L	H	L	L
PV-8	VH	-	-	?	-	-	-	-	H	-	VL
PV-9	VH	?	VL	?	L	VL	L	-	H	-	-
PV-10	VH	?	VL	?	VL	VL	H	-	-	-	-
PV-11	VH	?	VL	?	L	VL	H	-	-	-	-
PV-12	VH	?	VL	?	VL	VL	H	-	-	-	-
PV-13	VH	?	VL	?	L	VL	H	-	L	-	-

Identify and Manage Risks > Implement Risk Identification

Vulnerability and Threat Identification
Assessor: Kelly Hood | Due: April 17, 2018 | Submitted: February 7, 2018

Activity Audit: 26 Total Practices

<input checked="" type="checkbox"/>	<input type="checkbox"/>	The organization has identified potential physical vulnerabilities that might lead to known risks.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	The organization has identified potential logical vulnerabilities that might lead to known risks.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	The organization collaborates with relevant partners (e.g., facilities management, system operations personnel) to periodically catalog known vulnerabilities.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	A standard set of tools and/or methods is used to identify vulnerabilities.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Vulnerability identification draws from meaningful and sufficiently disparate sources of information.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Vulnerability identification sources are kept current.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Vulnerabilities are being actively discovered.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	There exists a recorded plan for performing vulnerability identification activities.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	A repository is used for recording information about vulnerabilities and their resolution.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Underlying causes for vulnerabilities are identified (e.g., through root-cause analysis).



Risk Questionnaire

RE-1c: How likely is it that Customer or Privacy Data is disclosed because of:

[PV-1] Internal breach due to inadequate network segmentation?
Very Low Low High **Very High**

[PV-2] Improperly tested and/or vulnerable web service or software application leads to malicious activity?
Very Low Low High **Very High**

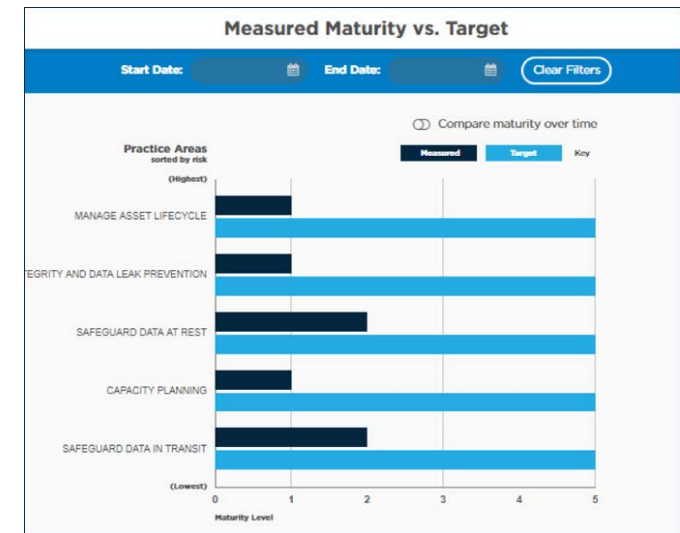
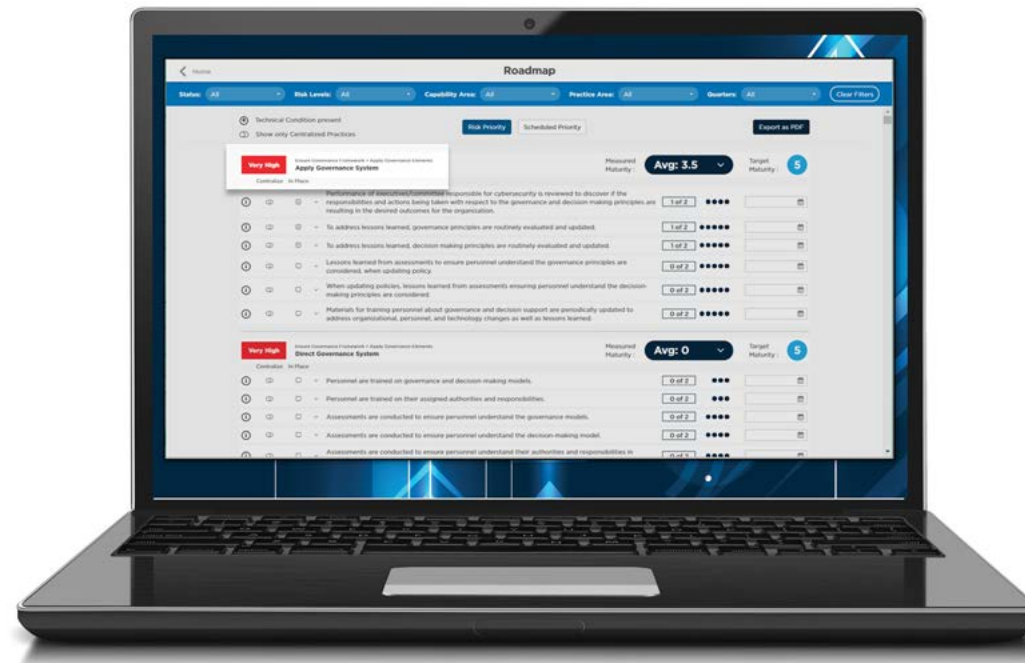
[PV-3] Attack through 3rd party partner?
Very Low Low High Very High

[PV-4] Staff fall victim to a social engineering attack?
Very Low Low High Very High

[PV-5] Unauthorized action occurs due to authentication issue?
Very Low Low High Very High

[PV-7] Poor practices due to lack of effective policy?
Very Low Low High **Very High**

[PV-8] Confidential data not destroyed properly?





CMMI[®] Institute

AN ISACA ENTERPRISE