Cyber-Supply Chain Risk Management

ISACA SAN DIEGO

July 21st, 2022

Mark Keelan - Director Compliance Practice

Agenda

- ISACA House Keeping
- Cyber Supply Chain Risk Management
  - Supply Chain State
  - NISTIR 8276
  - Government Response
  - Examples – Cyber Supply Chain Incident
  - Best Practices
  - Live Example
- Questions and Wrap Up

ISACA House Keeping

- Meeting is being recorded and will be shared on ISACA website
- CPE Certificate of Attendance
  - On-premises attendees: please make sure we checked you with the Eventbrite app
  - Online attendees: please make sure to complete the registration form we will share in the chat about half-way through the meeting, or you can self-submit your CPE (i.e. take screenshots to submit as proof of attendance)
- August Meeting: Andy Kim
  – Understanding CMMC 2.0
- Job Opportunities updated on the website
- Any community events, news, employment opportunities, etc. others would like to share in Chime or in-person

- If you have any questions and/or would like additional information, please email the chapter at isacasandiego@gmail.com or visit us online at https://isaca-sd.org

The World's Supply Chain is at RISK

Data Processing is one of the Top Risks!

A PERFECT STORM

1. Globalization
2. Economic Growth
3. Outsourcing

These trends have resulted in a world where organizations no longer fully control—and often do NOT HAVE FULL VISIBILITY into—the supply ecosystems of the products that they produce or the services that they deliver. And without sufficient control, organizations struggle to manage risks stemming from their supply chains and the products and services traversing them.

Source - NISTIR 8276

https://csrc.nist.gov/publications/detail/nistir/8276/final

Feb. 2021

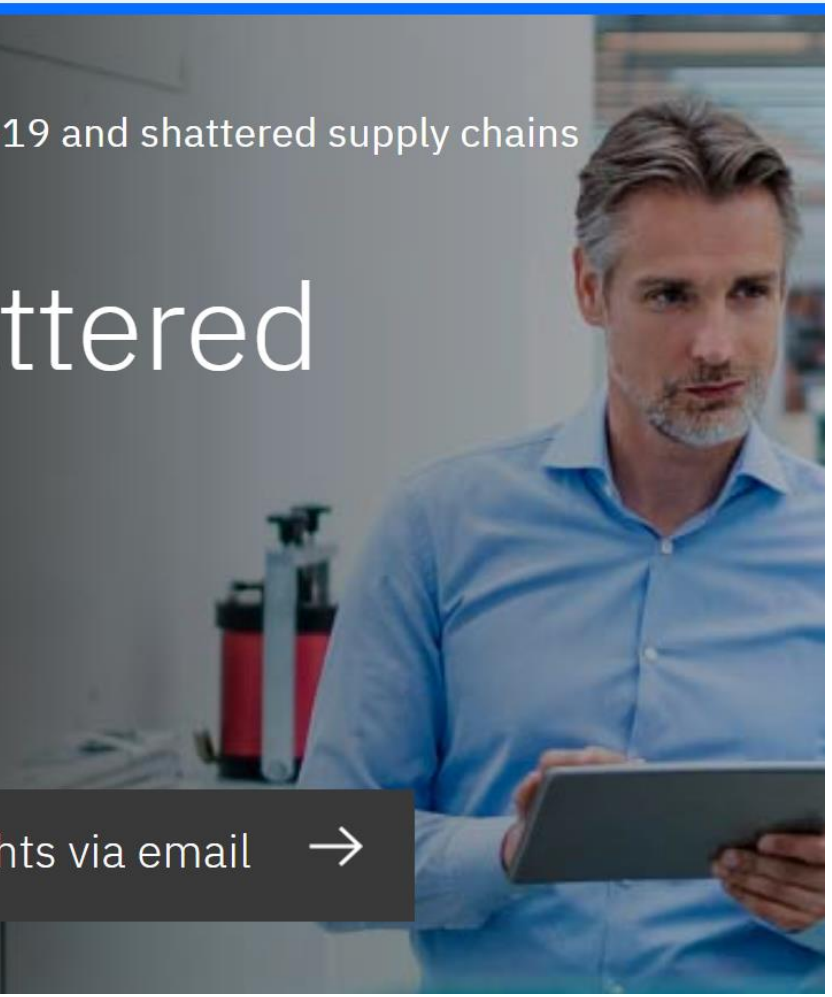
IBM

IBM Institute for Business

Our insights C-suite Study COVID-19

Home | Operations and Supply chain, COO | COVID-19 and shattered supply chains

COVID-19 and shattered supply chains



Download the report →

Get free insights via email →

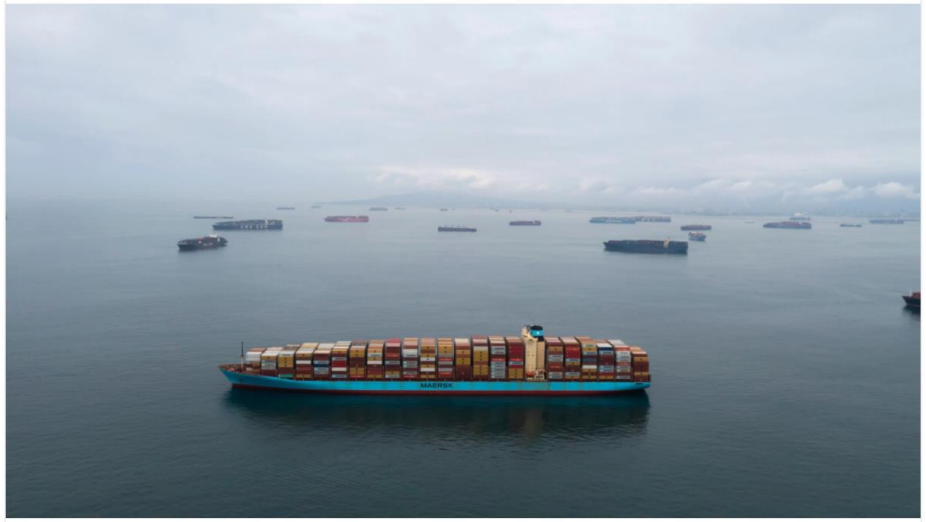
Record Number of Ships off CA Coast

Why a record number of container ships are backed up off the coast of California

With a dearth of places to anchor, some of the giant vessels are just drifting.

BY ERIK OLSEN | PUBLISHED SEP 16, 2021 2:00 PM

TECHNOLOGY



Mumbai Maersk at the Port of Tanjin Pelepas. Photo courtesy Maersk

2021 Container Rates Surge 333% From One Year Ago

Bloomberg

Total Views: 5206

July 8, 2021

Shipping Rates are off the Charts!

BREAKING Stocks extend losses as Russia-Ukraine tensions weigh on markets, Dow drops nearly 500 points

CNBC MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV WATCHLIST CRAMER PRO

TRANSPORTATION

Container shipping rates between U.S. and China exceed $20,000, hitting a record

PUBLISHED THU, AUG 5 2021•8:34 AM EDT | UPDATED THU, AUG 5 2021•8:35 AM EDT

REUTERS

SHARE

KEY POINTS

- Container shipping rates from China to the United States have scaled fresh highs above $20,000 per 40-foot box.

CNBC TV

Squawk on the Street WATCH LIVE

UP NEXT | TechCheck 11:00 AM ET Listen

China – US Transit Times Coming Down

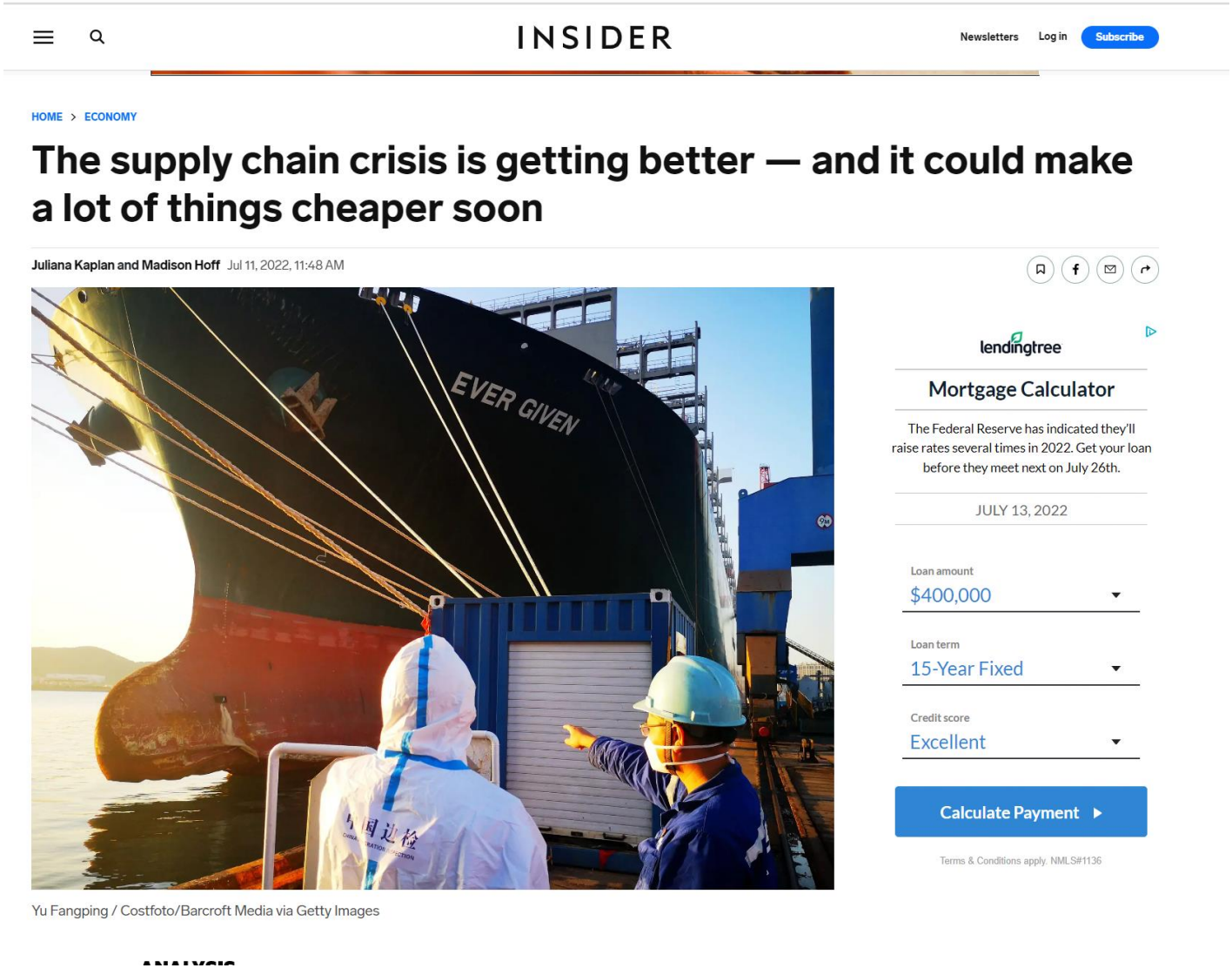
China – US Rates Coming Down

Asia – N. America West Coast **rates fell more than 30% in May** to $10,762/FEU and East Coast prices **fell 20% to $13,796/FEU**.

Both remain more than 35% higher than a year ago, but have returned to levels not seen since last summer.

Likewise, conditions at LA/Long Beach ports have improved over the last two months.

Supply Chain Improving



INSIDER

Newsletters Log in Subscribe

HOME > ECONOMY

The supply chain crisis is getting better — and it could make a lot of things cheaper soon

Juliana Kaplan and Madison Hoff Jul 11, 2022, 11:48 AM

Yu Fangping / Costfoto/Barcroft Media via Getty Images

flexport.

Back in October, it took more than 110 days for goods to make their way from Asia to the U.S. That has now fallen to 95 days. While 15 days may not seem that dramatic, it's a rate not seen since mid-2021.

https://www.businessinsider.com/supply-chain-crisis-over-prices-inflation-go-down-2022-7

How Big is the Problem?

Transportation & Logistics › Water Transport

Container shipping - statistics & facts

Published by Martin Placek,Sep 23, 2021

Maritime shipping is the backbone of world trade; it is estimated that some 80 percent of all goods are carried by sea. In terms of value, global maritime container trade is estimated to account for around 60 percent of all seaborne trade, which was valued at around 14 trillion U.S. dollars in 2019. While the number of goods carried by containers increased from around 102 million metric tons in 1980 to about 1.83 billion metric tons in 2017, vessels have likewise increased their capacity. Between 1980 and 2020, the deadweight tonnage of container ships has grown from about 11 million metric tons to around 275 million metric tons. With a total capacity of over four million TEUs*, Danish shipping line APM-Maersk is currently the largest container-shipping company globally, followed by MSC, COSCO, CMA CGM, and Hapag-Lloyd.

abc NEWS VIDEO LIVE SHOWS CORONAVIRUS JAN. 6 RIOT OLYMPICS

DHS warns of Russian cyberattack on US if it responds to Ukraine invasion

It comes as tensions are running high in the region.

By Luke Barr and Josh Margolin
January 24, 2022, 9:41 AM • 4 min read

Russia, DHS said, has a "range of offensive cyber tools that it could employ against US networks," and the attacks could range from a low level denial of service attack, to "destructive" attacks targeting critical infrastructure.

DHS says Russia "continues to target" and gain access to critical infrastructure in the United States, but Russia does not limit itself to conducting cyber operations just in the U.S.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Identifying Critical Infrastructure During COVID-19
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Sector-Specific Agencies
- Transportation Systems Sector
- Water and Wastewater Systems Sector

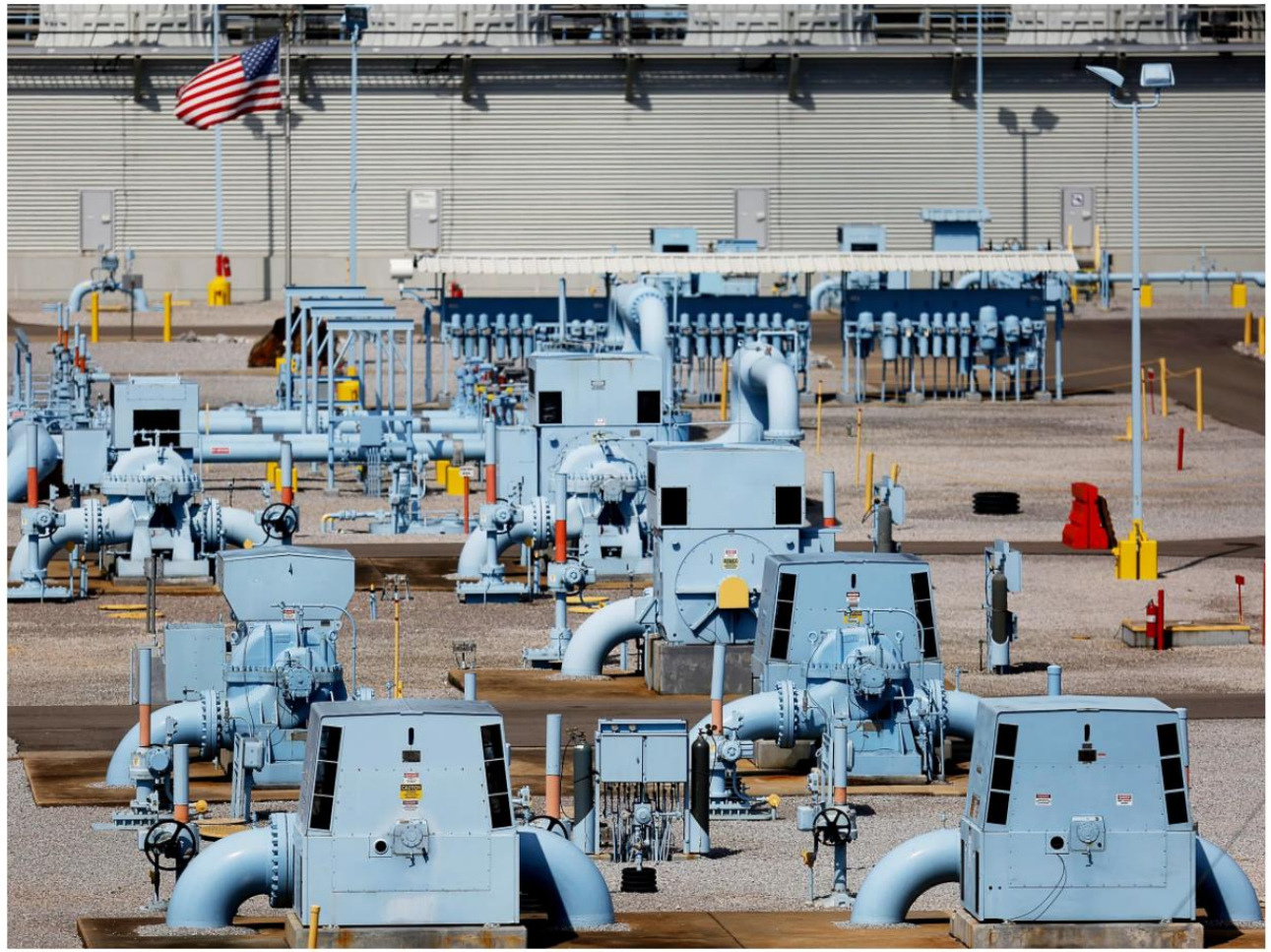
https://www.cisa.gov/

U ▪
S T

ANDY GREENBERG SECURITY 05.08.2021 05:33 PM

The Colonial Pipeline Hack Is a New Extreme for Ransomware

An attack has crippled the company's operations—and cut off a large portion of the East Coast's fuel supply—in an ominous development for critical infrastructure.



Colonial Pipeline supplies nearly half of the East Coast's fuel—until a ransomware attack took it offline. PHOTOGRAPH: LUKE SHARRETT/BLOOMBERG/GETTY IMAGES

Other Large Public Examples:

JBS USA paid an $11 million ransom in response to a cyberattack that led to the shutdown of its entire US beef processing operation.

NotPetya:
World's First $10 Billion Malware in 2017

Target Retailer
Attack came from HVAC provider
2014

RAND CORPORATION

OBJECTIVE ANALYSIS. EFFECTIVE SOLUTIONS.

The intersection of cyberattacks and supply chains creates a wicked new form of risk—and the stakes are as much about national security as they are economics.

Share on Twitter

Jonathan W. Welburn
@jwwelburn

Operations Researcher; Professor, Pardee RAND Graduate School

Ph.D. in decision science & operations research, University of Wisconsin

Biden Administration Executive Order

THE WHITE HOUSE

BRIEFING ROOM

Executive Order on America's Supply Chains

FEBRUARY 24, 2021 • PRESIDENTIAL ACTIONS

NISTIR 8276

Key Practices in Cyber Supply Chain Risk Management:

Observations from Industry

Jon Boyens
Celia Paulsen
Computer Security Division
Information Technology Laboratory

https://csrc.nist.gov/publications/detail/nistir/8276/final

Feb. 2021

Key Practices for C-SCRM

- 1. Integrate C-SCRM Across the Organization
- 2. Establish a Formal C-SCRM Program
- 3. Know and Manage Critical Suppliers
- 4. Understand the Organization’s Supply Chain
- 5. Closely Collaborate with Key Suppliers
- 6. Include Key Suppliers in Resilience and Improvement Activities
- 7. Assess and Monitor Throughout the Supplier Relationship
- 8. Plan for the Full Life Cycle

Appendix C—Recommendations Mapped to Key Government and Industry Resources

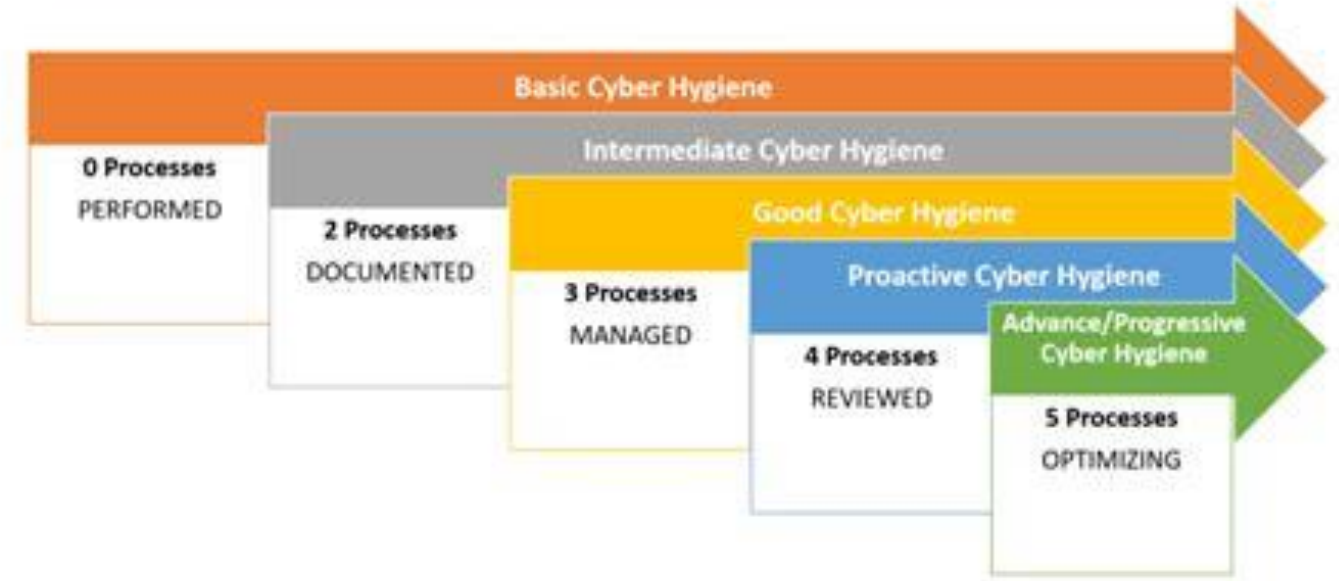
	NIST SP 800-161	NISTIR 7622	2015 Case studies	2019 Case studies	CSF	FSP	UTC	ISO/IEC 27002	ISO/IEC 27036	ISO/IEC 20243
Establish supply chain risk councils that include executives from across the organization (e.g., cyber, product security, procurement, ERM, business units, etc.)	✓		✓	✓	✓	✓				
Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security functions			✓	✓		✓				✓
Increase board involvement in C-SCRM through regular risk discussions and sharing of measures of performance			✓	✓		✓				
Integrate cybersecurity considerations into system and product life cycles	✓	✓	✓	✓	✓	✓		✓	✓	✓
Clearly define roles and responsibilities for security aspects of specific	✓		✓	✓		✓	✓	✓	✓	✓

2 Key Requirements for Simplifying Cyber Supply Chain Risk Management

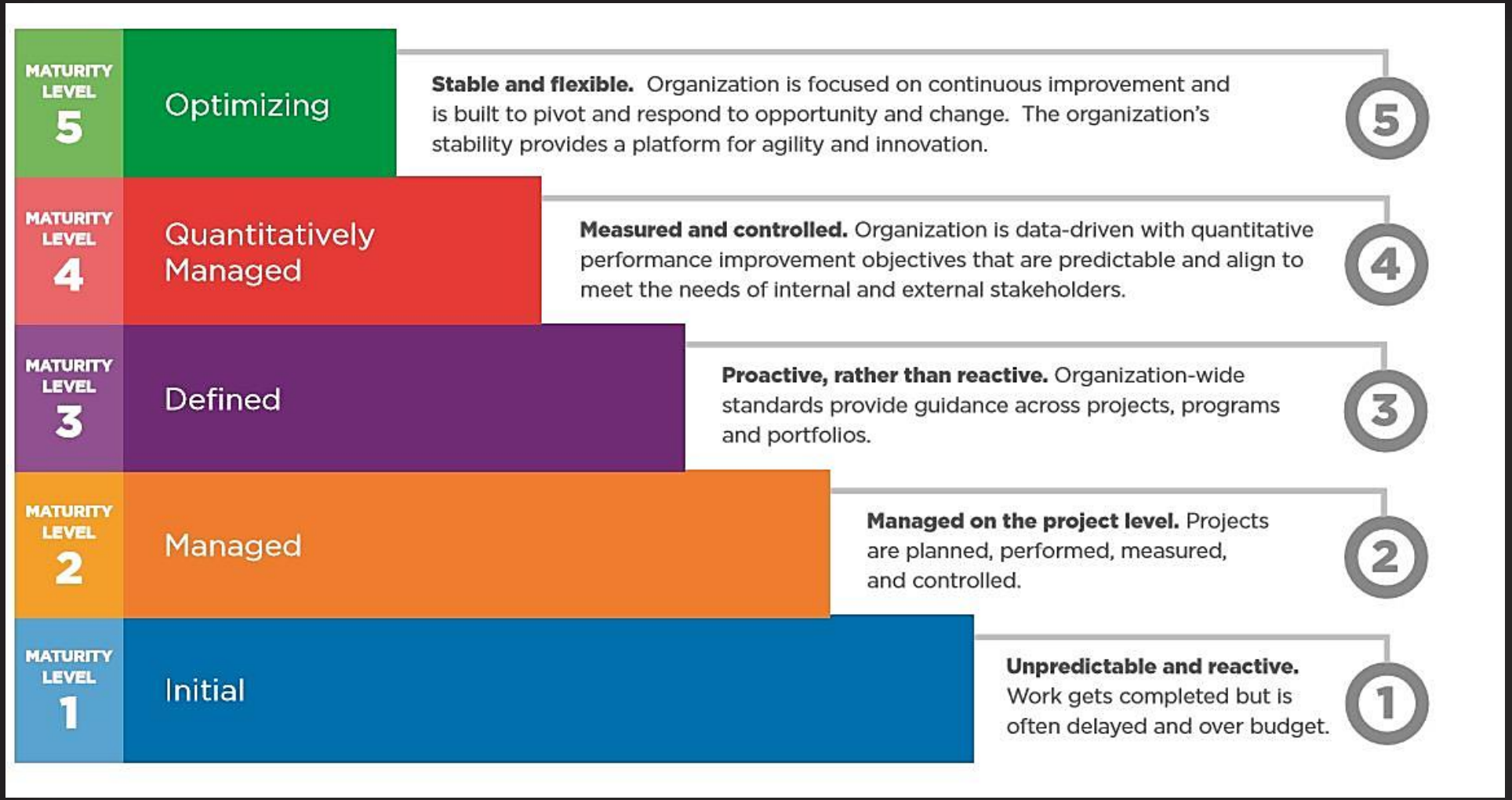
- **MEASURABLE & ACTIONABLE**
- Designed for Ease of Use
- Deployable
  - Anywhere
  - Anyone
- Uses Industry Standards Only
  - NIST Cybersecurity Framework
  - CMMI

CMMC – 3rd Party Cyber Risk Assessment

CMMC v1 - Levels

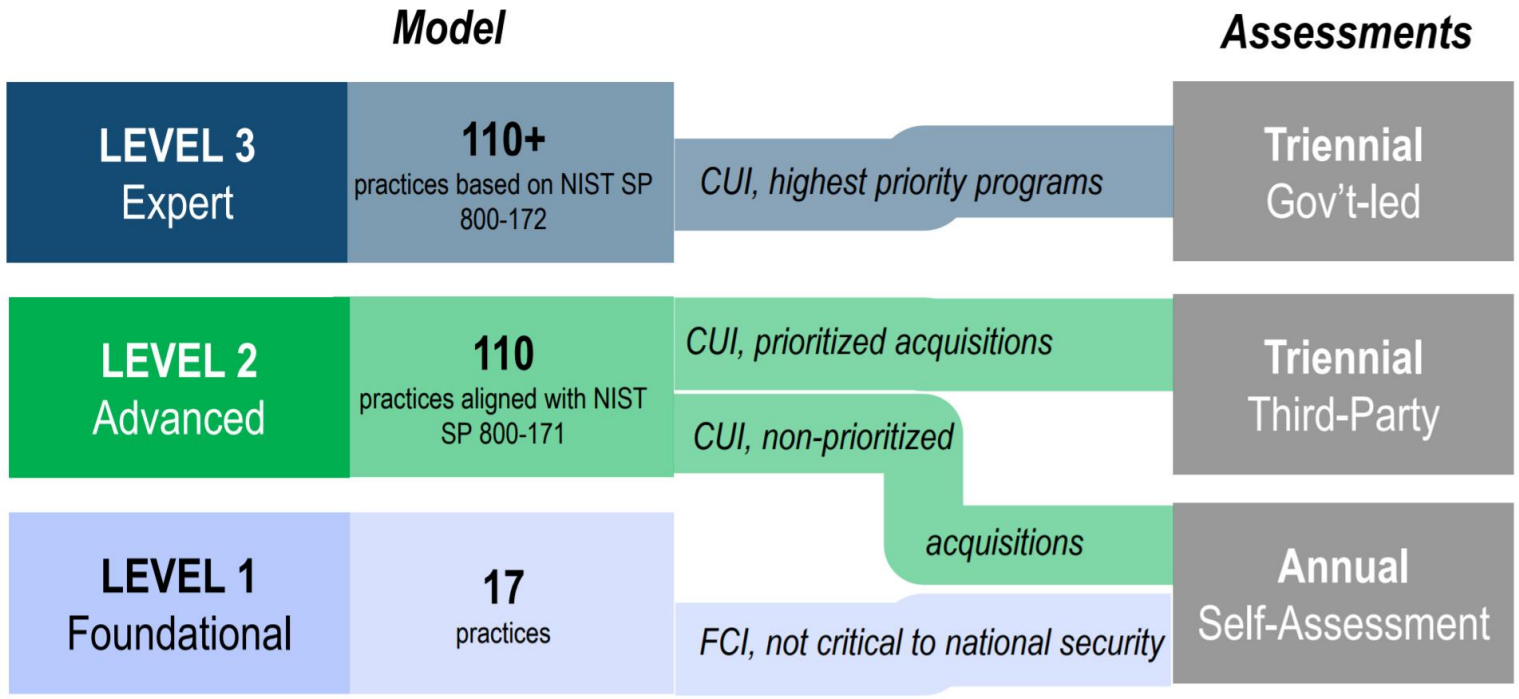


Capability Maturity Model - “Quantitative”



CMMC – 3rd Party Cyber Risk Assessment

CMMC v2 - Levels



https://www.acq.osd.mil/cmmc/docs/CMMC-2.0-Overview-2021-12-03.pdf

NIST Cybersecurity Framework – "Qualitative"

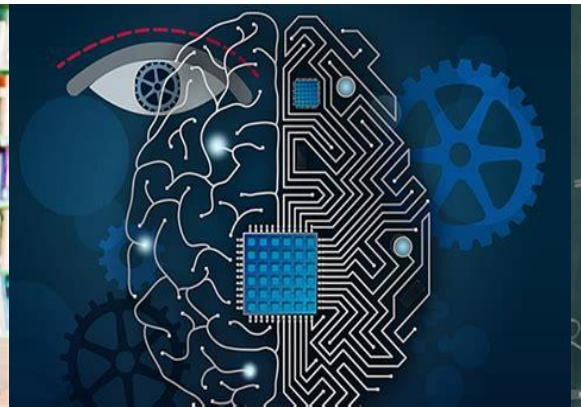
Function	Category	Subcategory	Informative References
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9

NIST CSF Framework

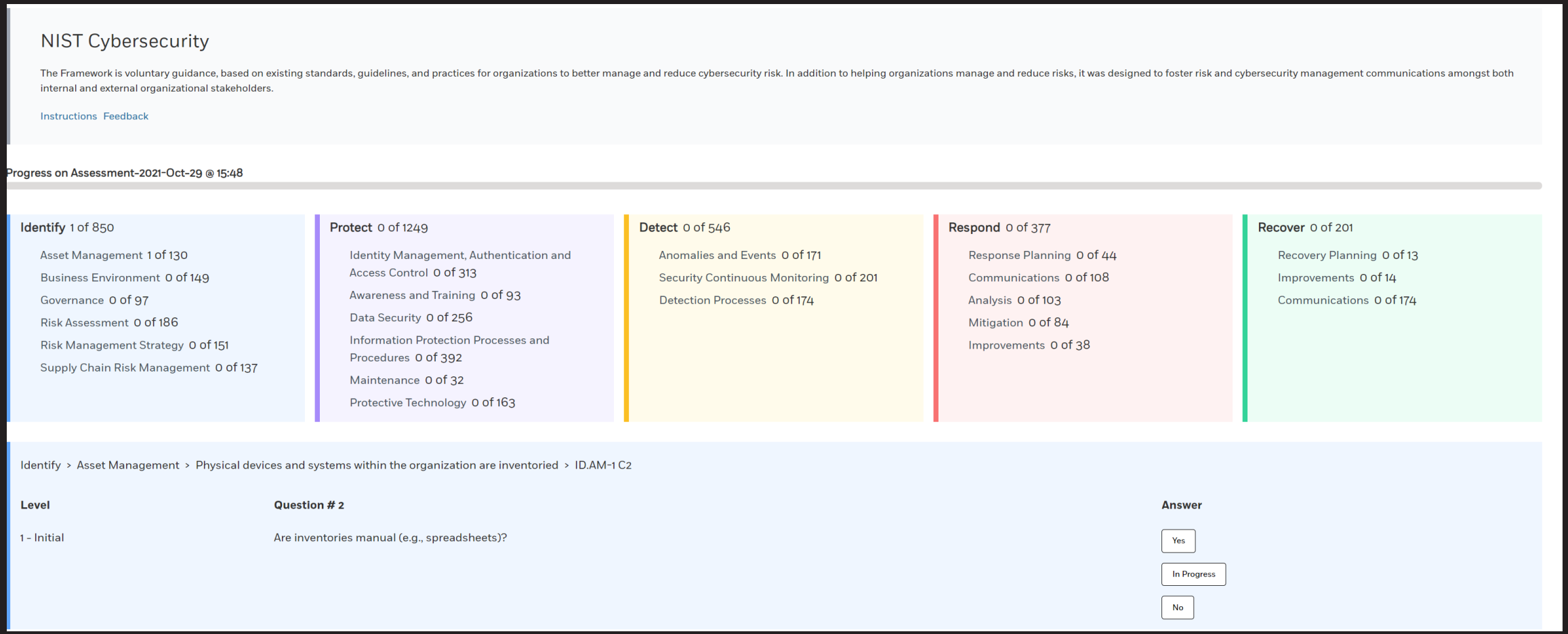
- Qualitative – NIST CSF
- Risk Focused
- Described in words
- Results
  - Narrative
  - Relative

CMMI

- Quantitative - CMMI
- Value Focused
- Described in numbers
- Results
  - Numeric Score
  - Normalized

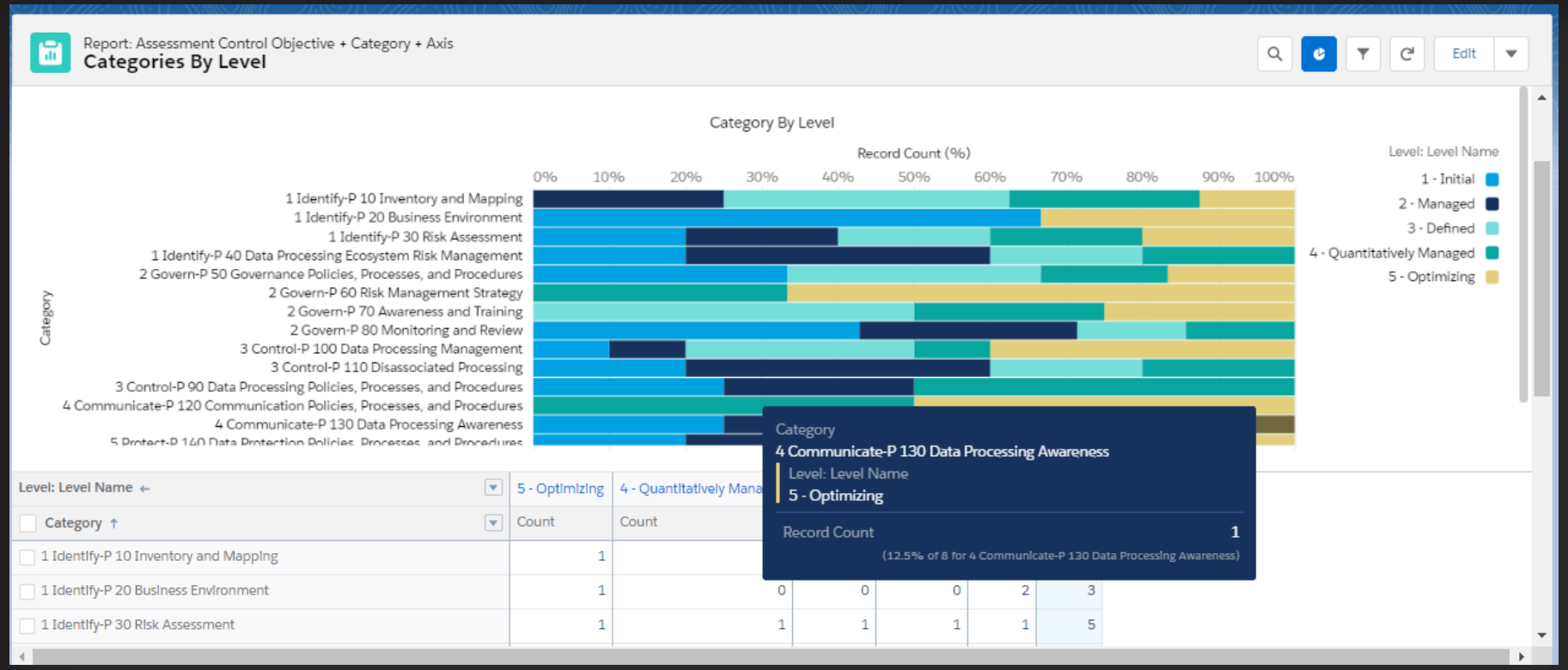


Clean & Straight Forward Cybersecurity Assessment



Assessment: Measurement & Reporting

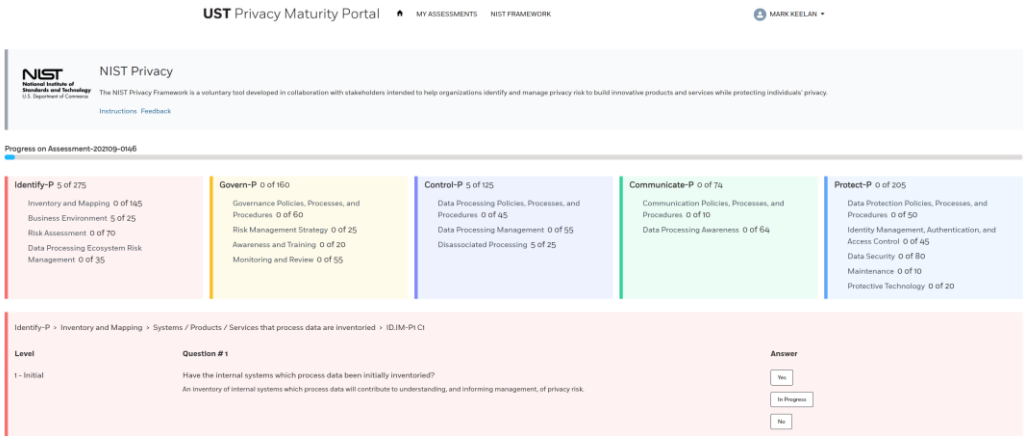
Interactive reports are available



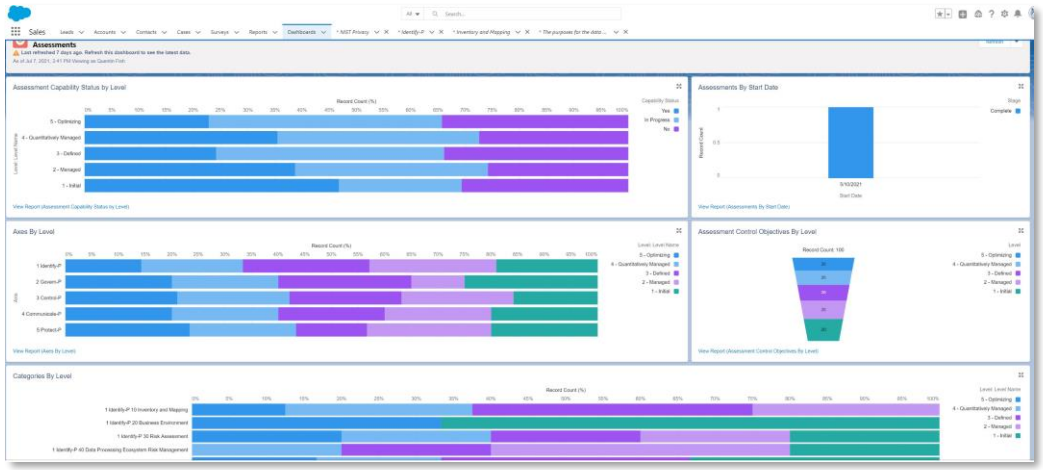
CMMI Not Limited to NIST C-SCRM Assessments

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

Guided on-line maturity assessments make it easy to survey your organization



Quantitative measurement of privacy value supports ROI for Investment in Privacy



HOME ASSESSMENTS QF.SCRATCH

Privacy and Cybersecurity Assessments

Welcome to the future of privacy and cybersecurity assessments. While individual certifications are important, the world of privacy and cybersecurity 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 or CyberSecurity Framework with the Capability Maturity Model Integration (CMMI).

NIST National Institute of Standards and Technology U.S. Department of Commerce

New NIST Privacy Assessment

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.

GDPR

New NIST Cybersecurity Assessment

The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

PIPEDA

New PIPEDA v2019.6 Assessment

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal privacy law for private-sector organizations in Canada. The purpose of the law is to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

ISO

New ISO27001 Assessment

ISO/IEC 27001, is an Information security management standard jointly published by the International Organization for Standardisation, and the International Electrotechnical Commission.

Assessments

Click the Assessment Name link to continue an Assessment or view the results.

3rd Party vs Internal Assessments

MOST COST-EFFICIENT PATH TO MINIMIZE CYBER RISK ACROSS YOUR SUPPLY CHAIN

Supplier Community Portal

MAKES IT EASY TO ASSESS YOUR SUPPLY CHAIN RISK ACROSS COMPLEX GLOBAL SUPPLY CHAINS

- Dedicated Supplier Community Cloud Environment
  - Client Branded
  - Multi-Brand / Multi-Region
  - Single Tenant
  - Customizable
  - Upgradable
- Automated Supplier On Boarding
  - Supplier receives e-mail with link to join community
  - Multi-brand e-mail templates
  - Self-registers on the portal
  - Establishes Secure Channel of Communication with the Supplier
- Supplier Risk Assessment Portal
  - Allows user to easily complete cybersecurity assessments
  - Supports multi-users per Supplier to answer 1 assessment
  - Supports synch of common answers across multiple frameworks

U ▪ S T

Supplier Community Management

GET YOUR SUPPLIERS TO PAY FOR COST OF COMPLIANCE

Supplier On-Boarding

Compliance Campaign Events

Supplier Funded Compliance

Creative Program Funding

Let Your Suppliers Pay For Compliance?

- Customer Funded Model
- Supplier Funded Model
  - Have your supplier network fund your assessment program
  - Have suppliers sign up for the network

Objectives & Outcomes

LIFECYLE OF CONTINUOUS IMPROVEMENT

OBJECTIVES

OUTCOMES

Why Does this Matter?

- Shutdown your company
  - Indirectly – by disrupting your supply chain
  - Directly – using you supply chain as an attack vector
- You need to Report Readiness
  - Executive Management – Business Risk
  - 10K – Shareholders if you are public
- Lost Growth and Customers
- National Security
  - Scary Scenarios
    - Loss of Food on Shelves
    - Disable water and power
    - No Gas for your car
    - Cripple National Defense

NIST Cybersecurity Supplier Chain Risk Assessment

Contacts at UST

Mark Keelan
mark.keelan@ust.com
Director – Compliance Practice

Austin Gould
austin.gould@ust.com
Marketing


-Question-

Copyright and confidentiality notice

UST
5 Polaris Way
Aliso Viejo, CA 92656

T +1 949 716 8757
F +1 949 716 8396

ust.com