Data Privacy: A Look at the NIST Privacy Framework 1.0

Webinar: January 27, 2021

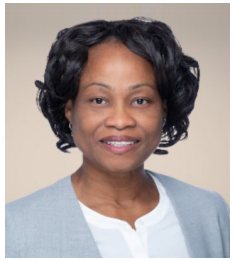
Mirena Taskova with special guests from NIST & Hyperproof

armanino

What you will learn today

- How to implement a successful global annual privacy strategy by using NIST privacy framework, privacy expertise and technology
- What is NIST and how it can be used for global privacy compliance
- How technology can help you with your privacy efforts

Panel



Pippa Akem
Senior Manager, Data Privacy
Armanino LLP
Pippa.Akem@armaninoLLP.com

Dean Quiambao
Chief Relationship Builder
Armanino LLP
DeanQ@amllp.com

Dylan Gilbert
Privacy Policy Advisor
National Institute of Standards and Technology (NIST)
dylan.gilbert@nist.gov

Mirena Taskova
Managing Director, Head of Privacy and Cybersecurity
Armanino LLP
Mirena.Taskova@armaninoLLP.com

Aidan Collins
Head of Enterprise Business
Hyperproof
aidan@hyperproof.io

armanino

2020 privacy highlights & welcome 2021

armanino

2020 privacy highlights

Welcome to California!

- **The CCPA** (California Consumer Privacy Act of 2018)
  - CCPA main developments
  - AG Regulations
  - AG Enforcement Action
  - CCPA private right of action trend
- **Hello CPRA!** (California Privacy Rights Act)
  - Key changes introduced by the CPRA to the CCPA
  - What comes next?
  - Be prepared!

Over to Europe

- **The Schrems II Decision**
  - Death of the EU-US Privacy Shield
  - Rise of Standard Contractual Clauses (SCCs)?
- **Global trends in Privacy**
  - Brazil (LGPD)
  - China (PIPL, CSL)
  - Canada (DCIA, CPPA)
  - India (PDPB)
  - New Zealand (NZ Privacy Act)
  - US federal privacy legislation & other state legislation (WA, PA, IL, MA, NY, NJ)
- **Privacy in the wake of a Pandemic**
  - Impact of Covid-19 on data transfer

armanino

Welcome 2021: global privacy trends

What should be on your radar in 2021?

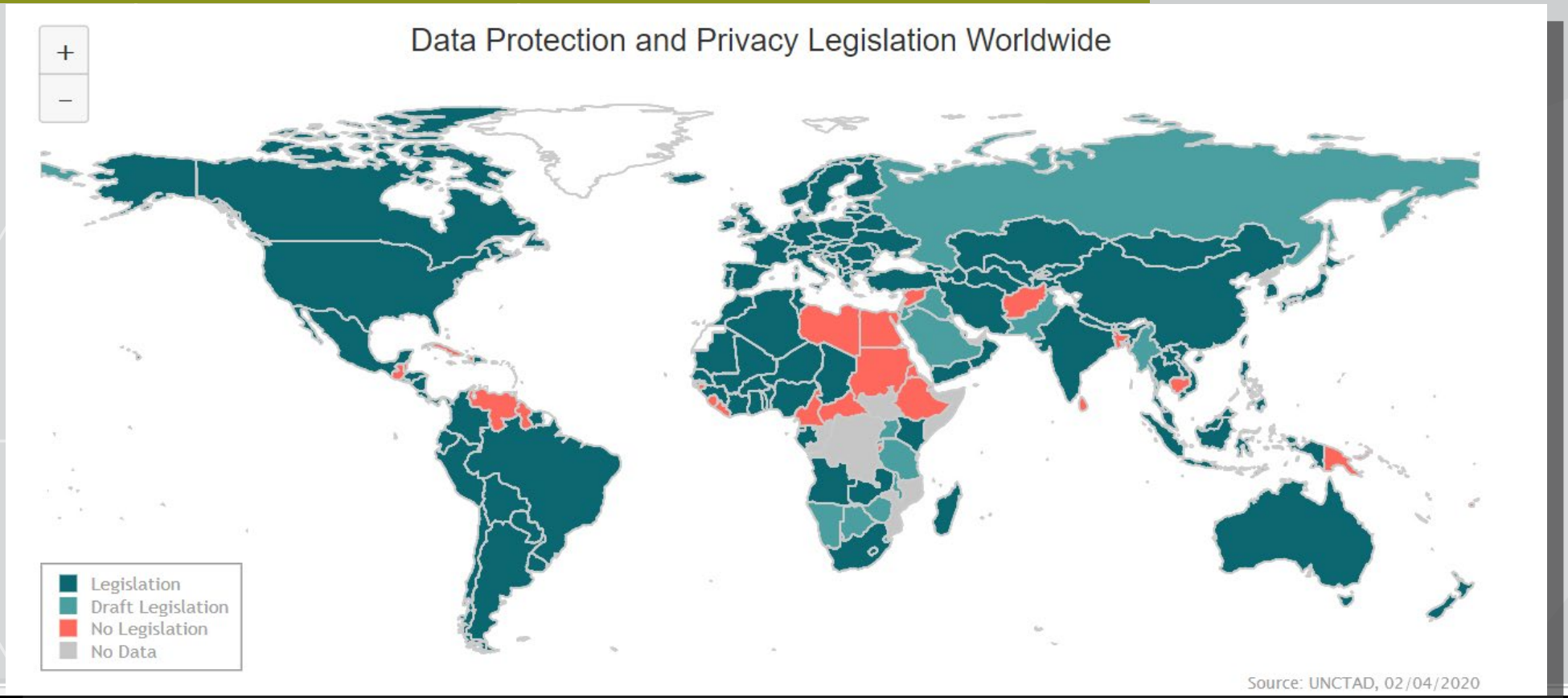
- **Brexit**
  - No, GDPR won't change
  - However, there are consequences (e.g., the data flow between the UK and the EU)
  - The UK will be, and should be treated as a separate entity from the EU
- **ePrivacy Directive**
  - Directive was meant to come into force around the same time as the GDPR
  - Multiple delays caused by EU members' inability to agree on the final text, now the pandemic
- **EDPB guidance & SCCs**
  - Part 1: Recommendations
  - Part 2: SCCs (DPA under Art 28 of the GDPR)
- **EDPB guidance & SCCs**
  - Part 1: Recommendations
  - Part 2: Data transfers SCCs (use both by controllers and processors as data exporters)
- **Cybersecurity** (No end to attacks, SI being accessed /NCID)
- **DSA and DMA** (Digital Service Act & Digital Markets Act)

armanino

QUESTIONS AND ANSWERS

armanino

How to ensure global privacy compliance?



armanino

NIST privacy framework

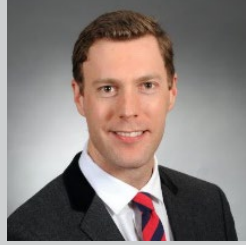
armanino

Privacy Framework Structure

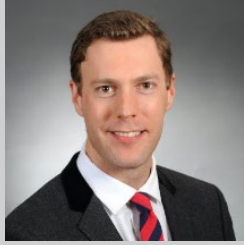
The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk

Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that the organization has prioritized to help it manage privacy risk

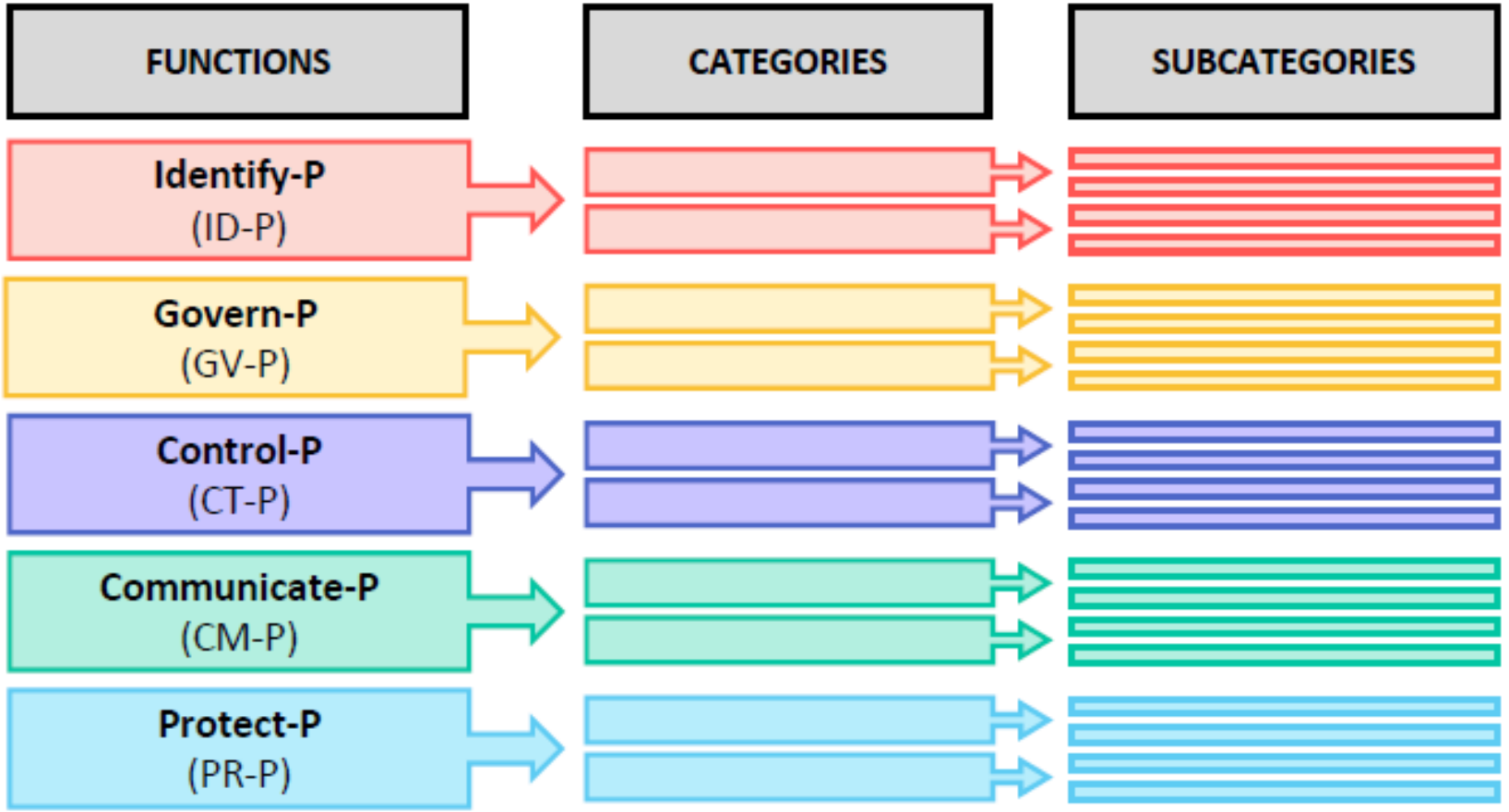
Implementation Tiers help an organization communicate about whether it has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile



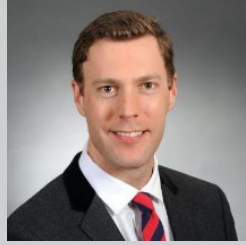
armanino



Privacy Framework Core



armanino



How to Use the Privacy Framework

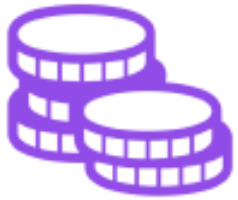
Informative References

Strengthening Accountability

Establishing or Improving a Privacy Program

Applying to the System Development Life Cycle

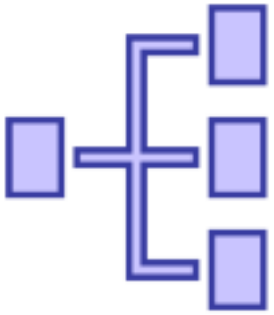
Using within the Data Processing Ecosystem



Informing Buying Decisions

armanino

Resource Repository

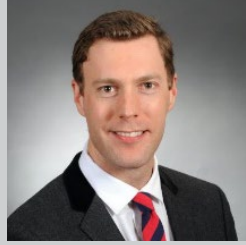


Crosswalks

- GDPR
- CCPA
- ISO/IEC 27701
- IAPP CIPM

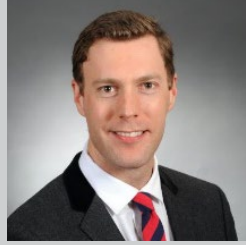
Guidelines & Tools

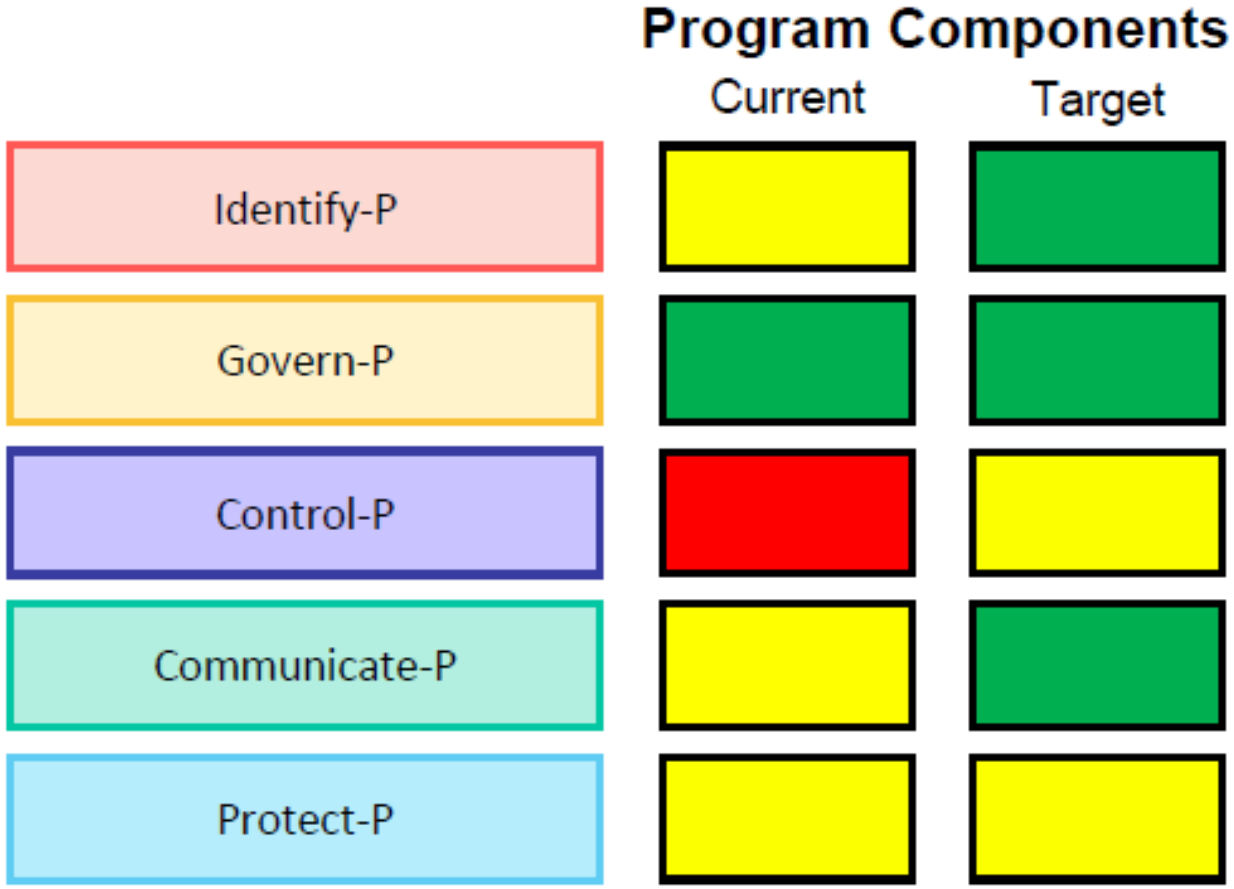
- NIST controls catalog
- NIST Privacy Risk Assessment Methodology
- LINDDUN privacy threat modeling framework
- IBM AI minimization toolkit



armanino

Communication and Advocacy with Leadership Example

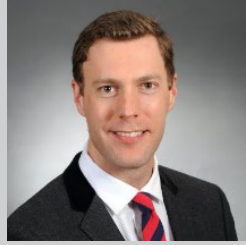




armanino

What value does the NIST privacy framework bring?

armanino



Value Proposition

Privacy Framework supports:

Building customer trust

Fulfilling current compliance obligations

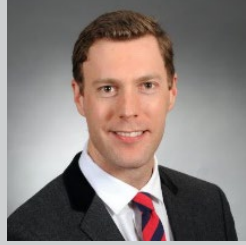
Facilitating communication

How to ensure efficient global privacy strategy?

armanino

How to perform NIST risk assessment?

armanino



Privacy Risk and Organizational Risk

Problem

arises from data processing

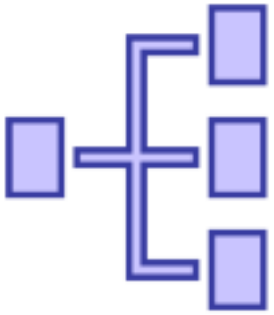
Individual

experiences direct impact
(e.g., embarrassment, discrimination, economic loss)

Organization

resulting impact
(e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)

Resource Repository

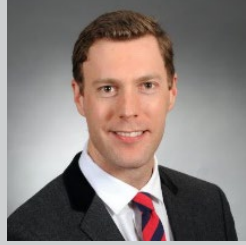


Crosswalks

- GDPR
- CCPA
- ISO/IEC 27701
- IAPP CIPM

Guidelines & Tools

- NIST controls catalog
- NIST Privacy Risk Assessment Methodology
- LINDDUN privacy threat modeling framework
- IBM AI minimization toolkit



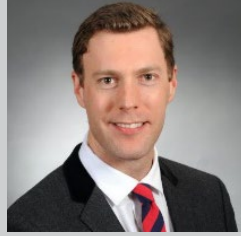
armanino

How to ensure uniform privacy & cybersecurity compliance?

armanino

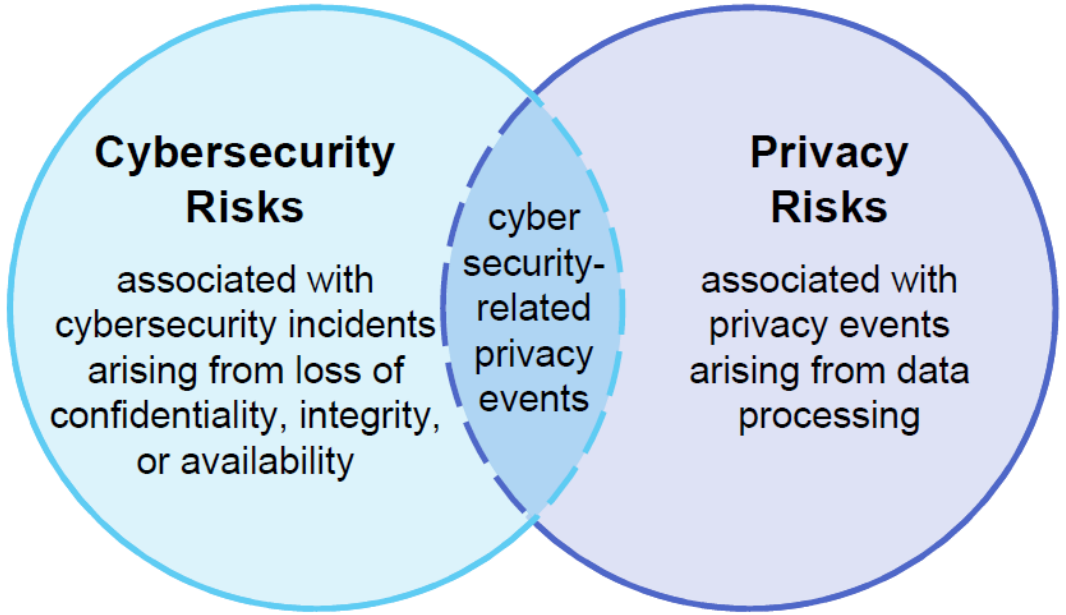
How does NIST assist with providing uniform privacy & cybersecurity approach?

armanino



NIST perspective

Relationship Between Cybersecurity and Privacy Risk



Data: A representation of information, including digital and non-digital formats

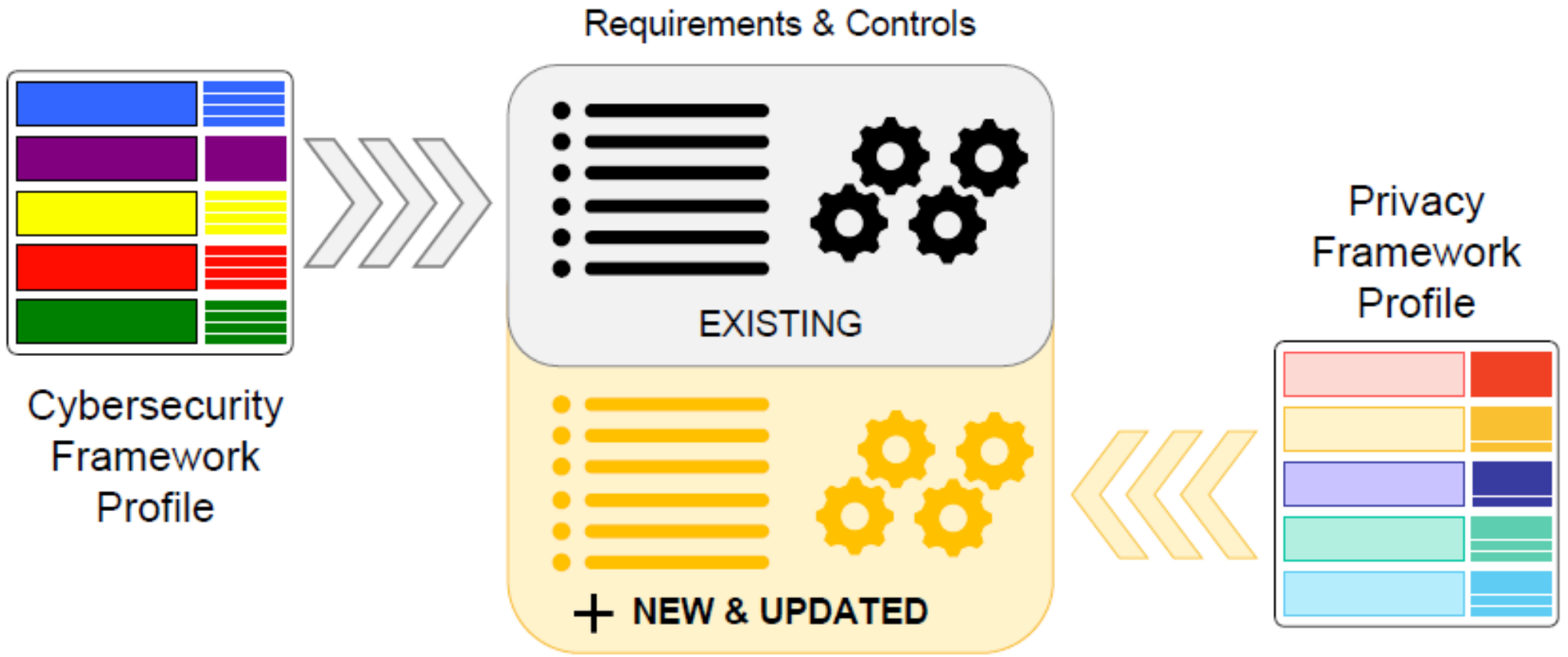
Privacy Event: The occurrence or potential occurrence of problematic data actions

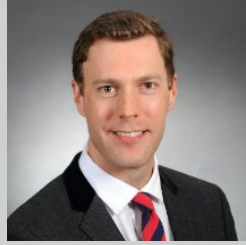
Data Processing: The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal)

Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

armanino

Program Alignment Example

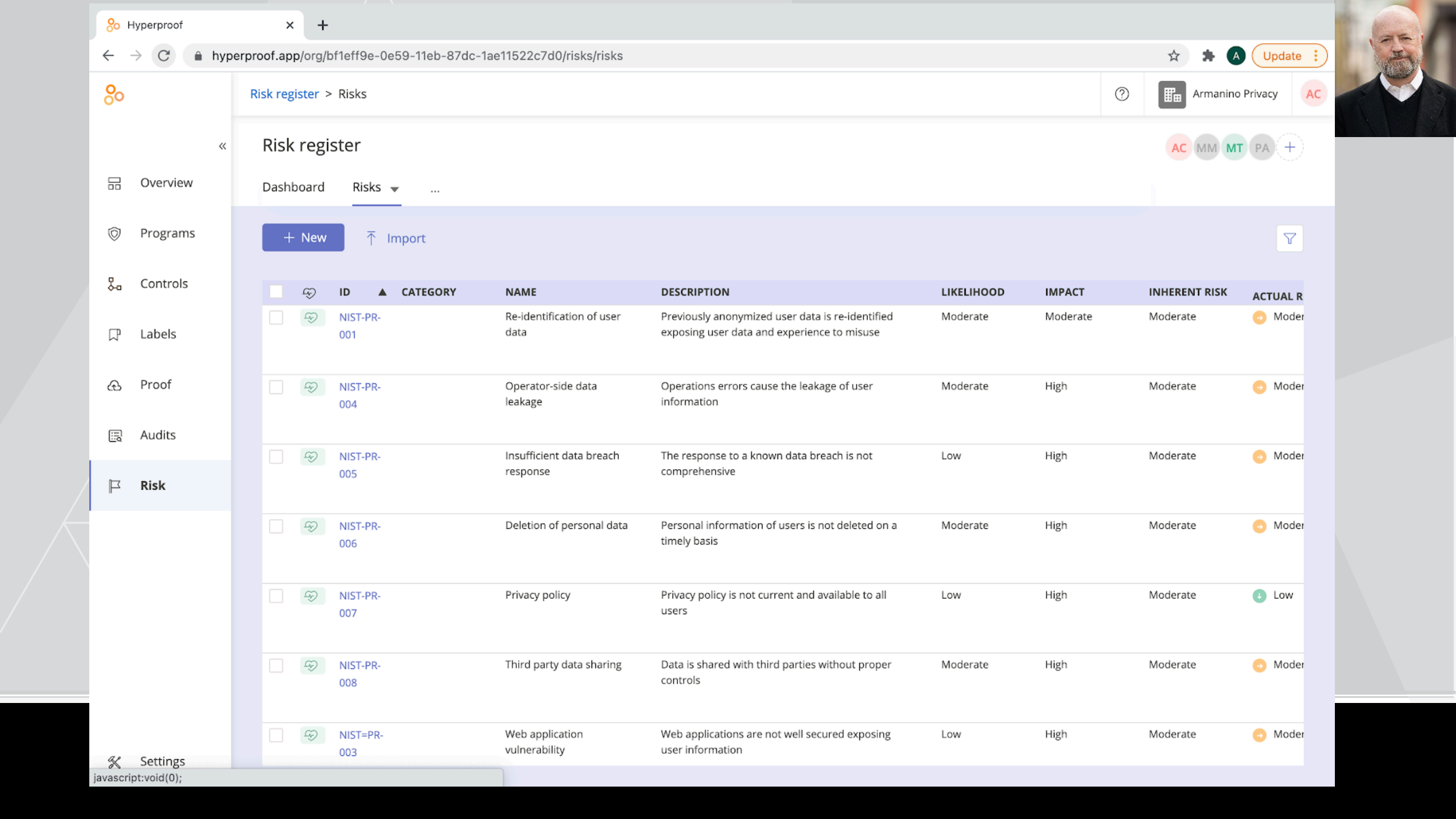




armanino

How technology can facilitate businesses?

armanino


Hyperproof
hyperproof.app/org/bf1eff9e-0e59-11eb-87dc-1ae11522c7d0/risks/risks
Update
Risk register > Risks
Armanino Privacy
AC
Risk register
AC MM MT PA
Overview
Programs
Controls
Labels
Proof
Audits
Risk
Settings
Dashboard
Risks
...
+ New
Import
ID
CATEGORY
NAME
DESCRIPTION
LIKELIHOOD
IMPACT
INHERENT RISK
ACTUAL R
NIST-PR-001
Re-identification of user data
Previously anonymized user data is re-identified exposing user data and experience to misuse
Moderate
Moderate
Moderate
Moder
NIST-PR-004
Operator-side data leakage
Operations errors cause the leakage of user information
Moderate
High
Moderate
Moder
NIST-PR-005
Insufficient data breach response
The response to a known data breach is not comprehensive
Low
High
Moderate
Moder
NIST-PR-006
Deletion of personal data
Personal information of users is not deleted on a timely basis
Moderate
High
Moderate
Moder
NIST-PR-007
Privacy policy
Privacy policy is not current and available to all users
Low
High
Moderate
Low
NIST-PR-008
Third party data sharing
Data is shared with third parties without proper controls
Moderate
High
Moderate
Moder
NIST=PR-003
Web application vulnerability
Web applications are not well secured exposing user information
Low
High
Moderate
Moder
javascript:void(0);

Hyperproof

hyperproof.app/org/bf1eff9e-0e59-11eb-87dc-1ae11522c7d0/risks/2dc0a50d-5e70-11eb-8d6f-ce18481d70d6

Update

Risk register > Risks > NIST-PR-007

Armanino Privacy

AC

Overview

Programs

Controls

Labels

Proof

Audits

Risk

Settings

+ Add

Link additional controls

NIST-PR-007 Privacy policy

Select all

CCPAREG-§ 999.304(a) Privacy policy

(a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and these regulations, including section 999.308.

CCPAREG-§ 999.304(b)

(b) A business that collects personal information from a consumer shall provide a notice at collection in accordance with the CCPA and these regulations, including section 999.305.

CCPAREG-§ 999.304(c)

(c) A business that sells personal information shall provide a notice of right to opt-out in accordance with the CCPA and these regulations, including section 999.306.

CCPAREG-§ 999.304(d)

Filter

Please type filter criteria below

NAME, ID AND DESCRIPTION

Enter control name, id or descriptior

PEOPLE

Select user...

DOMAIN

Select domain...

PROGRAM

Select program...

HEALTH

Select health...

IMPLEMENTATION

Select implementation...

TESTING

Select testing status

Where are the rest of my controls?

3 controls selected

Link selected controls

armanino

Hyperproof

hyperproof.app/org/bf1eff9e-0e59-11eb-87dc-1ae11522c7d0/risks/2dc0a50d-5e70-11eb-8d6f-ce18481d70d6

Update

Risk register > Risks > NIST-PR-007

Armanino Privacy AC

- Overview
- Programs
- Controls
- Labels
- Proof
- Audits
- **Risk**
- Settings

NIST-PR-007 Privacy policy

Details | Notes | ...

RISK ID
NIST-PR-007

RISK NAME
Privacy policy

DESCRIPTION
Privacy policy is not current and available to all users

CATEGORY

OWNER
Maria Mendieta

RESPONSE
Mitigate

RISK HEALTH	Healthy
TOLERANCE	High
ACTUAL RISK	Low
LIKELIHOOD	Low
IMPACT	High

LINKED CONTROLS

+ Add

ID	NAME	DESCRIPTION	MITIGATION %
CCPAREG-§ 999.304(a)	Privacy policy	(a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and these regulations, including section 999.308.	50%
CCPAREG-§ 999.304(b)		(b) A business that collects personal information from a consumer shall provide a notice at collection in accordance with the CCPA and these regulations, including section 999.305.	50%

armanino

Hyperproof

hyperproof.app/org/bf1eff9e-0e59-11eb-87dc-1ae11522c7d0/programs/5440c0e0-12f1-11eb-901c-fa77cd979eb6

Update

Programs > NIST Privacy Framework

Armanino Privacy

AC

NIST Privacy Framework

Critical

Dashboard | Details | Requirements | Controls | Labels | ...

- Overview
- Programs
- Controls
- Labels
- Proof
- Audits
- Risk
- Settings

Program summary (Created: 10/20/2020)

- Requirements 98
- Controls 98
- Labels 0
- Proof links 0

NIST PRIVACY

Program definition

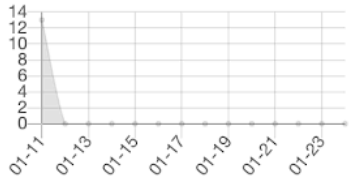
Requirements

36%

0% 100%

Completed	35
In progress	46
Not started	17

Activity



Controls

98 empty controls

Health

Critical	49
At risk	49
Healthy	0
(Not set)	0

Implementation

Unknown	0
Not started	14
In progress	22
Completed	62

Testing

Ineffective	13
Effective	34
In progress	15
Not tested	36

Freshness

Expired	21
Unknown	0
Fresh	77
(Not set)	0

Labels

Freshness

Reuse

Controls

1 link	98
2 links	0
3 links	0
4+ links	0

Labels

Explore

By members (1)

- Aidan Collins (Me)

By domains (6)

- (Not set)
- COMMUNICATE-P (CM-P): Develop an...
- CONTROL-P (CTP): Develop and imple...
- GOVERN-P (GV-P): Develop and imple...
- IDENTIFY-P (IDP): Develop the organiz...

Work/Needs Attention

Today

FRESHNESS

21 controls and 0 labels expired

Name/ID	Expire date
NISTP1.0_CT.DP-P1	1/30/1970
NISTP1.0_CT.DM-P7	1/30/1970
NISTP1.0_CM.AW-P4	1/30/1970
NISTP1.0_CM.AW-P3	1/30/1970
NISTP1.0_GV.AT-P3	1/30/1970
NISTP1.0_GV.AT-P1	1/30/1970
NISTP1.0_CT.DM-P10	1/30/1970

armanino

Hyperproof

hyperproof.app/org/bf1eff9e-0e59-11eb-87dc-1ae11522c7d0/home

Update

Armanino Privacy

AC

- Overview
- Programs
- Controls
- Labels
- Proof
- Audits
- Risk
- Settings

Overview

Programs

NAME	HEALTH	DEFINITION	IMPLEMENTATION	TESTING	FRESHNESS	OWNER
CalCPA Privacy Program	Critical	●	●	●	●	AC
NIST CSF	Critical	●	●	○	○	AC
NIST Privacy Framework	Critical	●	●	●	●	AC
HIPAA Security & Privacy	N/A	●				AC

See less

Controls

566 empty controls

Health

Critical	330
At risk	81
Healthy	1
(Not set)	155

Implementation

Unknown	0
Not started	430
In progress	42
Completed	95

Testing

Ineffective	30
Effective	67
In progress	35
Not tested	435

Freshness

Expired	38
Unknown	22
Fresh	77
(Not set)	430

Labels

Freshness

Reuse

Controls

1 link	566
2 links	1
3 links	0
4+ links	0

Labels

Explore

By members (4)

- Aidan Collins (Me)
- Maria Mendieta
- Mirena Taskova
- Pippa Akem

By domains (32)

- (Not set)
- Administrative safeguards
- Article 2. NOTICES TO CONSUMERS
- Article 3. BUSINESS PRACTICES FOR H...
- Article 4. VERIFICATION OF REQUESTS
- Article 5. SPECIAL RULES REGARDING ...
- Article 6. NON-DISCRIMINATION
- COMMUNICATE-P (CM-P): Develop an...
- CONTROL-P (CTP): Develop and imple...
- DETECT (DE) - Anomalies and Events (...
- DETECT (DE) - Detection Processes (DE...
- DETECT (DE) - Security Continuous Mo...
- GOVERN-P (GV-P): Develop and imple...
- IDENTIFY-P (IDP): Develop the organiz...
- IDENTIFY (ID) - Asset Management (ID....
- IDENTIFY (ID) - Business Environment (...

armanino

Hyperproof

hyperproof.app/org/bf1eff9e-0e59-11eb-87dc-1ae11522c7d0/risks

Update

Armanino Privacy

AC

Risk register

AC MM MT PA

Dashboard | Risks | ...

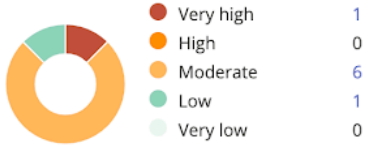
- Overview
- Programs
- Controls
- Labels
- Proof
- Audits
- Risk
- Settings

Risk summary

TOTAL RISKS 8 — 1 — 0 — 7

AVG INHERENT RISK	Moderate
AVG RISK TOLERANCE	High
AVG ACTUAL RISK	Moderate

Actual risk



Very high	1
High	0
Moderate	6
Low	1
Very low	0

Response

Transfer	1
Accept	3
Avoid	2
Mitigate	2

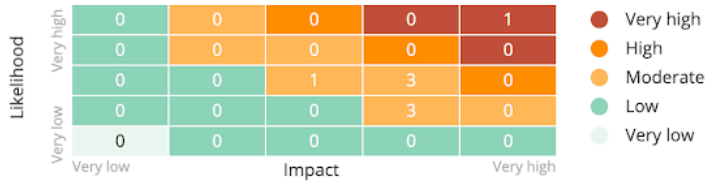
Risk health

Monthly | Quarterly | Yearly

Controls

Critical	2
At risk	0
Healthy	1
(Not set)	0

Risk heatmap



Explore

- By category (1)
  - (Not set)
- By response (4)
  - Accept
  - Avoid
  - Mitigate
  - Transfer
- By owner (4)
  - AC Aidan Collins (Me)
  - MT Mirena Taskova
  - MM Maria Mendieta
  - PA Pippa Akem

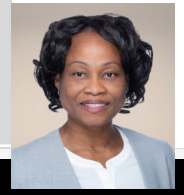
armanino

Top tips for successful annual privacy strategy

armanino

Top tips for successful annual privacy strategy

- Track global privacy developments, expectations, and best practices
- Build consensus and a team early!
- Monitor operational practices to identify new processes or material changes to existing processes; adopt privacy by design principles
- Establish Key Performance Metrics (KPIs), a report up, and evangelize through the organization!

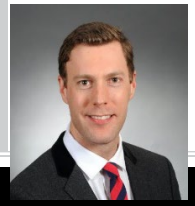


Pippa Akem
ARMANINO

- Evaluate your current privacy practices on the basis of a standard global privacy framework, such as NIST;
- Assess the current privacy risk;
- Create an annual privacy project plan by taking into consideration your current privacy posture, the evaluated privacy risk, the global privacy developments, as well as your specific business needs and budget;
- Assign an experienced privacy expert (e.g., external DPO) with proven global expertise to coordinate the privacy efforts;
- Implement the planned tasks and review success rate at the end of 2021.

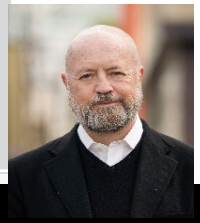
Mirena Taskova
ARMANINO

- Use the NIST Privacy Framework to help meet your privacy goals!
- Explore Privacy Framework implementation resources
  - Crosswalks (e.g., CCPA, GDPR)
  - Privacy Risk Assessment Methodology
  - Quick Start Guide for Small and Medium Businesses



Dylan Gilbert
NIST

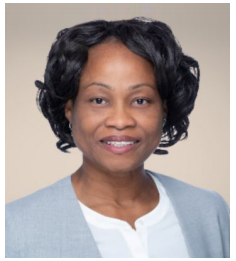
- Technology can help in three areas - process, content and monitoring / reporting.
- Use technology to support a well-defined process that includes stakeholders from across the organization.
- Get the best return on your investment in the NIST Privacy Framework by leveraging crosswalks to achieve compliance with other named frameworks.
- Monitor and communicate your progress on the implementation of NIST Privacy to show progress on improving your security & privacy control posture.



Aidan Collins
HYPERPROOF

armanino

Panel

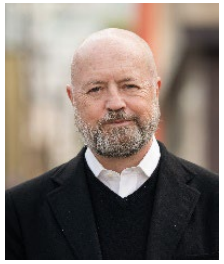


Pippa Akem
Senior Manager, Data Privacy
Armanino LLP
Pippa.Akem@armaninoLLP.com

Dean Quiambao
Chief Relationship Builder
Armanino LLP
DeanQ@amllp.com

Dylan Gilbert
Privacy Policy Advisor
National Institute of Standards and Technology (NIST)
dylan.gilbert@nist.gov

Mirena Taskova
Managing Director, Head of Privacy and Cybersecurity
Armanino LLP
Mirena.Taskova@armaninoLLP.com



Aidan Collins
Head of Enterprise Business
Hyperproof
aidan@hyperproof.io

armanino

THANK YOU

hyperproof

armanino