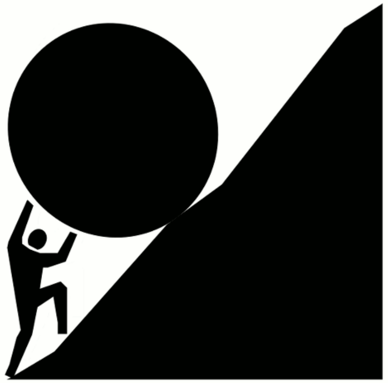
IT Pro Special Issue on Communications Recovery and Resilience

IT Risk and Resilience – Cybersecurity Response to COVID-19

Resilience and Reliability



Tim Weil – IEEE Senior Member
CU-Denver School of Risk Management
http://comsoc.ieee-denver.org

Cybersecurity Professional
SecurityFeeds – http://www.securityfeeds.com

Invited Talk
Denver, CO
Feb 22, 2021

Objectives of this Presentation

Cyberspace – Out Point of Departure

-- A Writer's Life

-- Risk Landscape Evaluation

-- ISO 27001 Information Security Management (BOK)

Information Security Management Models

-- Risk Management Framework (NIST SP 800-37)

-- Deming Cycle - Plan-Do-Check-Act

-- OODA Loop (Joe Boyd, USAF Fighter Pilot)

-- NIST Cybersecurity Frameworks

Global transformation caused by COVID-19

-- Global transformation of Information Technology Services

-- NIST Cybersecurity Framework (up close)

-- COVID Smackdown – NIST CSF vs Big Scary Monsters

-- Recovery and Resilience – IT Context for Business Continuity

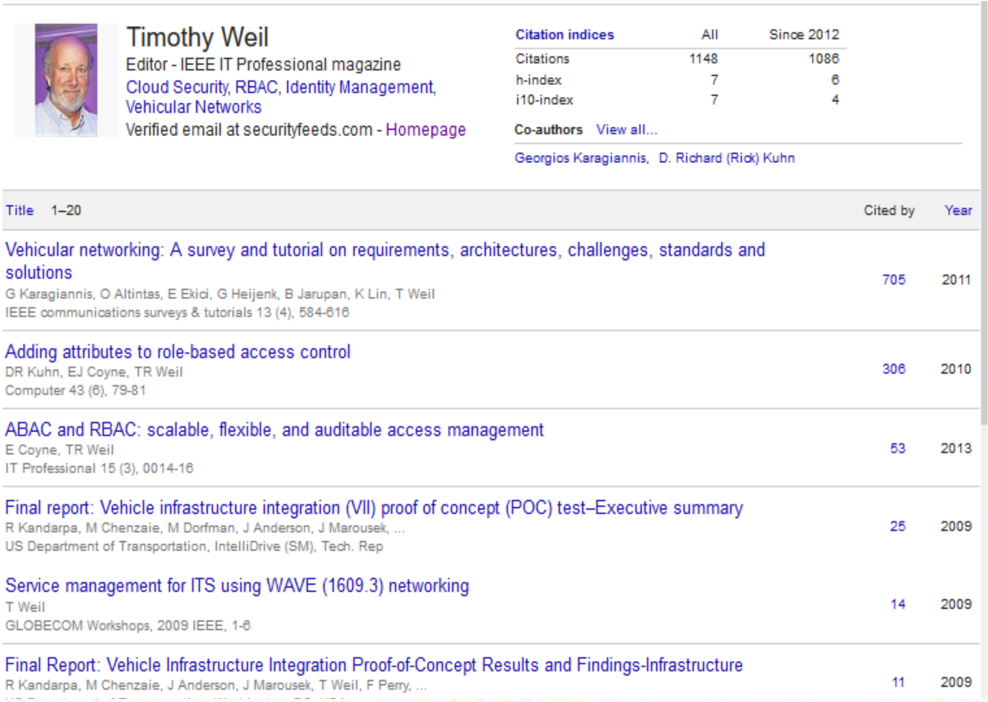
Writing and Editing for Computer Society Publications

-- 1st Citation for 'IT Risk and Resilience – Cybersecurity Response to COVID-19'

-- Random Cybersecurity Attack Simulation Model (RCSM)

-- Write Stuff

A Writer's Life –

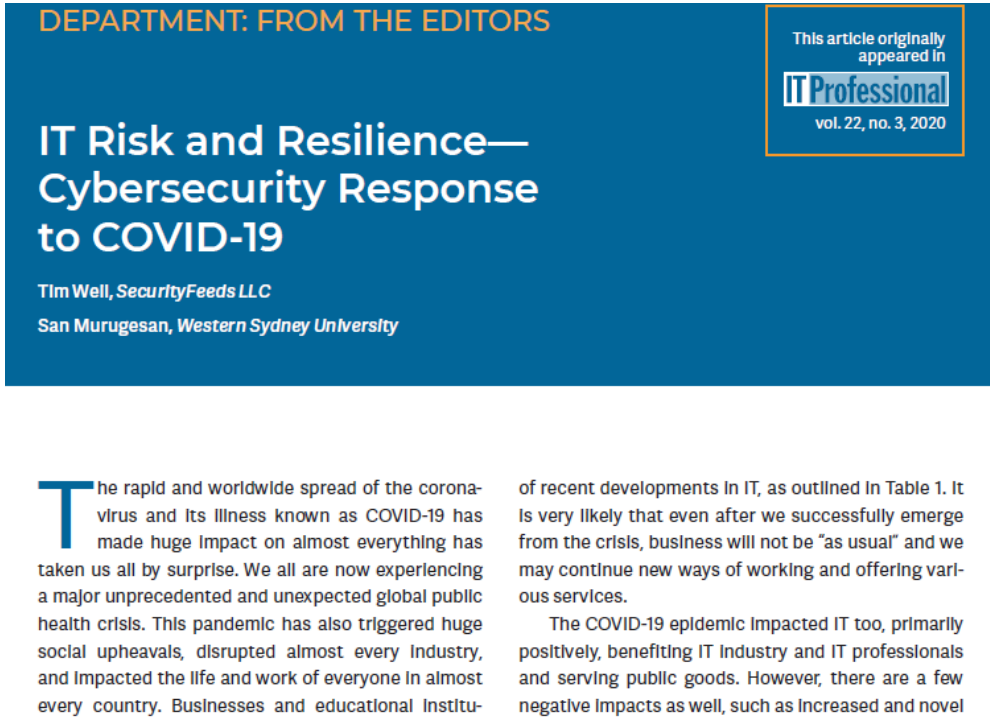


Timothy Weil
Editor - IEEE IT Professional magazine
Cloud Security, RBAC, Identity Management, Vehicular Networks
Verified email at securityfeeds.com - Homepage

Citation indices	All	Since 2012
Citations	1148	1086
h-index	7	6
i10-index	7	4

Co-authors View all...
Georgios Karagiannis, D. Richard (Rick) Kuhn

Title 1–20	Cited by	Year
Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions G Karagiannis, O Altintas, E Ekici, G Heijenk, B Jarupan, K Lin, T Weil IEEE communications surveys & tutorials 13 (4), 584-616	705	2011
Adding attributes to role-based access control DR Kuhn, EJ Coyne, TR Weil Computer 43 (6), 79-81	306	2010
ABAC and RBAC: scalable, flexible, and auditable access management E Coyne, TR Weil IT Professional 15 (3), 0014-16	53	2013
Final report: Vehicle infrastructure integration (VII) proof of concept (POC) test–Executive summary R Kandarpa, M Chenzaie, M Dorfman, J Anderson, J Marousek, ... US Department of Transportation, IntelliDrive (SM), Tech. Rep	25	2009
Service management for ITS using WAVE (1609.3) networking T Weil GLOBECOM Workshops, 2009 IEEE, 1-6	14	2009
Final Report: Vehicle Infrastructure Integration Proof-of-Concept Results and Findings-Infrastructure R Kandarpa, M Chenzaie, J Anderson, J Marousek, T Weil, F Perry, ...	11	2009



DEPARTMENT: FROM THE EDITORS

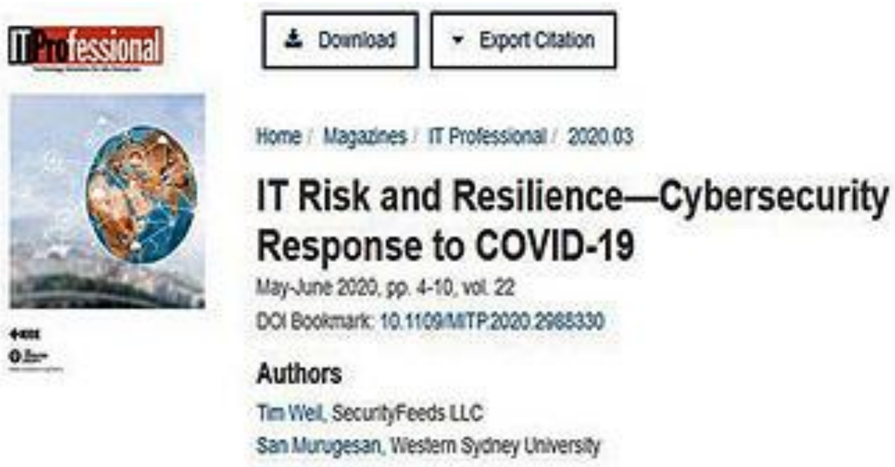
This article originally appeared in IT Professional vol. 22, no. 3, 2020

IT Risk and Resilience—Cybersecurity Response to COVID-19

Tim Weil, *SecurityFeeds LLC*
San Murugesan, *Western Sydney University*

The rapid and worldwide spread of the coronavirus and its illness known as COVID-19 has made huge impact on almost everything has taken us all by surprise. We all are now experiencing a major unprecedented and unexpected global public health crisis. This pandemic has also triggered huge social upheavals, disrupted almost every industry, and impacted the life and work of everyone in almost every country. Businesses and educational institu- of recent developments in IT, as outlined in Table 1. It is very likely that even after we successfully emerge from the crisis, business will not be "as usual" and we may continue new ways of working and offering various services.

The COVID-19 epidemic impacted IT too, primarily positively, benefiting IT industry and IT professionals and serving public goods. However, there are a few negative impacts as well, such as increased and novel



Download ▾ Export Citation

Home / Magazines / IT Professional / 2020.03

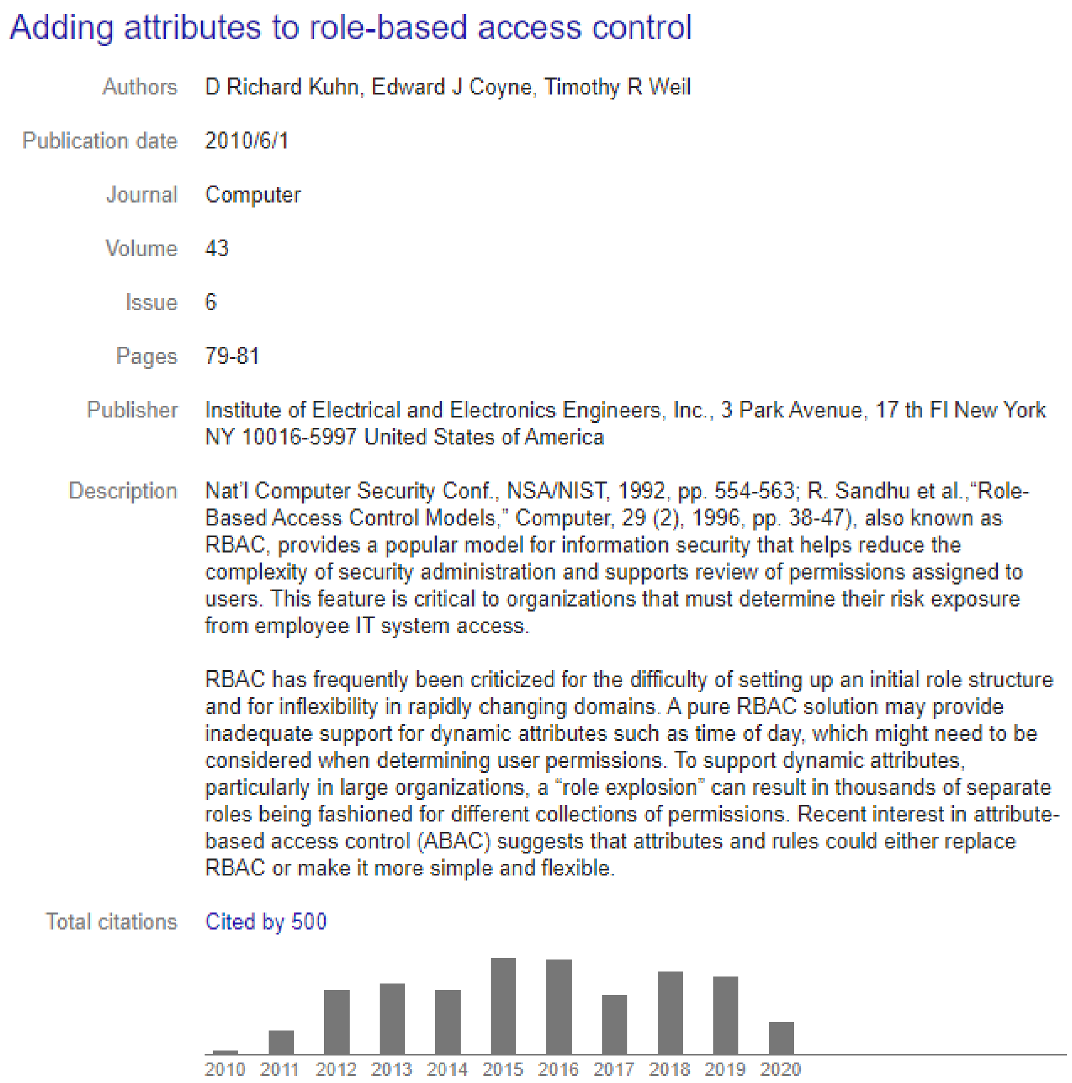
IT Risk and Resilience—Cybersecurity Response to COVID-19

May-June 2020, pp. 4-10, vol. 22
DOI Bookmark: 10.1109/MITP.2020.2988330

Authors
Tim Weil, SecurityFeeds LLC
San Murugesan, Western Sydney University

Adding Attributes to Role Based Access Control reaches 500 citations on Google Scholar - https://lnkd.in/ew_BQaF

COMPUTING edge
Security and Privacy
Data
Internet
Artificial Intelligence
IEEE
For Users of ZENITH Computers
SEXTANT
Video Image Processing With Zip and ImageWise
Building the '248
Fast Fractals for Your '150 or '100
IBM Emulation With the Scottie Board
Time- and Date-Stamp Your CP/M Files
A Brain Transplant for the Z100
IT Professional
IT SECURITY
GREEN SOFTWARE 44
GRAPH DATABASES 58
IEEE
Computer
JUNE 2010
CAPTURING THE WORLD
IEEE
IEEE SECURITY & PRIVACY
Risking Communications Security
POST
IEEE



Adding attributes to role-based access control

Authors D Richard Kuhn, Edward J Coyne, Timothy R Weil

Publication date 2010/6/1

Journal Computer

Volume 43

Issue 6

Pages 79-81

Publisher Institute of Electrical and Electronics Engineers, Inc., 3 Park Avenue, 17 th Fl New York NY 10016-5997 United States of America

Description Nat'l Computer Security Conf., NSA/NIST, 1992, pp. 554-563; R. Sandhu et al.,"Role-Based Access Control Models," Computer, 29 (2), 1996, pp. 38-47), also known as RBAC, provides a popular model for information security that helps reduce the complexity of security administration and supports review of permissions assigned to users. This feature is critical to organizations that must determine their risk exposure from employee IT system access.

RBAC has frequently been criticized for the difficulty of setting up an initial role structure and for inflexibility in rapidly changing domains. A pure RBAC solution may provide inadequate support for dynamic attributes such as time of day, which might need to be considered when determining user permissions. To support dynamic attributes, particularly in large organizations, a "role explosion" can result in thousands of separate roles being fashioned for different collections of permissions. Recent interest in attribute-based access control (ABAC) suggests that attributes and rules could either replace RBAC or make it more simple and flexible.

Total citations Cited by 500

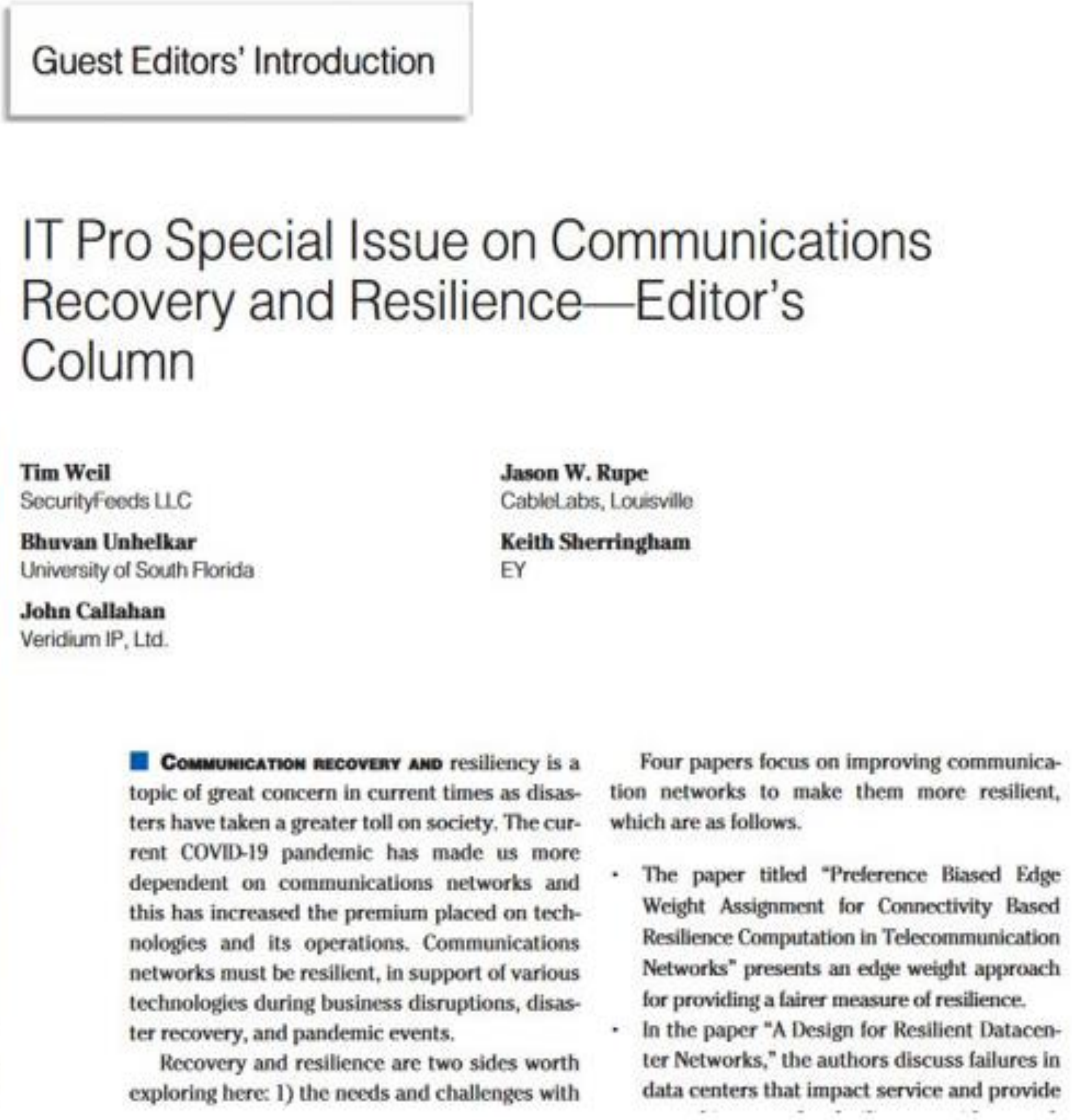
IT Professional

Technology Solutions for the Enterprise

VOLUME 22, NUMBER 6

NOVEMBER/DECEMBER 20

Resilience and Reliabilit



Guest Editors' Introduction

IT Pro Special Issue on Communications Recovery and Resilience—Editor's Column

Tim Weil
SecurityFeeds LLC

Bhuvan Unhelkar
University of South Florida

John Callahan
Veridium IP, Ltd.

Jason W. Rupe
CableLabs, Louisville

Keith Sherringham
EY

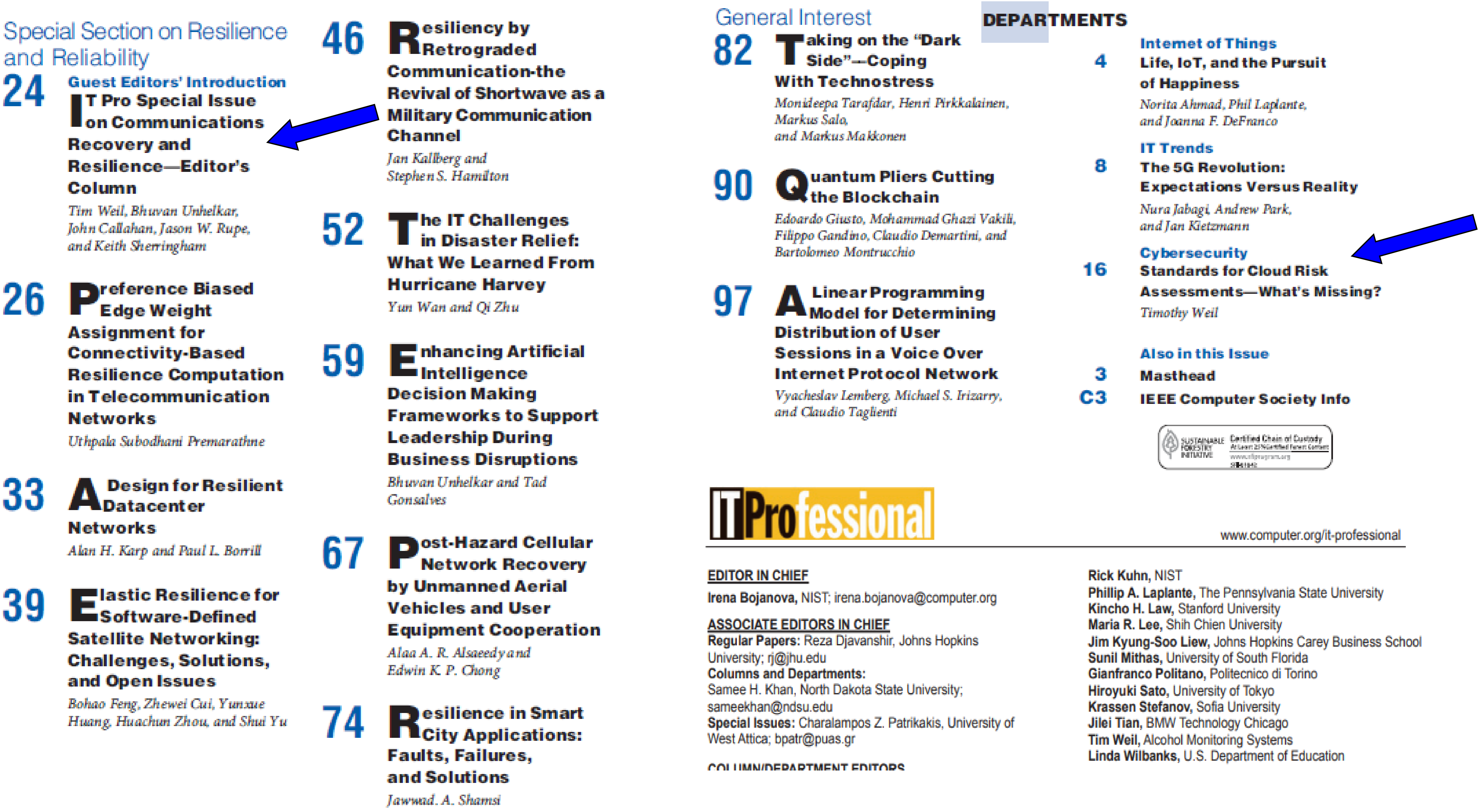
■ COMMUNICATION RECOVERY AND resiliency is a topic of great concern in current times as disasters have taken a greater toll on society. The current COVID-19 pandemic has made us more dependent on communications networks and this has increased the premium placed on technologies and its operations. Communications networks must be resilient, in support of various technologies during business disruptions, disaster recovery, and pandemic events.

Recovery and resilience are two sides worth exploring here: 1) the needs and challenges with

Four papers focus on improving communication networks to make them more resilient, which are as follows.

- The paper titled "Preference Biased Edge Weight Assignment for Connectivity Based Resilience Computation in Telecommunication Networks" presents an edge weight approach for providing a fairer measure of resilience.
- In the paper "A Design for Resilient Datacenter Networks," the authors discuss failures in data centers that impact service and provide

https://www.computer.org/csdl/magazine/it/2020/06/09250314/1oxkJTuIsMg



ITProfessional

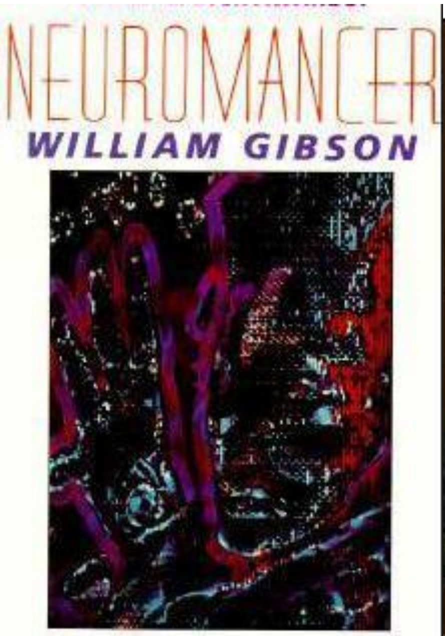
www.computer.org/it-professional

Table of Contents

- Cyberspace – Our Point of Departure
- Information Security Management Models
- Frameworks for Risk Management
- COVID Smackdown – NIST CSF vs Big Scary Monsters
- Random Cybersecurity Attack Simulation Model (RCSM)
- References + Q&A

Cyberspace – Our Point of Departure – Wired Magazine (June ‘08) - https://www.wired.com/2008/05/pentagon-define/

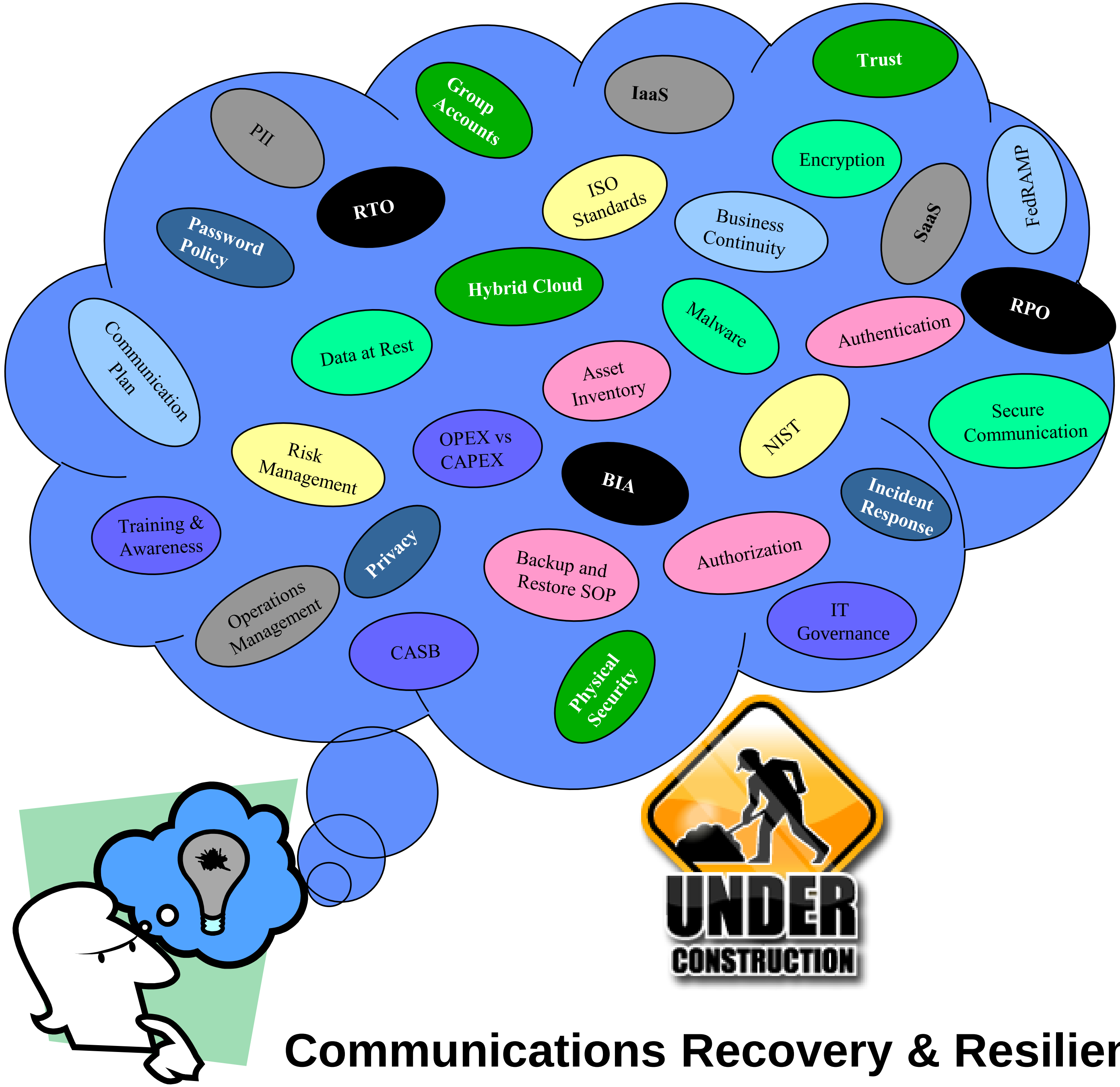
26 YEARS AFTER GIBSON, PENTAGON DEFINES 'CYBERSPACE'



"More than two decades after novelist William Gibson coined the term cyberspace as a 'consensual hallucination' of data... the Pentagon has come up with its own definition,"* **Inside Defense* reports. "A May 12 'for official use only' memo signed by Deputy Defense Secretary Gordon England... offers a 28-word meaning for the term.“ It is decidedly "less poetic" than Gibson's

Cyberspace, England writes, is “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” *

*It is a far cry from the prose Gibson used in his 1984 novel “Neuromancer” to describe cyberspace: “A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.”



IT 101 – What Problems Are We Trying to Solve?

- Identify 'Fix-It' areas in the program
- Understand Current State (Remediation)
- Improve 'ad hoc', 'not my problem' state
- **Reduce Program Risk**
- Improve Continuous Monitoring Process

Antarctica, the only continent without coronavirus, braces for summer rotation

PUBLISHED SUN, SEP 27 2020·9:30 AM EDT | UPDATED SUN, SEP 27 2020·12:56 PM EDT

Emma Newburger
@EMMA_NEWBURGER

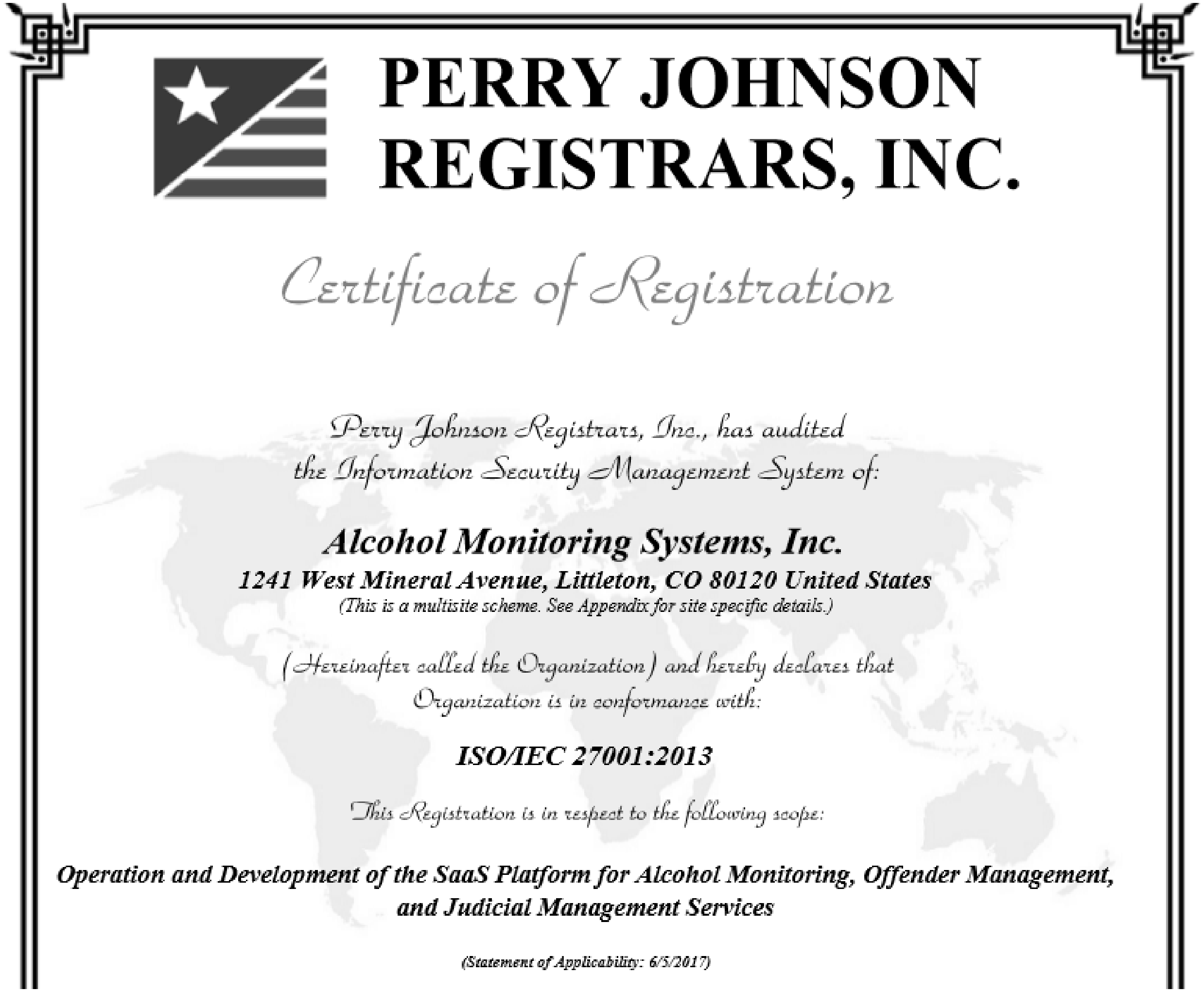
KEY POINTS

- Antarctica, the coldest and most isolated part of the world, is the only continent still untouched by the coronavirus.
- But as Antarctica's harsh winter comes to a close, critical global efforts are

TRENDING NOW

If you work
due to Cov
tax surpris
coming

Context of the Risk Assessment – AMS Products and Services – http://www.scramsystems.com



PERRY JOHNSON REGISTRARS, INC.

Certificate of Registration

Perry Johnson Registrars, Inc., has audited
the Information Security Management System of:

Alcohol Monitoring Systems, Inc.
1241 West Mineral Avenue, Littleton, CO 80120 United States
(This is a multisite scheme. See Appendix for site specific details.)

(Hereinafter called the Organization) and hereby declares that
Organization is in conformance with:

ISO/IEC 27001:2013

This Registration is in respect to the following scope:

Operation and Development of the SaaS Platform for Alcohol Monitoring, Offender Management, and Judicial Management Services

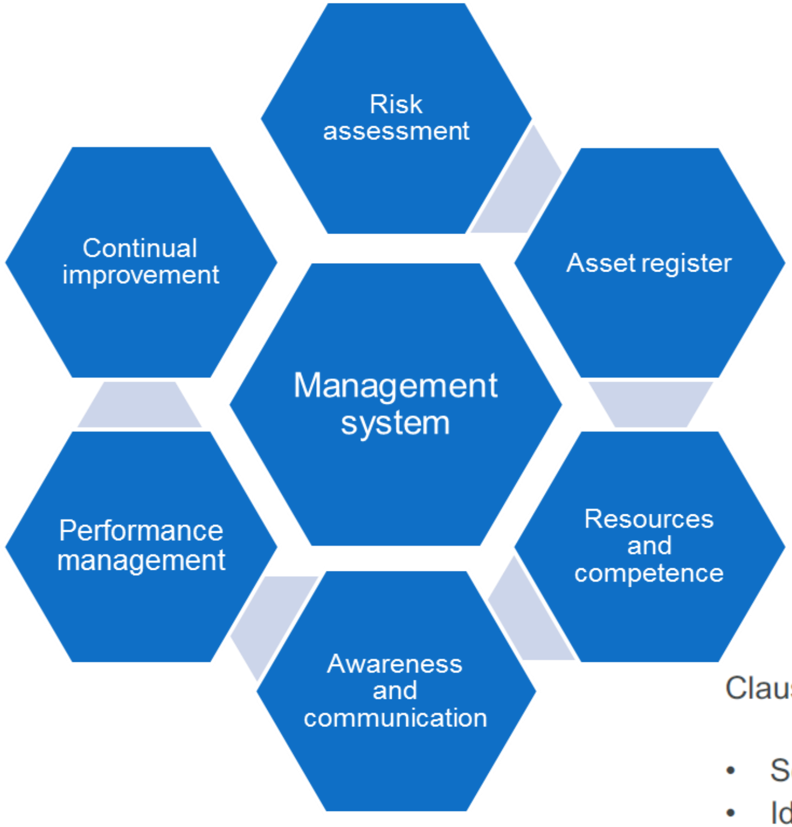
(Statement of Applicability: 6/5/2017)

After a thorough independent audit, SCRAM Systems has received ISO/IEC 27001:2013 ***certification for alcohol monitoring, offender management, and judicial management services in SCRAMnet, our Software as a Service (SaaS) program***. This confirms that SCRAM Systems has implemented internationally-recognized best practices and standards for its Information Security Management System (ISMS).

The certification complements the ISO 9001 certification for quality management systems (QMS) acquired previously.

ISO is an independent, international organization that develops standards to help businesses create and deliver quality products, services, and systems. The International Electrotechnical Commission (IEC) develops standards for information technology (IT) and information and communications technology (ICT).nt.

The ISO/IEC 27001 standard



Clauses 4 through 10 deal with:

- Scoping of the ISMS
- Identifying and evaluating Risks
- Risk Treatment and mitigation
- Managing and measuring performance of the ISMS
- Tracking non-conformities and resolution
- Continuous improvement

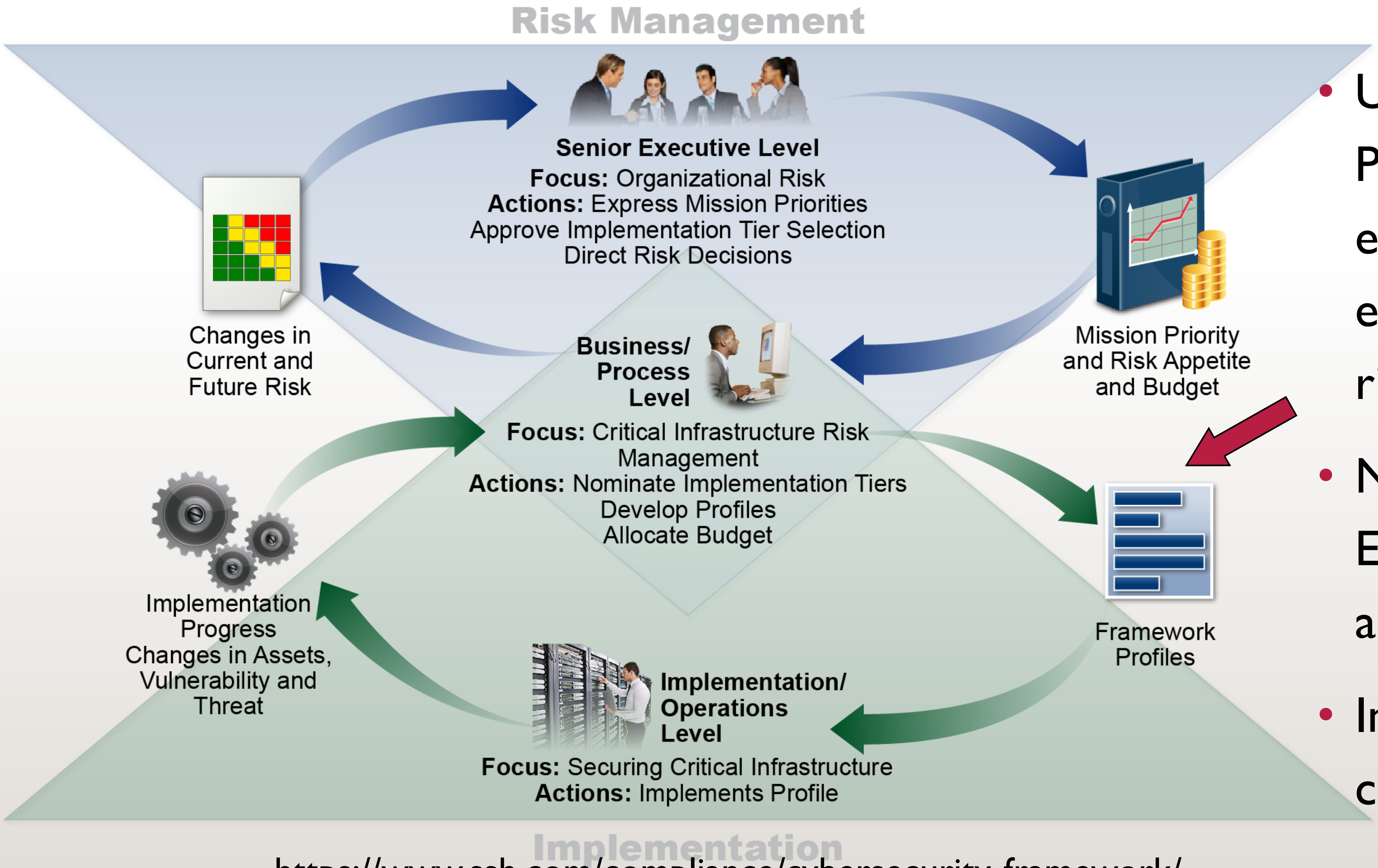
Annex A deals with:
114 Optional controls for risk mitigation

ISO/IEC 27001 Controls

Information security policies	Organisation of information security	Human resources security	Asset management
Access control	Cryptography	Physical and environmental security	Operations security
Communications security	System acquisition, development and maintenance	Supplier relationships	Incident management
	Business continuity management	Compliance	

Table of Contents

- Cyberspace – Our Point of Departure
- Information Security Management Models
- Frameworks for Risk Management
- COVID Smackdown – NIST CSF vs Big Scary Monsters
- Random Cybersecurity Attack Simulation Model (RCSM)
- References + Q&A


Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget
Implementation Progress
Changes in Assets, Vulnerability and Threat
Framework Profiles
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

https://www.ssh.com/compliance/cybersecurity-framework/

- Use Risk Matrix to Prioritize actions and expenditures. Most economic value for each risk considered.
- Nominate Tasks and Expenditures for budget allocation
- Implementation of critical Infrastructure

Cybersecurity shouldn’t be an afterthought

Cyberthreats should not be thought of just in the context of IT security and privacy design. Adequate cybersecurity must involve the active participation of everyone in an organization, as well as users. Approaches generally reflect some variation on the common-sense method of evaluating the problem, preparing, acting, and assessing the results.

Federal agencies use the **Risk Management Framework (RMF)** to Assess and Authorize enterprise systems

The RMF model has been accelerated for **Cloud Environments (RMF4CE)**

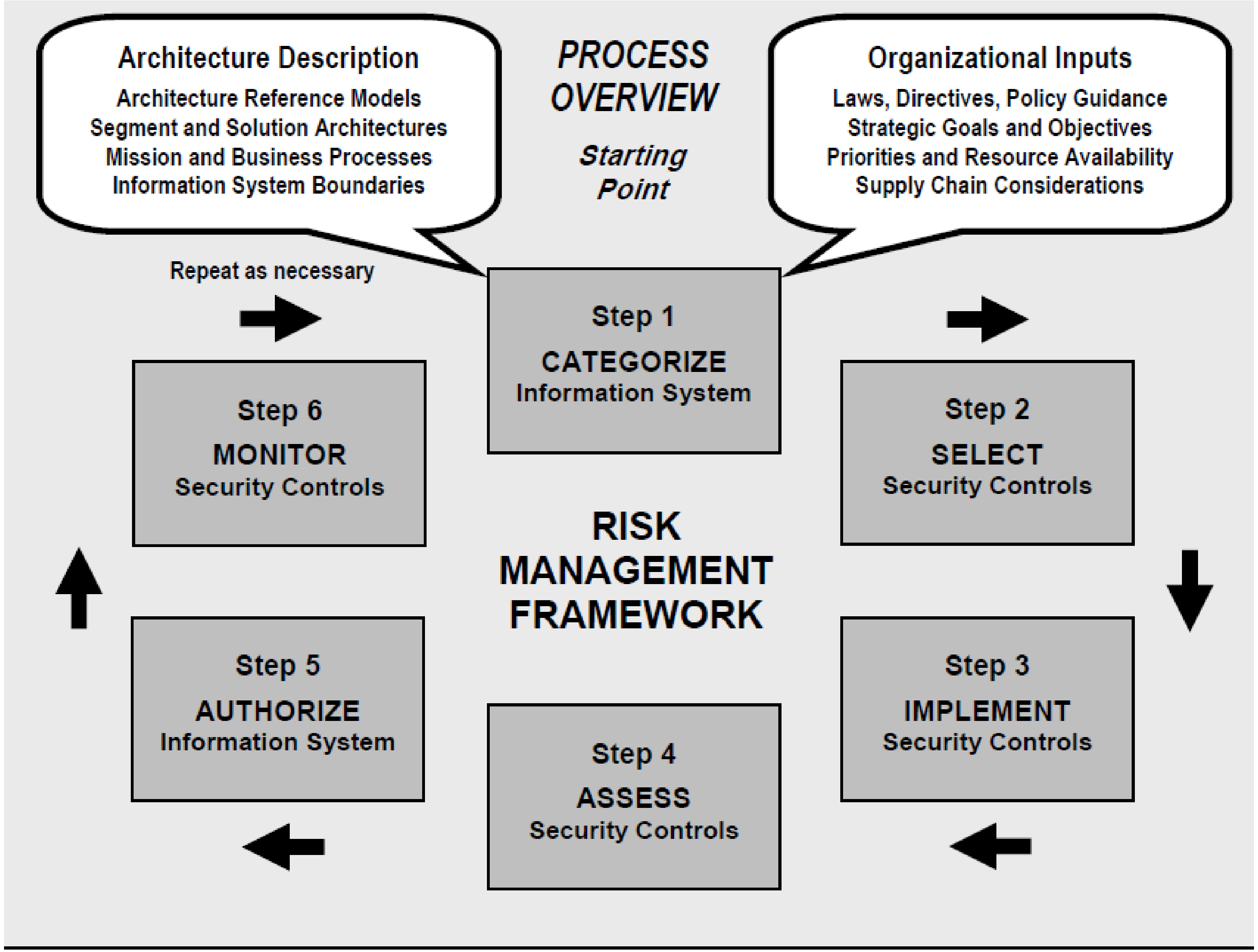
Managers learn a **Plan-Do-Check-Act** (PDCA) cycle.

Fighter pilots are taught to **Observe-Orient-Decide-Act (OODA)**.

In cybersecurity the latest incarnation of this common-sense approach is the popular **NIST Cybersecurity Framework (CSF),** which teaches **Identify-Protect-Detect-Respond-Recover.**

As in other fields, these activities are intended to be performed in a continuous cycle, modifying plans and actions as the organization learns from successes and failures.

The FISMA Risk Management Framework.



Architecture Description

Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

PROCESS OVERVIEW

Starting Point

Organizational Inputs

Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

Repeat as necessary

Step 1
CATEGORIZE
Information System

Step 2
SELECT
Security Controls

Step 3
IMPLEMENT
Security Controls

Step 4
ASSESS
Security Controls

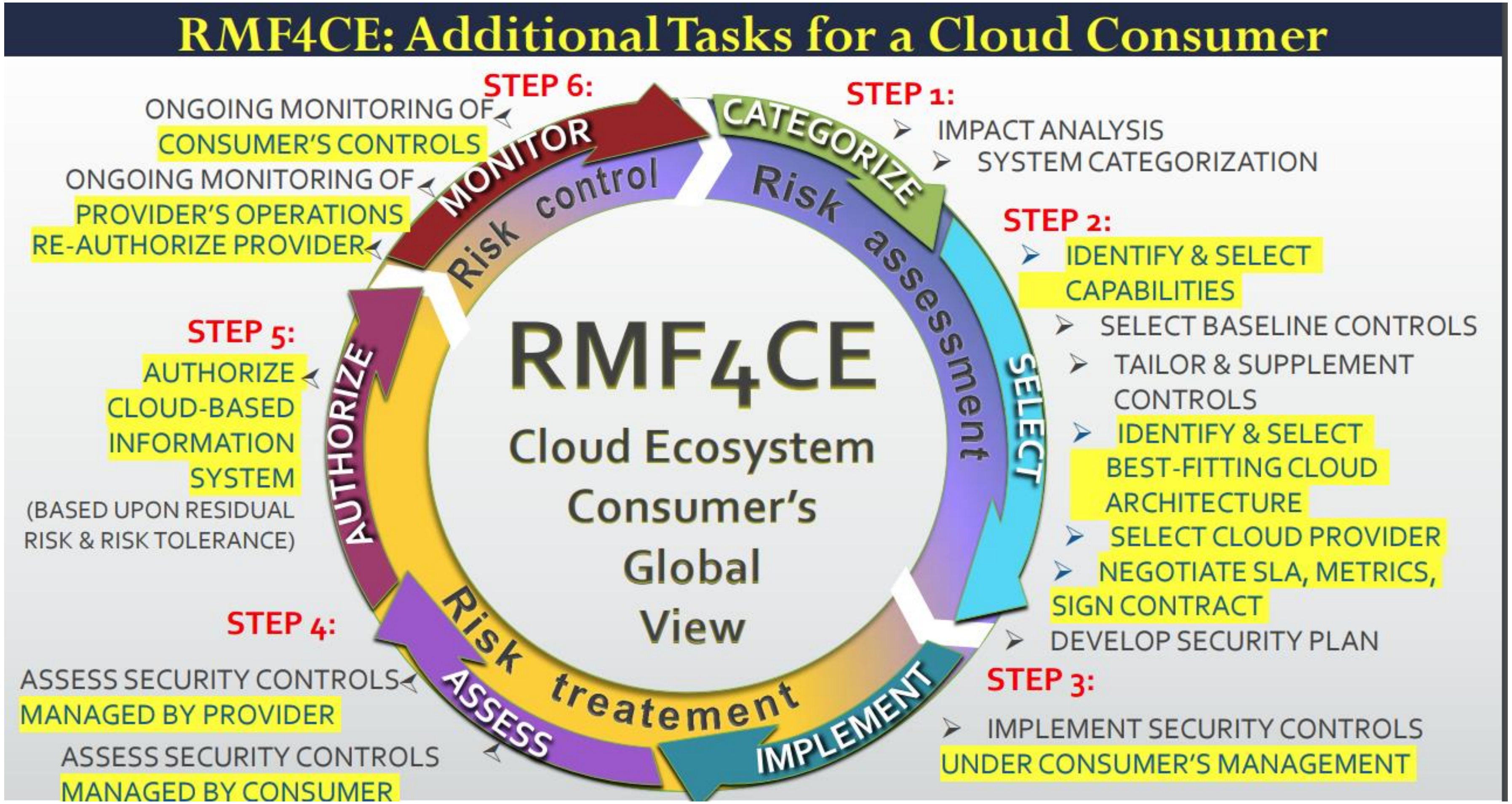
Step 5
AUTHORIZE
Information System

Step 6
MONITOR
Security Controls

RISK MANAGEMENT FRAMEWORK

FIGURE 2-2: RISK MANAGEMENT FRAMEWORK

RMF For Cloud Environments



RMF4CE: Additional Tasks for a Cloud Consumer

STEP 1:
- IMPACT ANALYSIS
- SYSTEM CATEGORIZATION

STEP 2:
- IDENTIFY & SELECT CAPABILITIES
- SELECT BASELINE CONTROLS
- TAILOR & SUPPLEMENT CONTROLS
- IDENTIFY & SELECT BEST-FITTING CLOUD ARCHITECTURE
- SELECT CLOUD PROVIDER
- NEGOTIATE SLA, METRICS, SIGN CONTRACT
- DEVELOP SECURITY PLAN

STEP 3:
- IMPLEMENT SECURITY CONTROLS UNDER CONSUMER'S MANAGEMENT

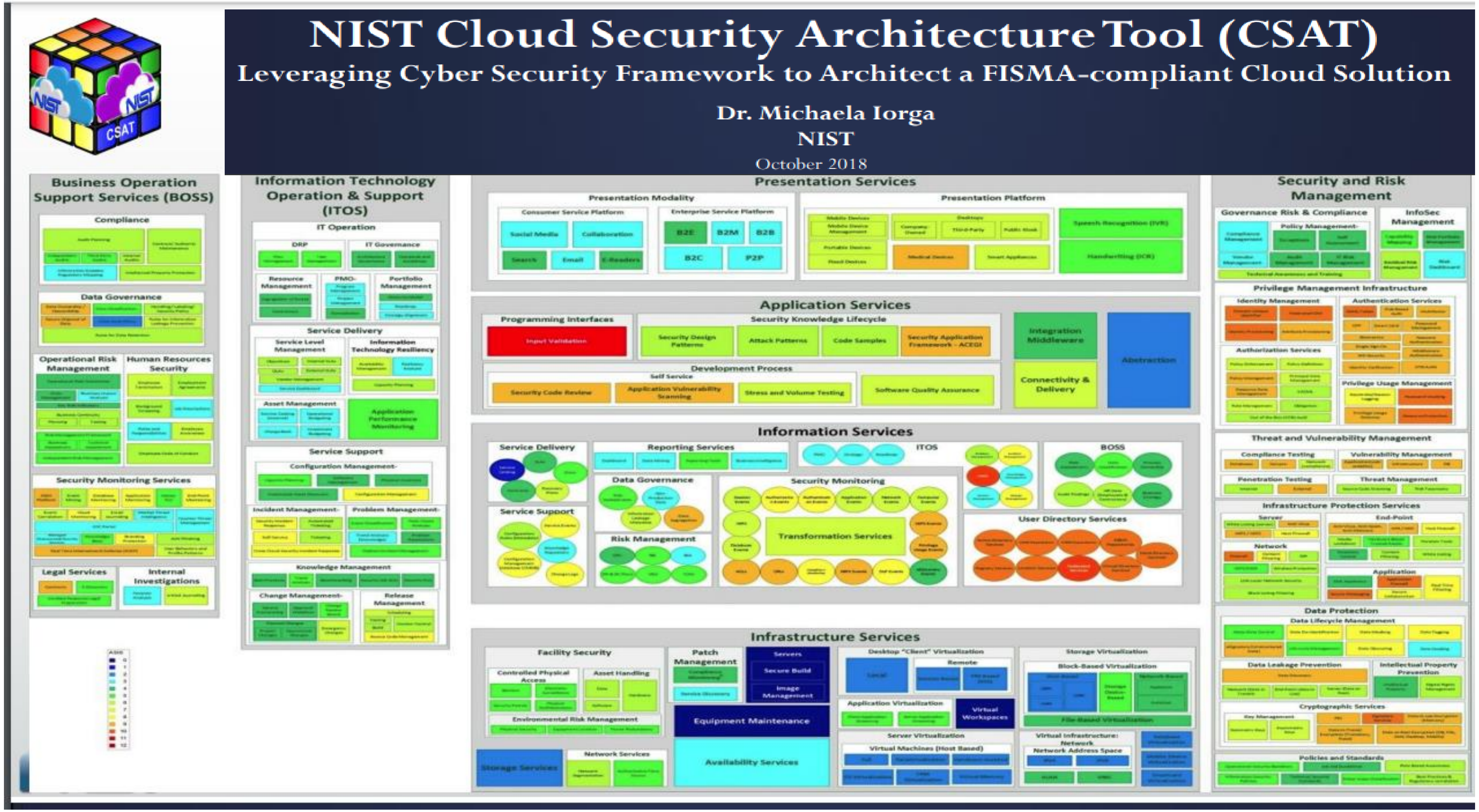
STEP 4:
- ASSESS SECURITY CONTROLS MANAGED BY PROVIDER
- ASSESS SECURITY CONTROLS MANAGED BY CONSUMER

STEP 5:
- AUTHORIZE CLOUD-BASED INFORMATION SYSTEM

(BASED UPON RESIDUAL RISK & RISK TOLERANCE)

STEP 6:
- ONGOING MONITORING OF CONSUMER'S CONTROLS
- ONGOING MONITORING OF PROVIDER'S OPERATIONS
- RE-AUTHORIZE PROVIDER

RMF For Cloud Environments



NIST Cloud Security Architecture Tool (CSAT)

Leveraging Cyber Security Framework to Architect a FISMA-compliant Cloud Solution

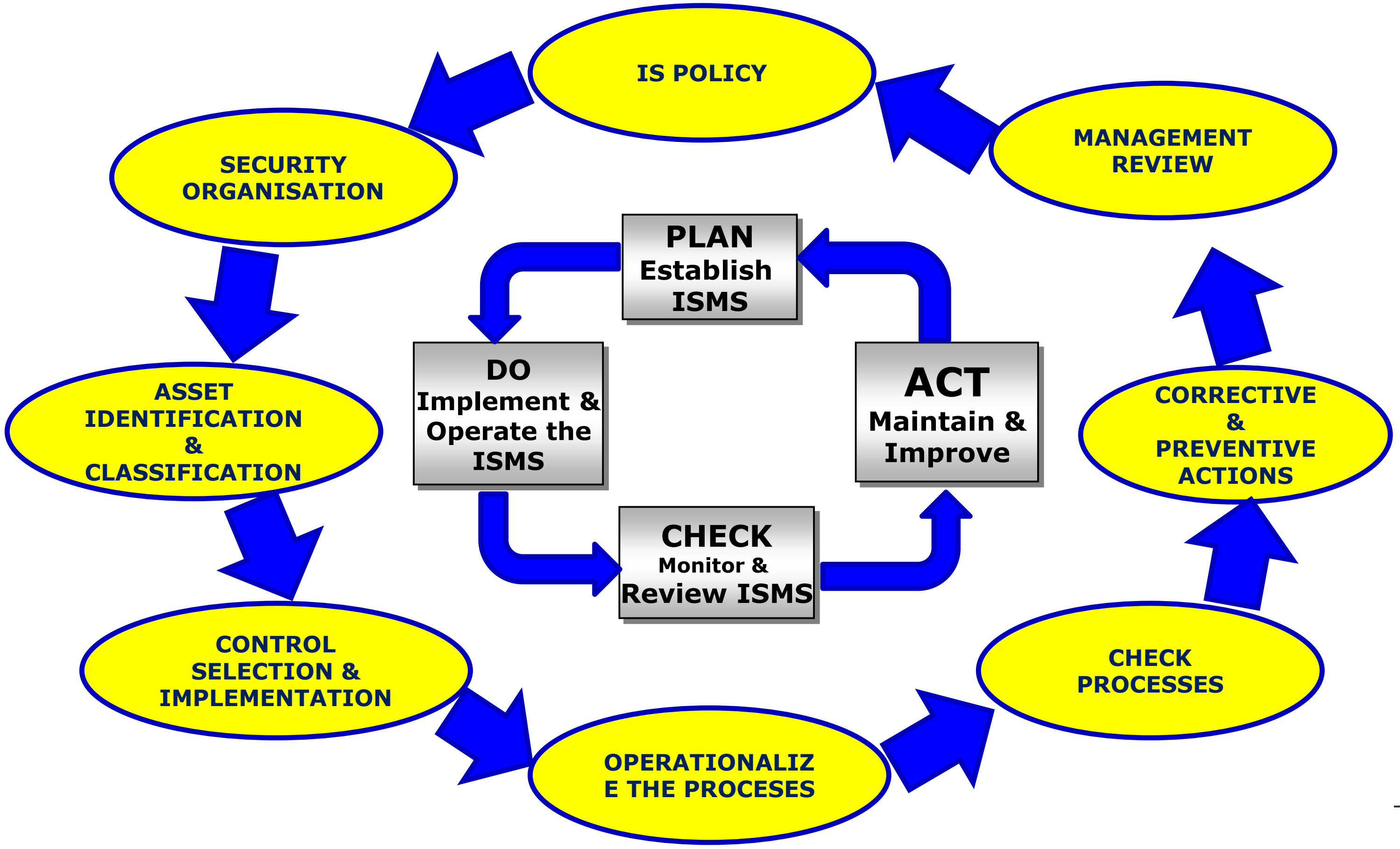
Dr. Michaela Iorga

NIST

October 2018

https://www.fbcinc.com/e/FITSC/presentations/Iorga-FITSC-CSAT_with_RMFOSCAL.pdf

ISMS PROCESS CYCLE – ISO 27001



IS POLICY

SECURITY ORGANISATION

ASSET IDENTIFICATION & CLASSIFICATION

CONTROL SELECTION & IMPLEMENTATION

OPERATIONALIZE THE PROCESES

CHECK PROCESSES

CORRECTIVE & PREVENTIVE ACTIONS

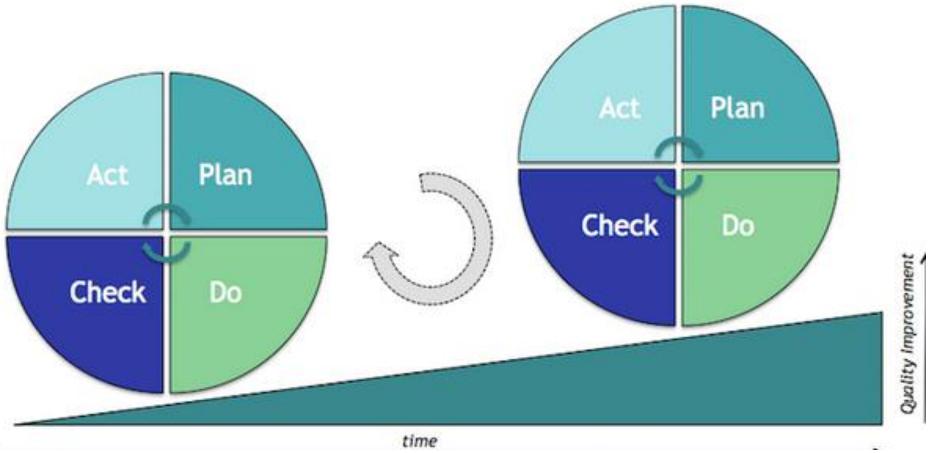
MANAGEMENT REVIEW

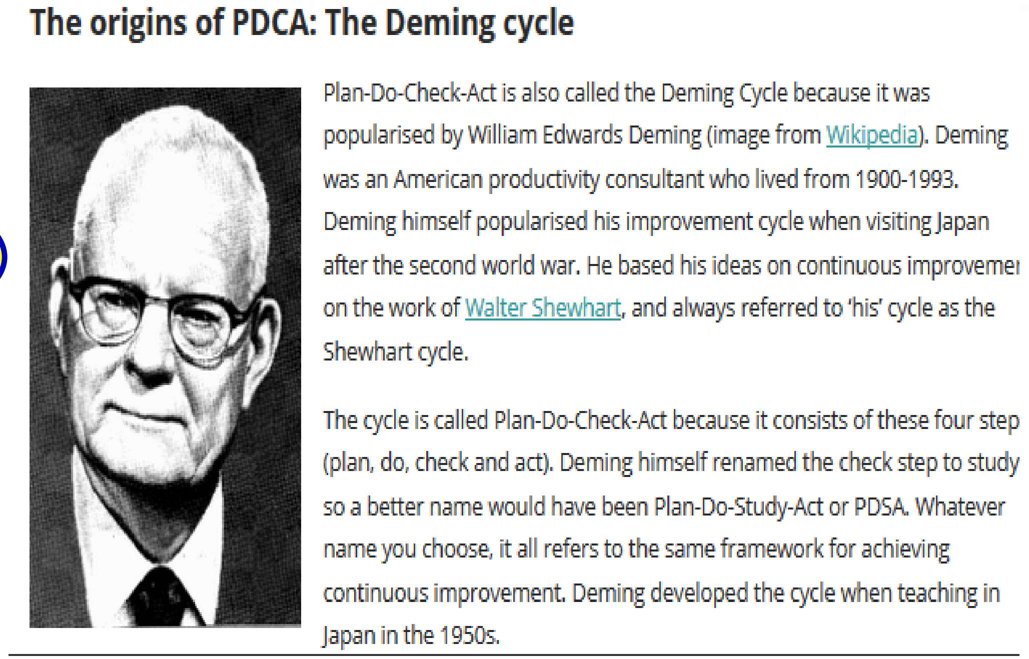
PLAN Establish ISMS

DO Implement & Operate the ISMS

CHECK Monitor & Review ISMS

ACT Maintain & Improve



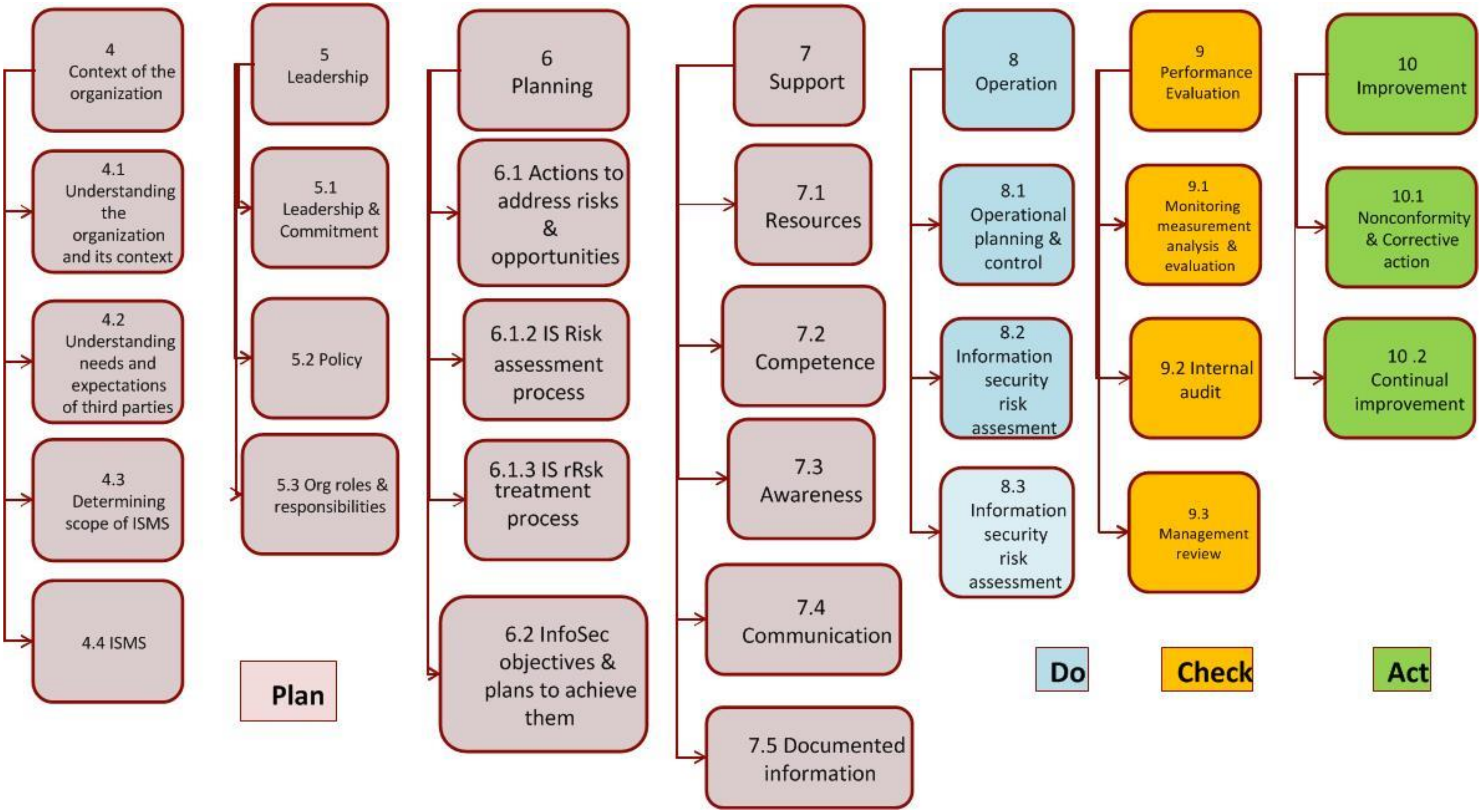


The origins of PDCA: The Deming cycle

Plan-Do-Check-Act is also called the Deming Cycle because it was popularised by William Edwards Deming (image from Wikipedia). Deming was an American productivity consultant who lived from 1900-1993. Deming himself popularised his improvement cycle when visiting Japan after the second world war. He based his ideas on continuous improveme on the work of Walter Shewhart, and always referred to 'his' cycle as the Shewhart cycle.

The cycle is called Plan-Do-Check-Act because it consists of these four step (plan, do, check and act). Deming himself renamed the check step to study so a better name would have been Plan-Do-Study-Act or PDSA. Whatever name you choose, it all refers to the same framework for achieving continuous improvement. Deming developed the cycle when teaching in Japan in the 1950s.

Plan Do Check Act (ISO 27001 Implementation Plan)



4 Context of the organization
- 4.1 Understanding the organization and its context
- 4.2 Understanding needs and expectations of third parties
- 4.3 Determining scope of ISMS
- 4.4 ISMS

5 Leadership
- 5.1 Leadership & Commitment
- 5.2 Policy
- 5.3 Org roles & responsibilities

6 Planning
- 6.1 Actions to address risks & opportunities
- 6.1.2 IS Risk assessment process
- 6.1.3 IS rRsk treatment process
- 6.2 InfoSec objectives & plans to achieve them

7 Support
- 7.1 Resources
- 7.2 Competence
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented information

8 Operation
- 8.1 Operational planning & control
- 8.2 Information security risk assesment
- 8.3 Information security risk assessment

9 Performance Evaluation
- 9.1 Monitoring measurement analysis & evaluation
- 9.2 Internal audit
- 9.3 Management review

10 Improvement
- 10.1 Nonconformity & Corrective action
- 10 .2 Continual improvement

Plan

Do

Check

Act

Risk Management - *OODA Loop*

On the surface – and how many people still interpret the OODA model – it seems to be a simple step-by-step loop. For our purposes here, in this series, we could reframe ‘**Observe’ as ‘sense**‘ – the process of sensing out what seems to be happening in our world – and ‘**Orient’ as ‘make-sense‘** – literally ‘sensemaking’ from what we’ve observed – which leads us onward to **decide and act,** at which point we loop back to sense and make-sense again.

O

A

Act

Accept, Transfer, Mitigate,
Remediate, or Avoid the risk

O

Observe

Requirements and Work Products

D

Decide

IT management goals for reducing risk

Recommended approaches

Allocate Budget and Resource

O

Remember This?

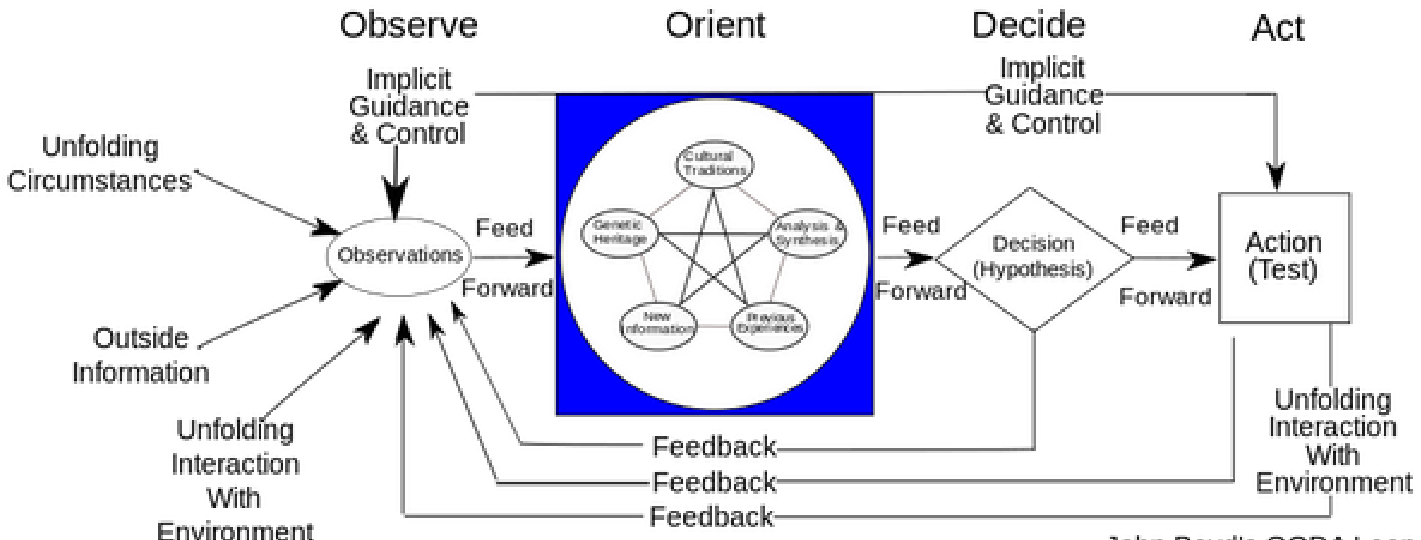
Orient (*You are here*)

Identify trends

Distill the areas of risk

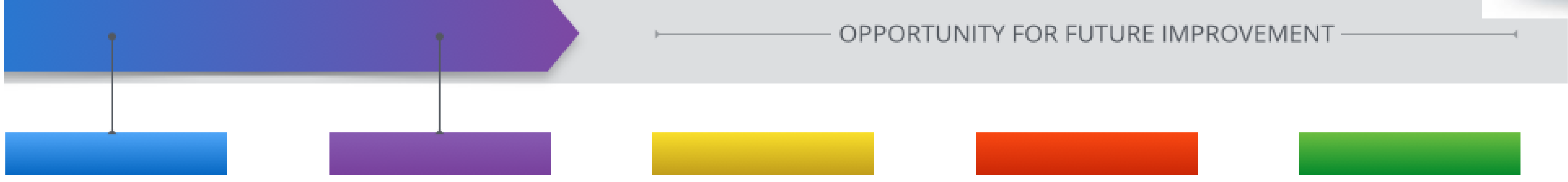
Identify a coordinator

Streamline the process & incorporate best practices



John Boyd's OODA Loop

NIST Cybersecurity Framework –



IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

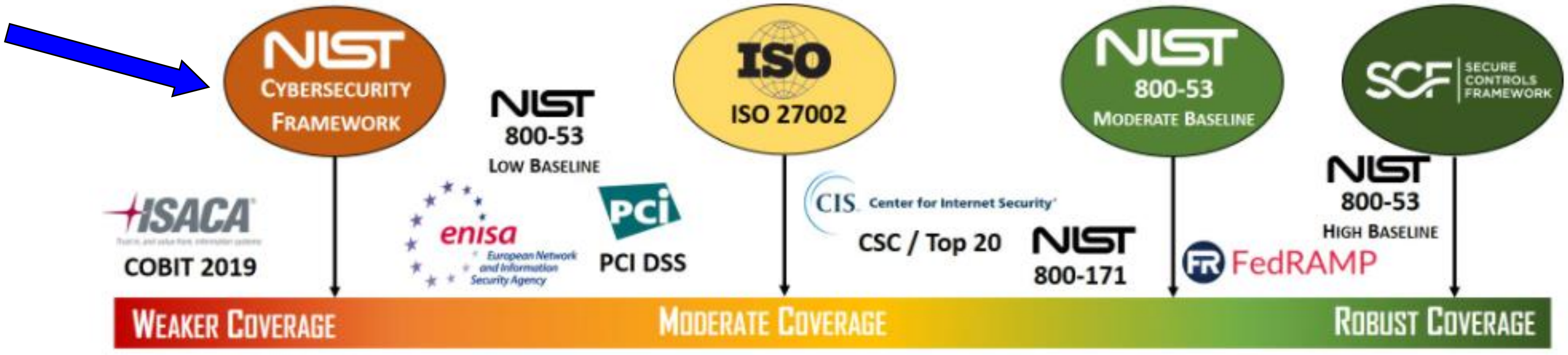
- Recover planning
- Improvements
- Communications

From process view, cybersecurity starts from understanding the organization, its mission, its risk tolerance. Part of this is understanding the organization's role in critical infrastructure. These are used to define roles, responsibilities, policies, and processes. Cybersecurity is realized as technical controls, monitoring, and planned responses. The processes are reviewed and improved based on experience.

Which framework is right for my business?

- **NIST Cybersecurity Framework** ***vs*** **ISO 27002** ***vs*** **NIST 800-53** ***vs*** **Secure Controls Framework**

- It is important to understand that ***picking a cybersecurity framework is more of a business decision and less of a technical decision***. Realistically, the process of selecting a cybersecurity framework must be driven by a fundamental understanding of what your organization needs to comply with from a statutory, regulatory and contractual perspective, since that understanding establishes the *minimum* set of requirements necessary to **(1)** not be considered negligent with reasonable expectations for security & privacy; **(2)** comply with applicable laws, regulations and contracts; and **(3)** implement the proper controls to secure your systems, applications and processes from reasonable threats. This understanding makes it pretty easy to determine where on the "framework spectrum" (shown below) you need to focus for selecting a set of cybersecurity principles to follow. This process generally leads to selecting either the NIST Cybersecurity Framework, ISO 27002 or NIST 800-53 as a starting point:

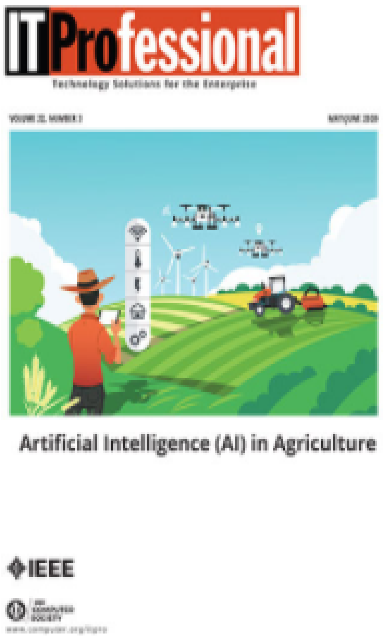


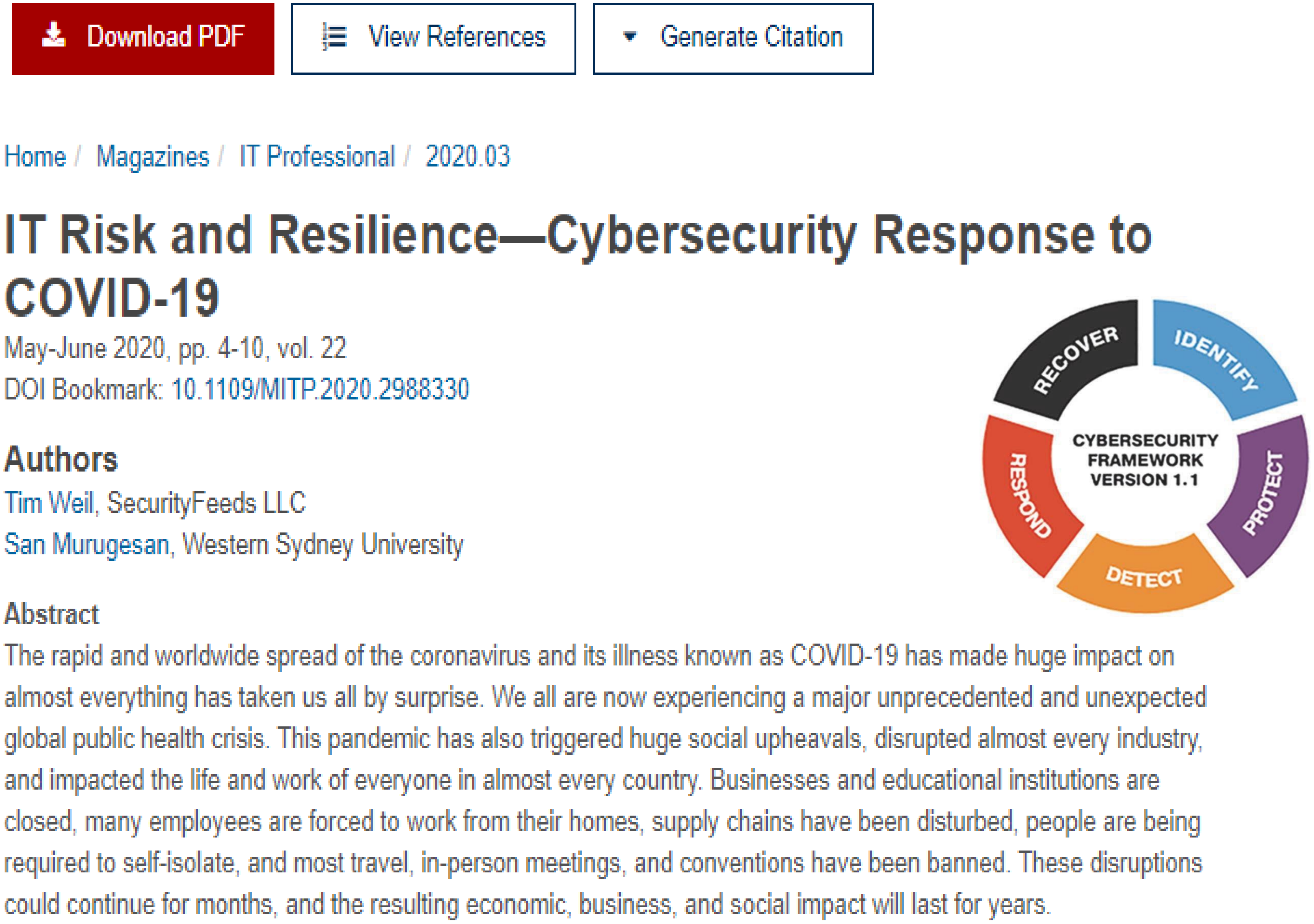
https://www.complianceforge.com/faq/nist-800-53-vs-iso-27002-vs-nist-csf.html

Table of Contents

- Cyberspace – Our Point of Departure
- Information Security Management Models
- Frameworks for Risk Management
- COVID Smackdown – NIST CSF vs Big Scary Monsters
- Random Cybersecurity Attack Simulation Model (RCSM)
- References + Q&A

Global transformation caused by COVID-19


IT Professional
Technology Solutions for the Enterprise
Artificial Intelligence (AI) in Agriculture
IEEE


Download PDF
View References
Generate Citation
Home / Magazines / IT Professional / 2020.03
RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

IT Risk and Resilience—Cybersecurity Response to COVID-19

May-June 2020, pp. 4-10, vol. 22

DOI Bookmark: 10.1109/MITP.2020.2988330

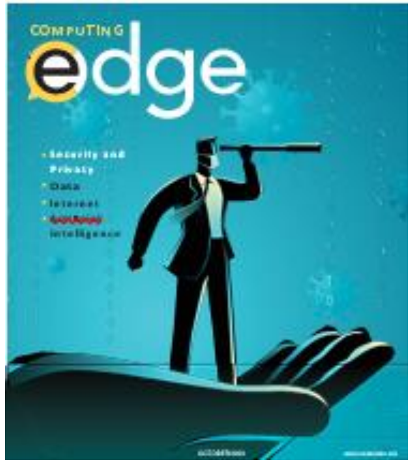
Authors

Tim Weil, SecurityFeeds LLC

San Murugesan, Western Sydney University

Abstract

The rapid and worldwide spread of the coronavirus and its illness known as COVID-19 has made huge impact on almost everything has taken us all by surprise. We all are now experiencing a major unprecedented and unexpected global public health crisis. This pandemic has also triggered huge social upheavals, disrupted almost every industry, and impacted the life and work of everyone in almost every country. Businesses and educational institutions are closed, many employees are forced to work from their homes, supply chains have been disturbed, people are being required to self-isolate, and most travel, in-person meetings, and conventions have been banned. These disruptions could continue for months, and the resulting economic, business, and social impact will last for years.



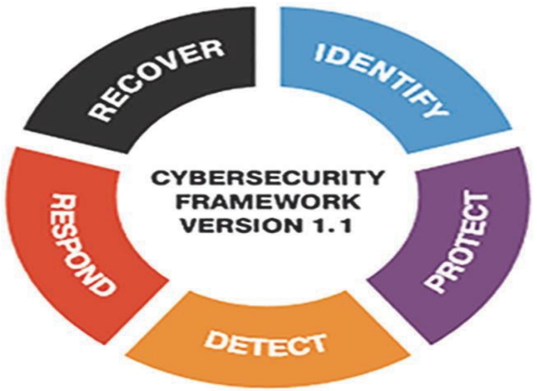
Global transformation caused by COVID-19

Industry	Response/Impact	Response	Underlying technology/ operation
Education	Widespread closure of educational institutions; access to labs is restricted; projects have been mothballed; and fieldwork interrupted	Virtual learning environment (online teaching, presentation, assessment, and consultation); convocation online	Online video conferencing software, virtual labs on cloud
Healthcare	Overcrowded hospitals, inability to meet the demands on them	Contact tracing, forecasting resource requirements, allotment of scare resources based on a patient's survivability, COVID-19 vaccine development, telehealth (online consultation with a doctor or medical professional); automated diagnosis	AI, ML, cloud computing, chatbot
Business	Closure of business, avoidance ofin-person retail shopping	Adherence to social distancing, services online, work from home	Chatbot, drone delivery, online meeting software, virtual office/desktop, remote access to work
Industry	Closure of business, avoidance of in-person retail shopping	Work from home, remote operations, automation and autonomous operation	Robots, automation, 3-D printing
Retail	Stores closed, only online service, avoidance of retail shopping	Online shopping, home delivery	The Web, online payment, contactless payment
Government	Spike in demands from citizens for assistance, disruption to normal operations	Migration to online services	Cloud, the Web, online meeting application
Entertainment	Entertainment venues (parks, cinema) closed, sports without spectators	Viewing online	Audio and video streaming, virtual reality
Personal life and social interaction	Lockdown	Indoor activities	Phone, audio and video chats, streaming, online gaming
Spirituality and religious practices	Places of worship closed	Online participation, prayers from home, worship through livestream	Audio and video streaming, virtual reality
Conferences	In-person conferences banned; virtual conferences	Online presentation and discussion	Video streaming, virtual conference software

Global transformation caused by COVID-19

https://www.thinkcsc.com/nist-cybersecurity-framework/

COVID-19 Made a NIST Cybersecurity Framework More Critical for Ohio Businesses



The Ohio Data Protection Act

As a refresher, the Ohio Data Protection Act provides businesses that store or transmit personal information a safe harbor in the event they experience a breach. However, you can only qualify if you follow the NIST cybersecurity framework. This Act is a significant step forward for all organizations interested in limiting their liability should a data breach occur. It offers clear steps to organizations on what they must do to qualify for safe harbor under the Act. With or without a pandemic, minimizing risk of liability while simultaneously establishing better protocols to protect your customers and your data is a win-win.

Principals of a NIST-Based Cybersecurity Network

The threat landscape continues to grow more complex. As a result, cyberattacks are more sophisticated than ever. New threats are discovered daily. The NIST framework is designed to help you have a comprehensive cybersecurity strategy in place to protect your organization, your people, your data, and your customers.

The principals of the NIST framework are:

- Use common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors, and uses
- Risk-based
- Based on international standards
- A living document
- Guided by many perspectives – private sector, academia, public sector

Global transformation caused by COVID-19

CYBERSECURITY FRAMEWORK (CSF)

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

CSF Core

What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impact of incidents?

What techniques can restore capabilities?

Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
Protect	Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & Procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**
Detect	Anomalies and Events	**DE.AE**
	Security Continuous Monitoring	**DE.CM**
	Detection Processes	**DE.DP**
Respond	Response Planning	**RS.RP**
	Communications	**RS.CO**
	Analysis	**RS.AN**
	Mitigation	**RS.MI**
	Improvements	**RS.IM**
Recover	Recovery Planning	**RC.RP**
	Improvements	**RC.IM**
	Communications	**RC.CO**

Framework Core is a set of activities, outcomes and references that detail approaches to aspects of cyber security.

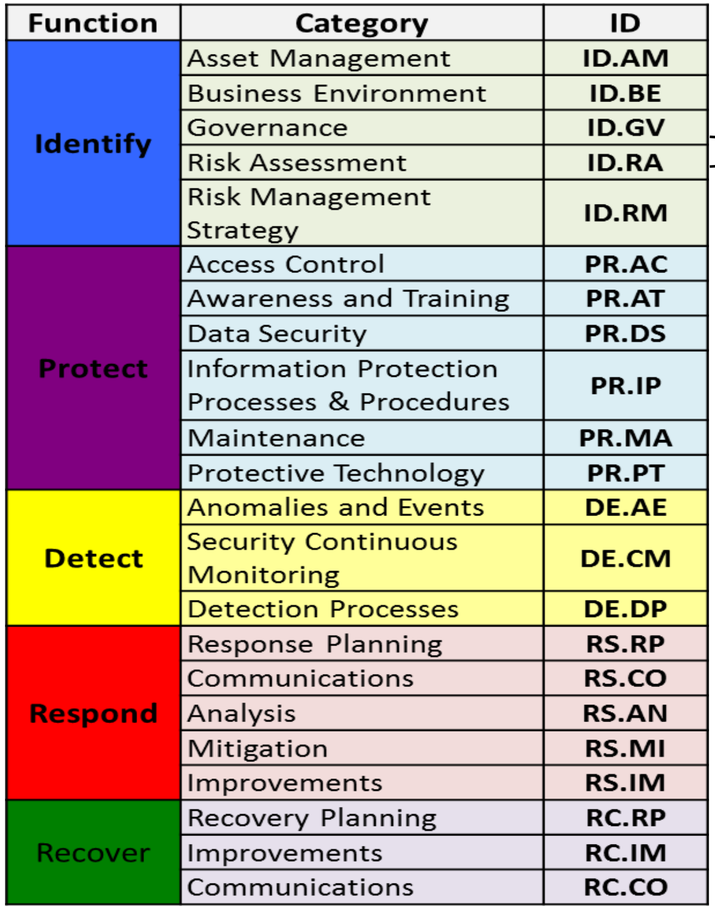
The core comprises five functions, which are subdivided into 22 categories (groups of cyber security outcomes) and 98 subcategories (security controls).

Global transformation caused by COVID-19

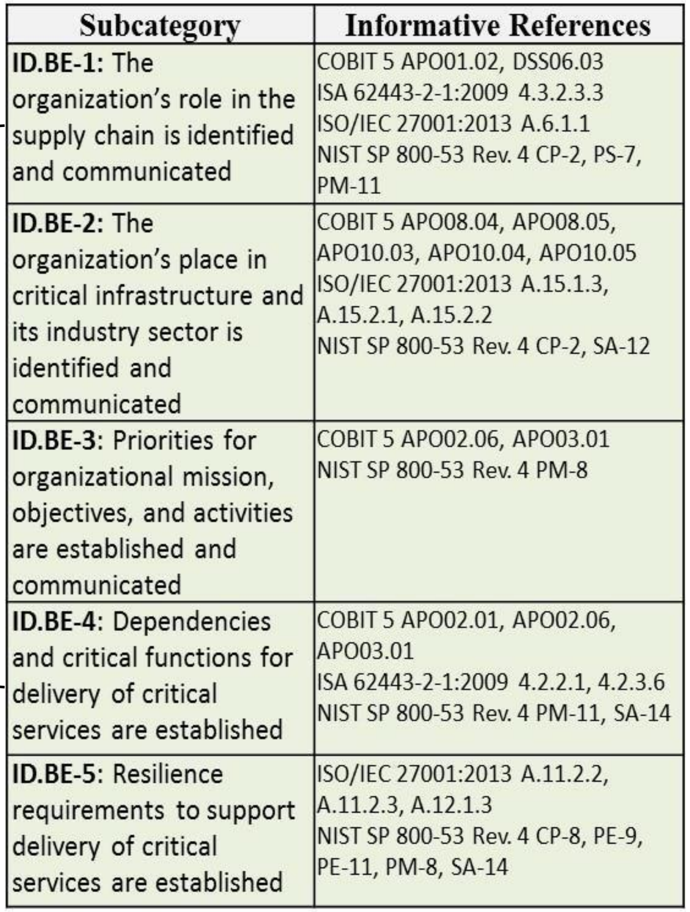
CYBERSECURITY FRAMEWORK (CSF)

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

CSF Core



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO



Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

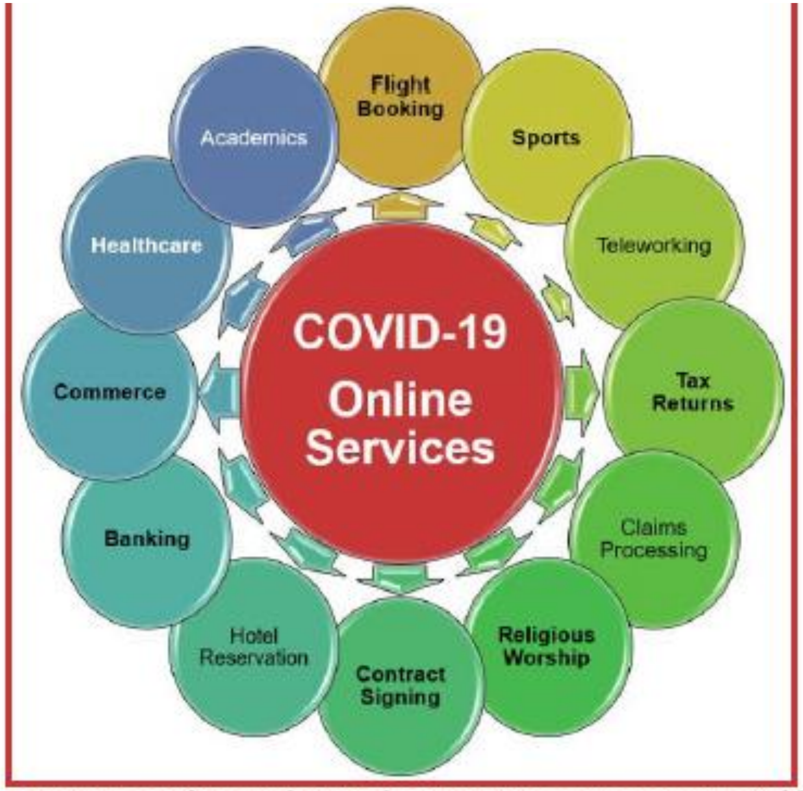
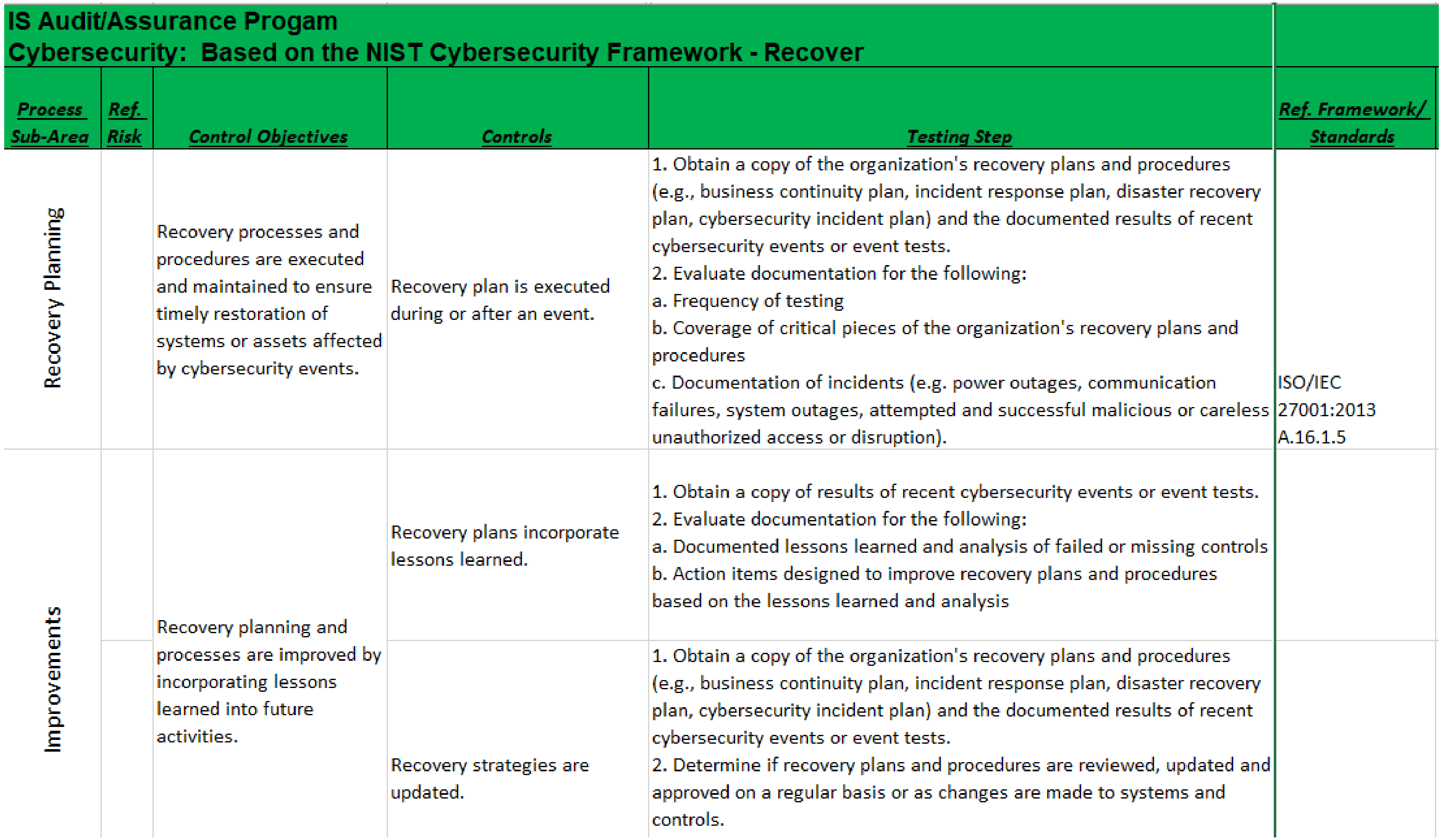


Figure 2: Some online and virtual computing services promoted by COVID-19 induced social distancing.

Global transformation caused by COVID-19 - CYBERSECURITY FRAMEWORK (CSF) - Recover



IS Audit/Assurance Progam
Cybersecurity: Based on the NIST Cybersecurity Framework - Recover

Process Sub-Area	Ref. Risk	Control Objectives	Controls	Testing Step	Ref. Framework/ Standards
Recovery Planning		Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	Recovery plan is executed during or after an event.	1. Obtain a copy of the organization's recovery plans and procedures (e.g., business continuity plan, incident response plan, disaster recovery plan, cybersecurity incident plan) and the documented results of recent cybersecurity events or event tests. 2. Evaluate documentation for the following: a. Frequency of testing b. Coverage of critical pieces of the organization's recovery plans and procedures c. Documentation of incidents (e.g. power outages, communication failures, system outages, attempted and successful malicious or careless unauthorized access or disruption).	ISO/IEC 27001:2013 A.16.1.5
Improvements		Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery plans incorporate lessons learned.	1. Obtain a copy of results of recent cybersecurity events or event tests. 2. Evaluate documentation for the following: a. Documented lessons learned and analysis of failed or missing controls b. Action items designed to improve recovery plans and procedures based on the lessons learned and analysis	
			Recovery strategies are updated.	1. Obtain a copy of the organization's recovery plans and procedures (e.g., business continuity plan, incident response plan, disaster recovery plan, cybersecurity incident plan) and the documented results of recent cybersecurity events or event tests. 2. Determine if recovery plans and procedures are reviewed, updated and approved on a regular basis or as changes are made to systems and controls.	

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

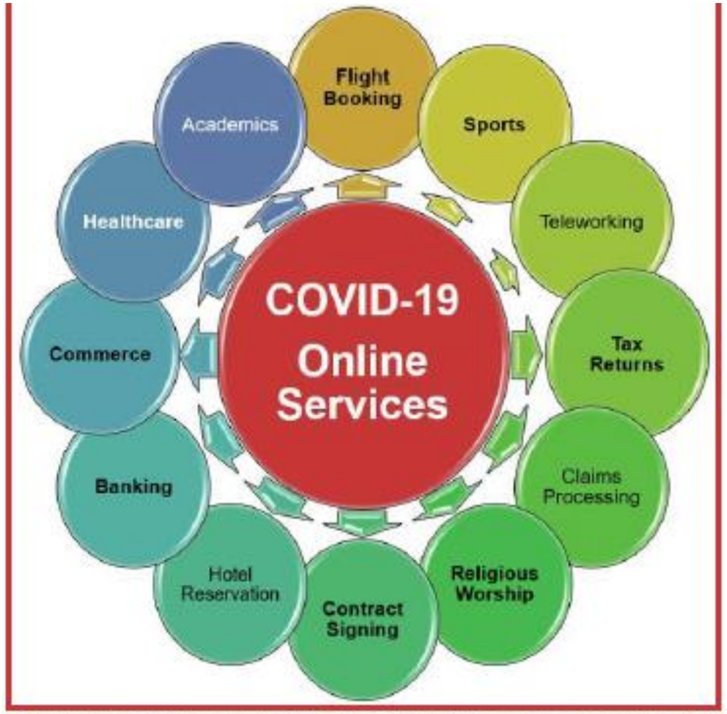
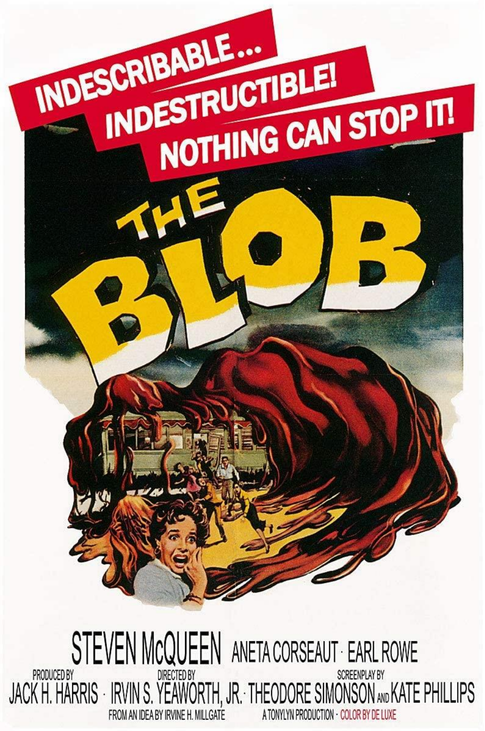


Figure 2: Some online and virtual computing services promoted by COVID-19 induced social distancing.

Big Scary Monsters - Global transformation caused by COVID-19

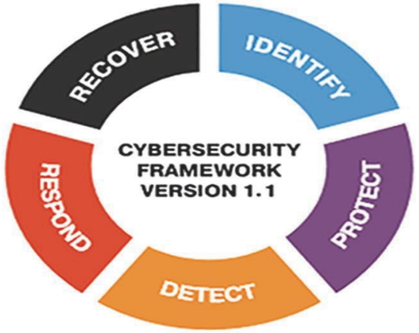

INDESCRIBABLE...
INDESTRUCTIBLE!
NOTHING CAN STOP IT!
THE BLOB
STEVEN McQUEEN ANETA CORSEAUT · EARL ROWE
PRODUCED BY JACK H. HARRIS · DIRECTED BY IRVIN S. YEAWORTH, JR. · SCREENPLAY BY THEODORE SIMONSON AND KATE PHILLIPS
FROM AN IDEA BY IRVINE H. MILLGATE
A TONYLYN PRODUCTION · COLOR BY DE LUXE

The Blob is an amorphous mass of alien goo that appears in the 1958 film of the same name. Appearing as nothing more than a mass of red gelatin, this creature possesses animalistic intelligence, acting purely on the instinct to feed. It feeds on flesh and gains mass as it consumes other creatures

A HORROR HORDE OF CRAWL-AND-CRUSH GIANTS
CLAWING OUT OF THE EARTH
FROM MILE-DEEP
CATACOMBS!
"THEM!"
"This city is under martial law until we annihilate THEM!"
Kill one and two take it's place!
THE AMAZING NEW WARNER BROS. SENSATION!
"THEM!" JAMES WHITMORE . EDMUND GWENN . JOAN WELDON . JAMES ARNESS

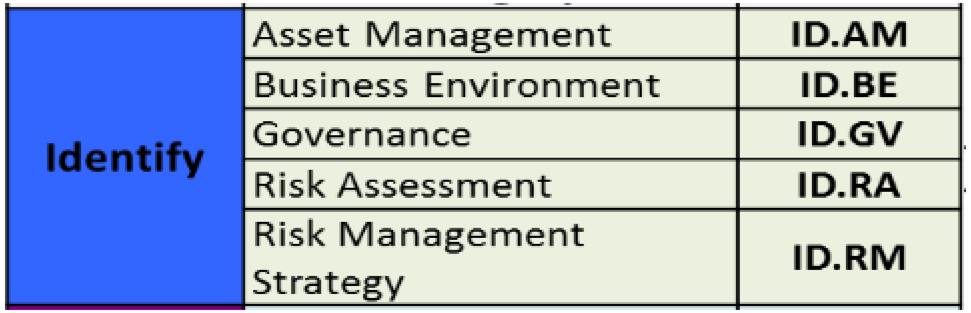
Them While investigating a series of mysterious deaths, Sergeant Ben Peterson finds a young girl agent Robert Graham and scientist Dr. Harold Medford), he discovers that all the incidents are due to giant ants that have been mutated by atomic radiation. Peterson and Graham, with the aid of the military, attempt to find the queen ants and destroy the nests before the danger spreads.

The FUD Factor – Fear, Uncertainty and Doubt

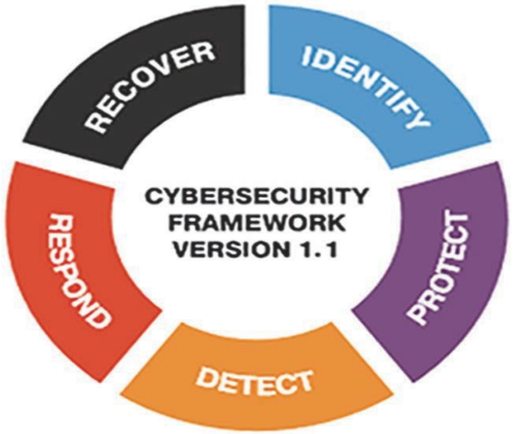


CSF Identify Categories related to COVID-19

A HORROR HORDE OF CRAWL-AND-CRUSH GIANTS
CLAWING OUT OF THE EARTH
FROM MILE-DEEP
CATACOMBS!
"THEM"
"This city is under martial law until we annihilate THEM!"
Kill one and two take it's place!
THE AMAZING NEW WARNER BROS. SENSATION!
"THEM!" JAMES WHITMORE . EDMUND GWENN . JOAN WELDON . JAMES ARNESS

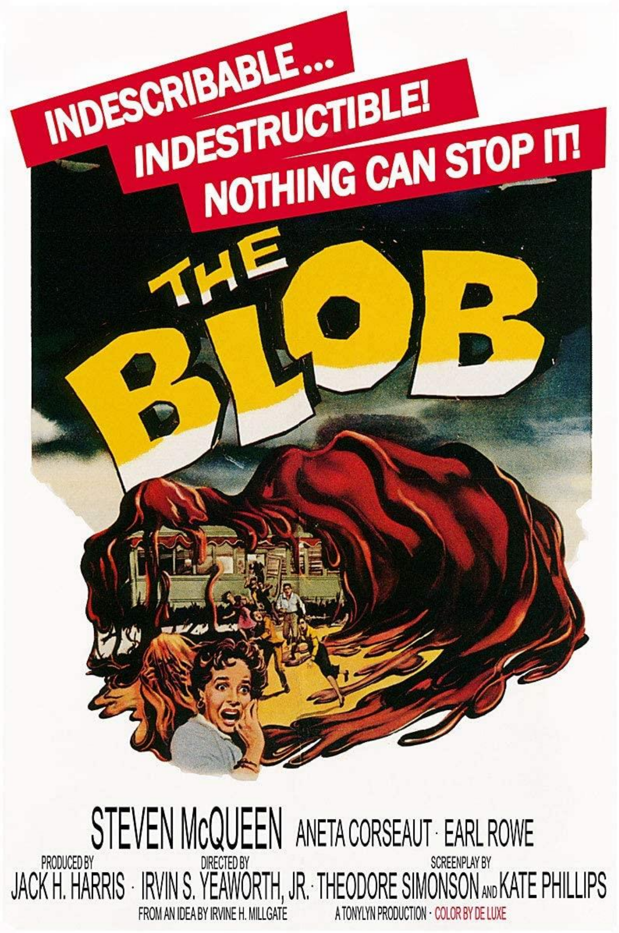


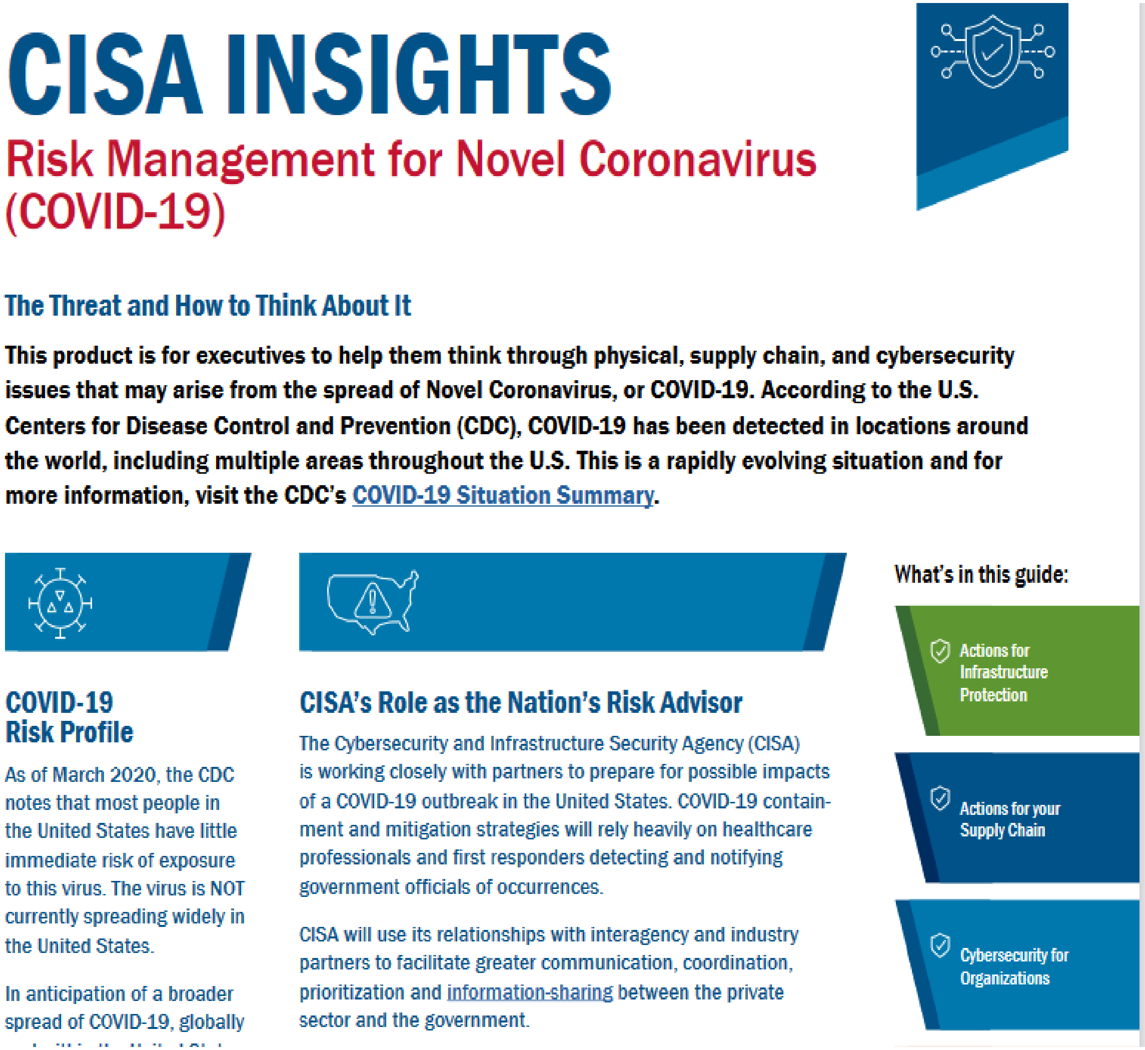
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM



Cybersecurity management response	Online resource
CxO Education (Security Architects Partners)	https://security-architect.com/waking-up-to-the-new-covid-19-cybersecurity-reality/
COVID-19 Joint Acquisition Task Force	https://www.acq.osd.mil/jatf.html
US DHS Cyber and Infrastructure Agency (CISA)	https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf
NIST SP 800-46 Guide to enterprise telework, remote access, and BYOD security	https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

CSF Identify Controls for COVID-19


INDESCRIBABLE...
INDESTRUCTIBLE!
NOTHING CAN STOP IT!
THE BLOB
STEVEN McQUEEN ANETA CORSEAUT · EARL ROWE
PRODUCED BY JACK H. HARRIS · DIRECTED BY IRVIN S. YEAWORTH, JR. · SCREENPLAY BY THEODORE SIMONSON AND KATE PHILLIPS
FROM AN IDEA BY IRVINE H. MILLGATE · A TONYLYN PRODUCTION · COLOR BY DE LUXE



CISA INSIGHTS

Risk Management for Novel Coronavirus (COVID-19)

The Threat and How to Think About It

This product is for executives to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19. According to the U.S. Centers for Disease Control and Prevention (CDC), COVID-19 has been detected in locations around the world, including multiple areas throughout the U.S. This is a rapidly evolving situation and for more information, visit the CDC's COVID-19 Situation Summary.

COVID-19 Risk Profile

As of March 2020, the CDC notes that most people in the United States have little immediate risk of exposure to this virus. The virus is NOT currently spreading widely in the United States.

In anticipation of a broader spread of COVID-19, globally

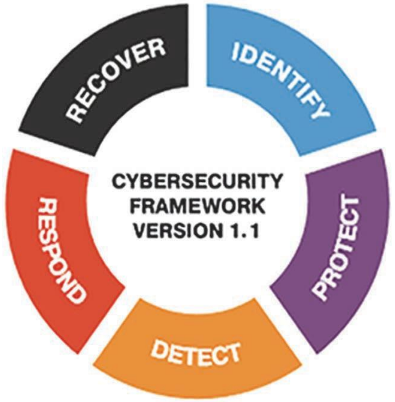
CISA's Role as the Nation's Risk Advisor

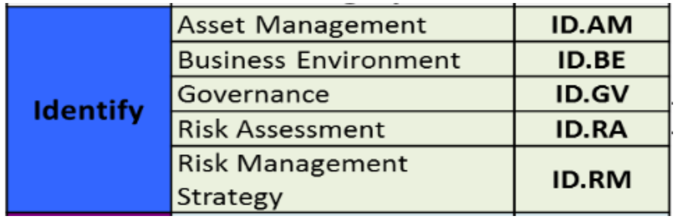
The Cybersecurity and Infrastructure Security Agency (CISA) is working closely with partners to prepare for possible impacts of a COVID-19 outbreak in the United States. COVID-19 containment and mitigation strategies will rely heavily on healthcare professionals and first responders detecting and notifying government officials of occurrences.

CISA will use its relationships with interagency and industry partners to facilitate greater communication, coordination, prioritization and information-sharing between the private sector and the government.

What's in this guide:

- Actions for Infrastructure Protection
- Actions for your Supply Chain
- Cybersecurity for Organizations

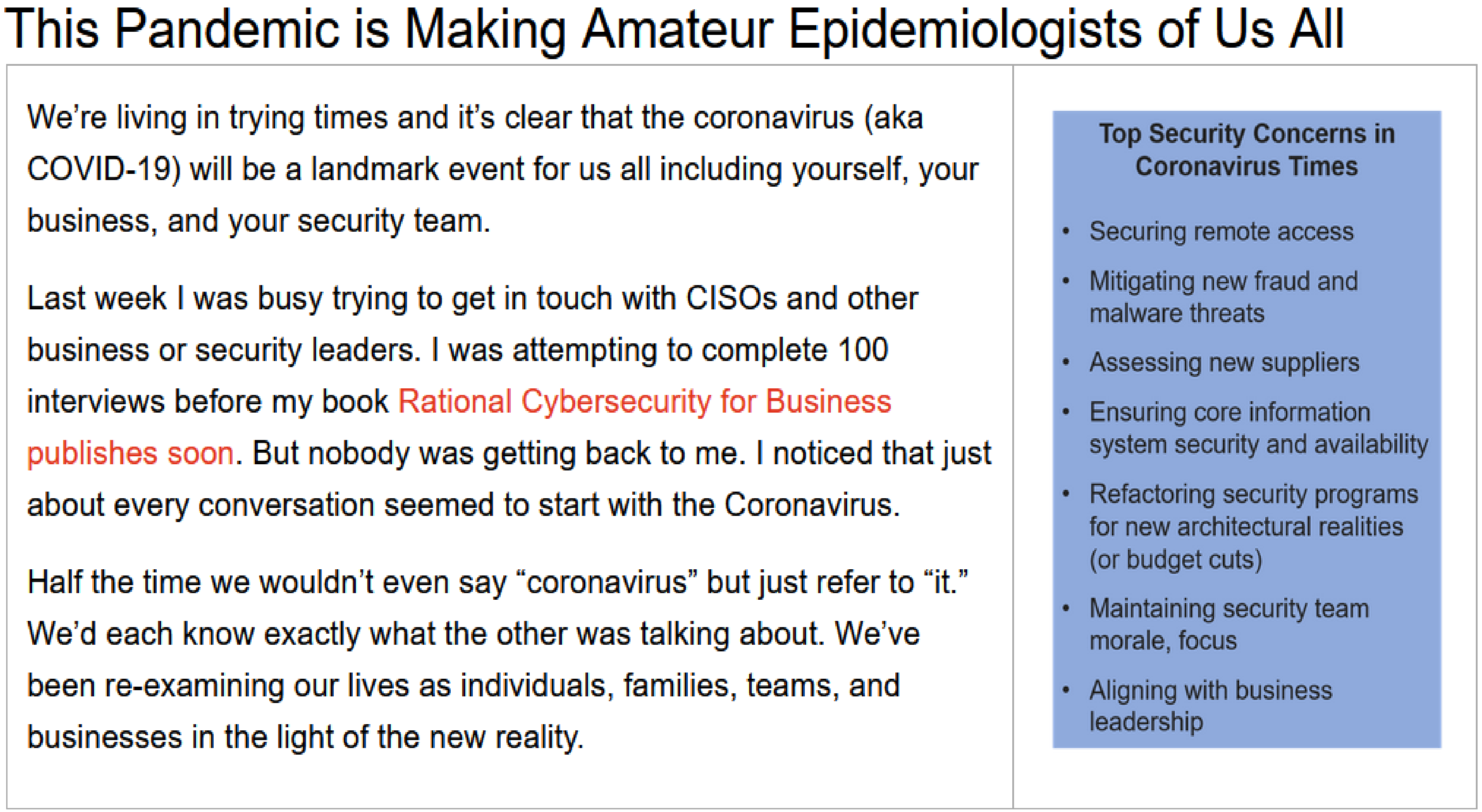




Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM

https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf

CSF Protect Controls for COVID-19 – https://security-architect.com/waking-up-to-the-new-covid-19-cybersecurity-reality/



This Pandemic is Making Amateur Epidemiologists of Us All

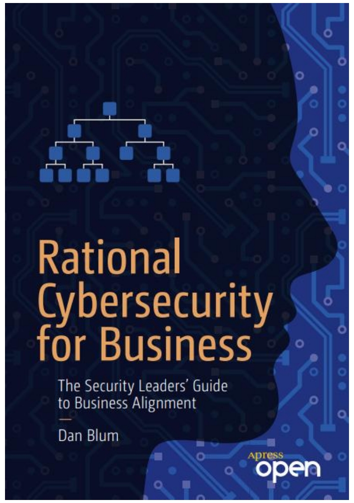
We're living in trying times and it's clear that the coronavirus (aka COVID-19) will be a landmark event for us all including yourself, your business, and your security team.

Last week I was busy trying to get in touch with CISOs and other business or security leaders. I was attempting to complete 100 interviews before my book Rational Cybersecurity for Business publishes soon. But nobody was getting back to me. I noticed that just about every conversation seemed to start with the Coronavirus.

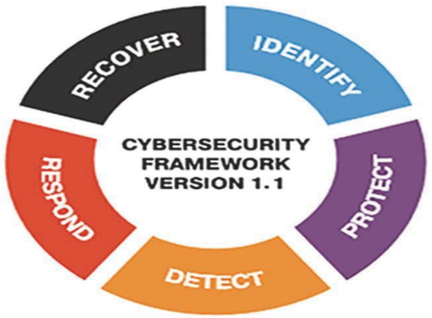
Half the time we wouldn't even say "coronavirus" but just refer to "it." We'd each know exactly what the other was talking about. We've been re-examining our lives as individuals, families, teams, and businesses in the light of the new reality.

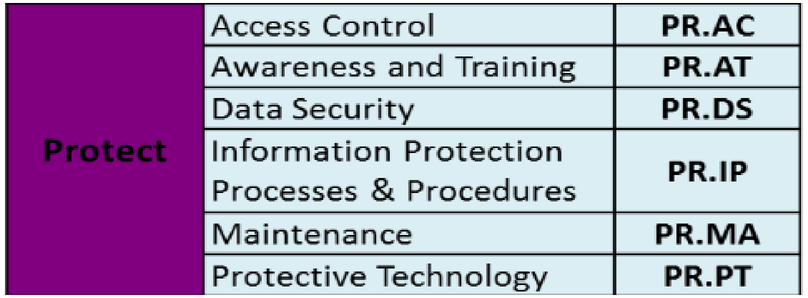
Top Security Concerns in Coronavirus Times

- Securing remote access
- Mitigating new fraud and malware threats
- Assessing new suppliers
- Ensuring core information system security and availability
- Refactoring security programs for new architectural realities (or budget cuts)
- Maintaining security team morale, focus
- Aligning with business leadership



Rational Cybersecurity for Business
The Security Leaders' Guide to Business Alignment
Dan Blum
Apress open



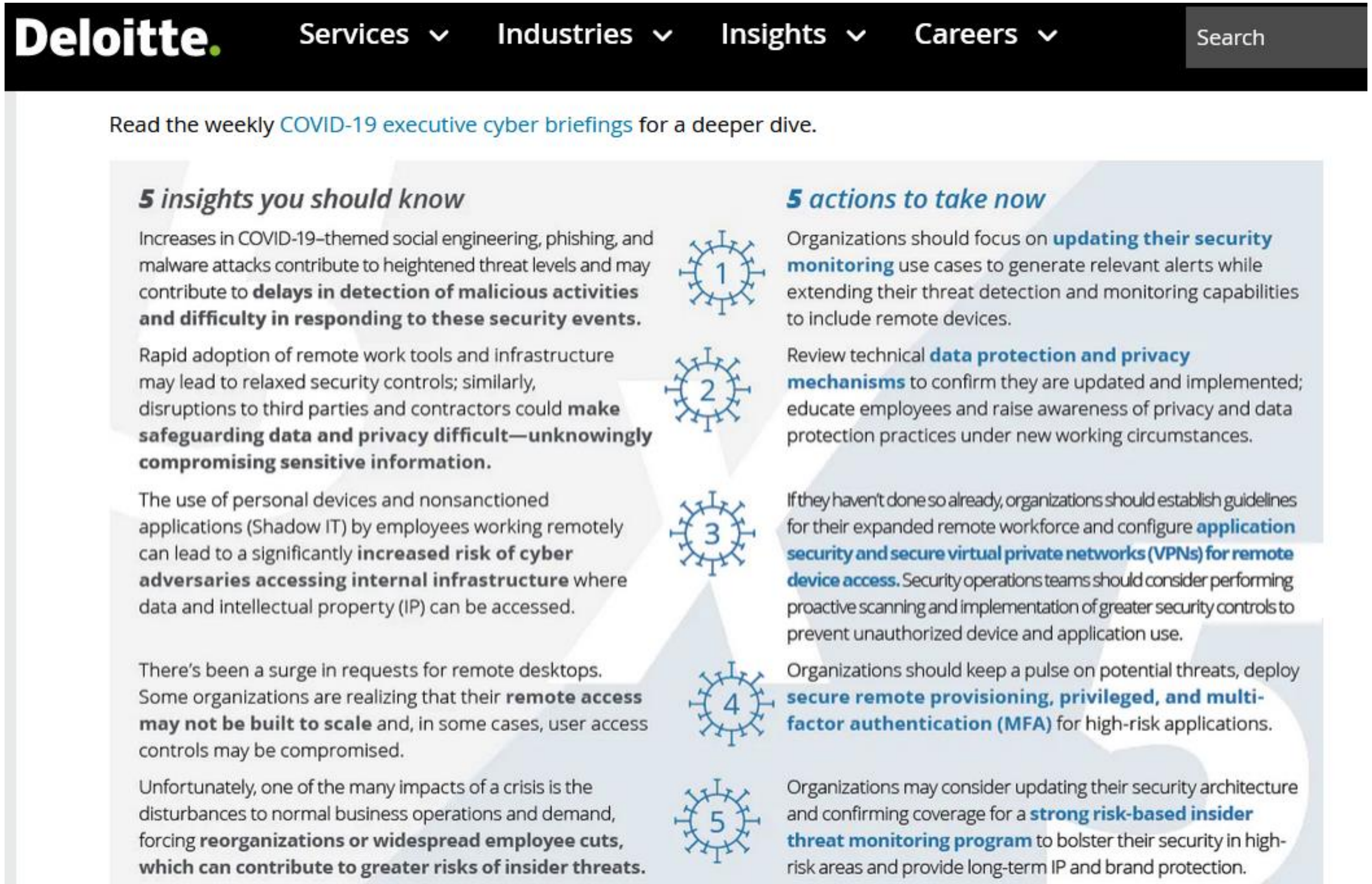


Protect	Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & Procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**

Rational Cybersecurity for Business The Security Leaders' Guide to Business Alignment Authors: Dan Blum https://www.apress.com/us/book/9781484259511

CSF Protect Controls for COVID-19 –

https://www2.deloitte.com/us/en/pages/risk/articles/5-actions-insights-cyber-security-privacy-covid-19.html



Read the weekly COVID-19 executive cyber briefings for a deeper dive.

5 insights you should know

Increases in COVID-19–themed social engineering, phishing, and malware attacks contribute to heightened threat levels and may contribute to **delays in detection of malicious activities and difficulty in responding to these security events.**

Rapid adoption of remote work tools and infrastructure may lead to relaxed security controls; similarly, disruptions to third parties and contractors could **make safeguarding data and privacy difficult—unknowingly compromising sensitive information.**

The use of personal devices and nonsanctioned applications (Shadow IT) by employees working remotely can lead to a significantly **increased risk of cyber adversaries accessing internal infrastructure** where data and intellectual property (IP) can be accessed.

There's been a surge in requests for remote desktops. Some organizations are realizing that their **remote access may not be built to scale** and, in some cases, user access controls may be compromised.

Unfortunately, one of the many impacts of a crisis is the disturbances to normal business operations and demand, forcing **reorganizations or widespread employee cuts, which can contribute to greater risks of insider threats.**

5 actions to take now

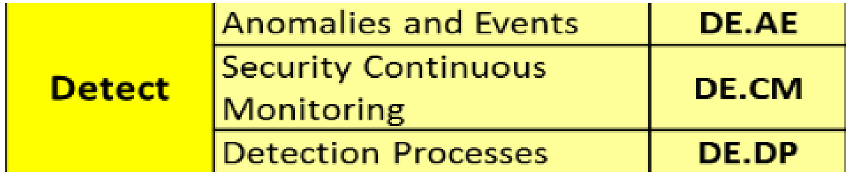
1 Organizations should focus on **updating their security monitoring** use cases to generate relevant alerts while extending their threat detection and monitoring capabilities to include remote devices.

2 Review technical **data protection and privacy mechanisms** to confirm they are updated and implemented; educate employees and raise awareness of privacy and data protection practices under new working circumstances.

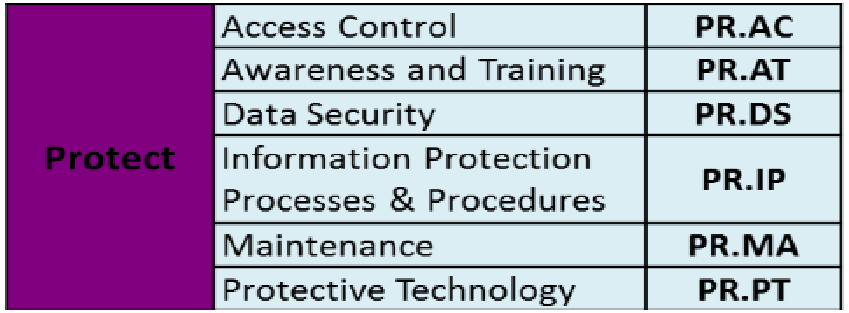
3 If they haven't done so already, organizations should establish guidelines for their expanded remote workforce and configure **application security and secure virtual private networks (VPNs) for remote device access.** Security operations teams should consider performing proactive scanning and implementation of greater security controls to prevent unauthorized device and application use.

4 Organizations should keep a pulse on potential threats, deploy **secure remote provisioning, privileged, and multi-factor authentication (MFA)** for high-risk applications.

5 Organizations may consider updating their security architecture and confirming coverage for a **strong risk-based insider threat monitoring program** to bolster their security in high-risk areas and provide long-term IP and brand protection.



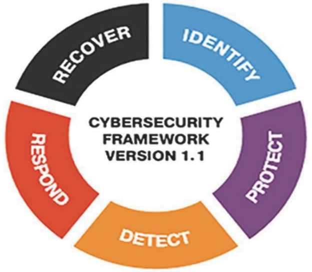
Detect	Anomalies and Events	**DE.AE**
	Security Continuous Monitoring	**DE.CM**
	Detection Processes	**DE.DP**



Protect	Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & Procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**

Exposure

- Phishing and Malware
- Remote Work Tools
- Shadow IT
- Remote Desktops
- Personnel Disruption



Remediation

- Security Monitoring
- Data Protection and Privacy
- Application Security / VPN for Telework
- Secure Privileged Access Management
- Risk-based Threat Monitoring Program

CSF Detect Controls for COVID-19 - Threats and Vulnerabilities

A HORROR HORDE OF CRAWL-AND-CRUSH GIANTS
CLAWING OUT OF THE EARTH
FROM MILE-DEEP
CATACOMBS!
"THEM"
"This city is under martial law until we annihilate THEM!"
Kill one and two take it's place!
THE AMAZING NEW WARNER BROS. SENSATION!
"THEM!" JAMES WHITMORE . EDMUND GWENN . JOAN WELDON . JAMES ARNESS

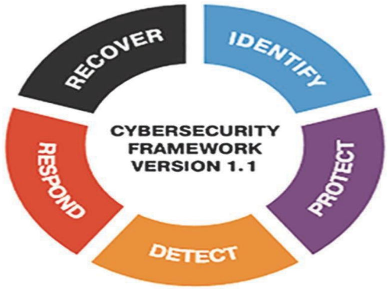
Threats and Vulnerabilities provides industry example of the CSF Protect / Detect examples listed here. They include: –

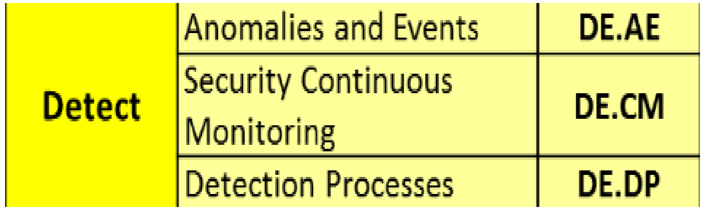
ZOOM bombing - Security and privacy vulnerabilities in teleconferencing software allow trolling hackers to intercept authentication credentials and inject objectionable content

COVID-19 phishing attacks – As reported in FBI bulletins there were fake, malicious emails that appeared to be from the Center for Disease Control (CDC). They contained malware attachments, or aimed to hijack user credentials.

Malware – An example of malware is a Corona Trojan overwriting master boot record (mbr) and disabling hard disk storage. Ransomware attacks on healthcare systems have been escalating during the pandemic.

Network Availability –While performance of core communication networks and clouds remained satisfactory despite substantial increase in traffic, some collaborative applications faced spikes in service outages



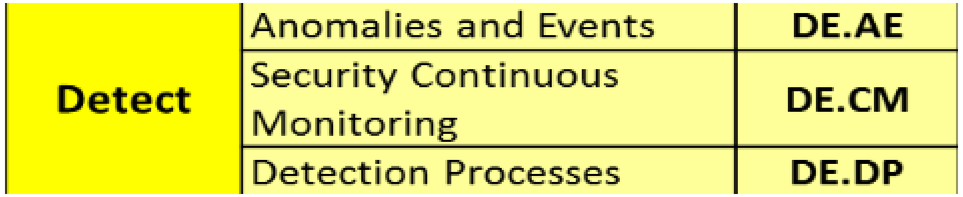


Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP

Threats and Vulnerabilities	Online Resource
ZOOM bombing	https://delta.ncsu.edu/news/2020/04/02/zoom-security-and-privacy/
Spyware and Phishing	https://www.coalfire.com/The-Coalfire-Blog/March-2020/COVID-19-incites-cyber-crimes-of-opportunity
Malware and Phishing	https://www.webarxsecurity.com/covid-19-cyber-attacks/
Health Check – ISPs, Cloud Providers, UCaaS During Pandemic_	https://www.networkworld.com/article/3534130/covid-19-weekly-health-check-of-isps-cloud-providers-and-conferencing-services.html

CSF Detect Controls for COVID-19

A HORROR HORDE OF CRAWL-AND-CRUSH GIANTS
CLAWING OUT OF THE EARTH
FROM MILE-DEEP
CATACOMBS!
"THEM"
"This city is under martial law until we annihilate THEM!"
Kill one and two take it's place!
THE AMAZING NEW WARNER BROS. SENSATION!
"THEM!" JAMES WHITMORE . EDMUND GWENN . JOAN WELDON . JAMES ARNESS



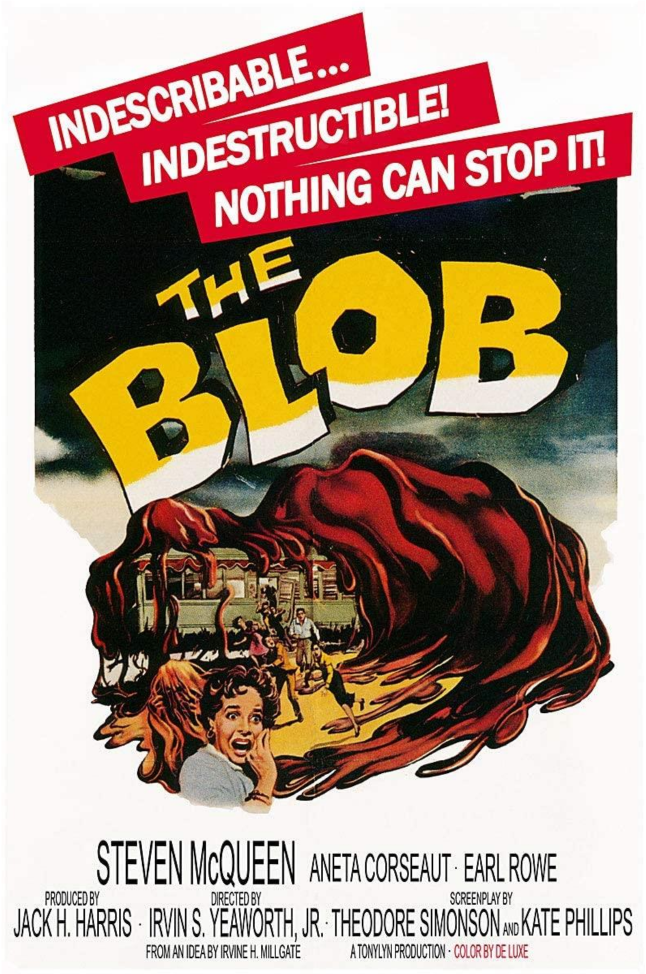
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP

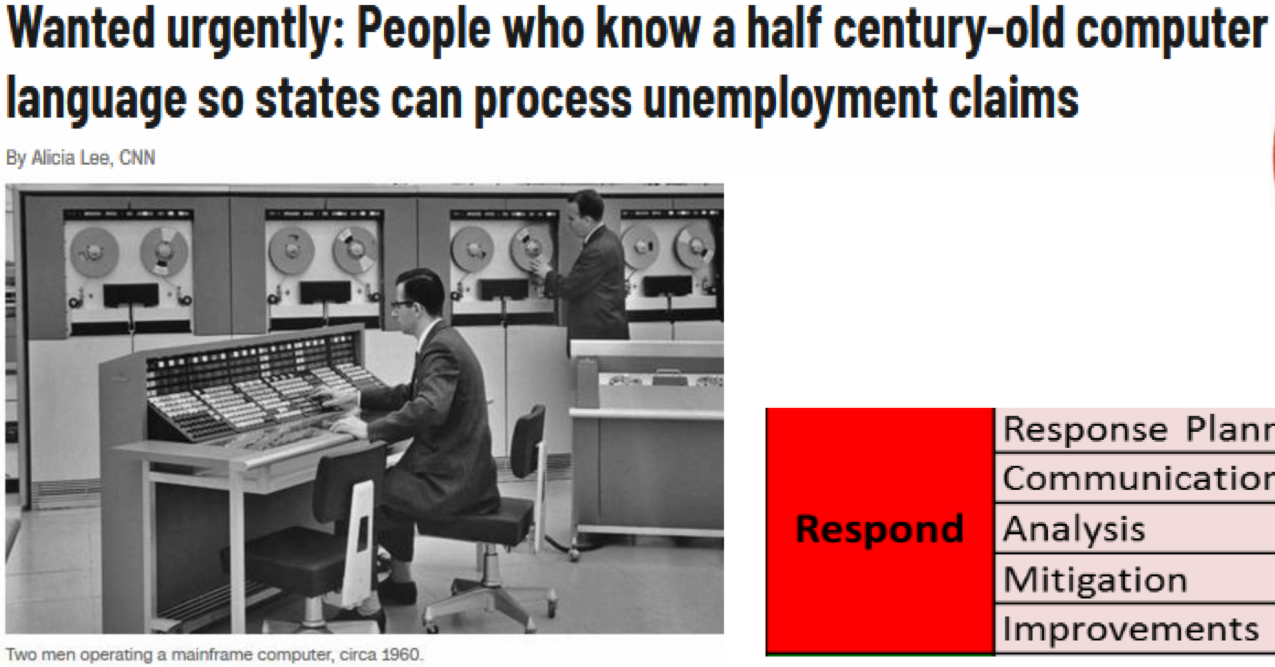
RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

Date	Description of cyber attack	Type of attack
4/8/2020	The exposure to compromised e-commerce websites is greater than ever. 26% increase in web skimming in March.	Malware
4/8/2020	‘Latest vaccine release for Corona-virus (COVID-19)’ mall spam spreads NanocoreRAT malware	Malware
4/8/2020	NCSC Advisory: COVID-19 exploited by malicious cyber actors	Social Engineering
4/7/2020	Fake COVID19 website is spreading FirebirdRAT via fake DHL emails	Malware
4/6/2020	Rush to adopt online learning under COVID-19 exposes schools to cyberattacks	Zoom bombing
4/4/2020	Sophisticated COVID-19–Based Phishing Attacks Leverage PDF Attachments and SaaS to Bypass Defenses	Phishing, Malware
4/4/2020	CDC Warns of COVID-19-Related Phone Scams, Phishing Attacks	Phishing

https://www.webarxsecurity.com/covid-19-cyber-attacks/

CSF Respond Controls for COVID-19

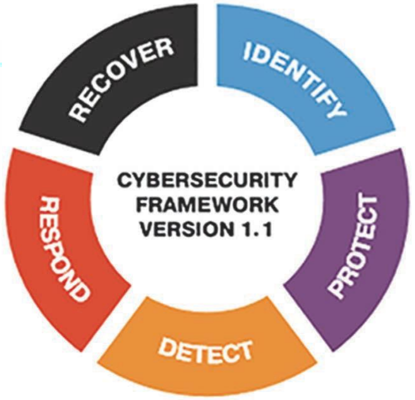

INDESCRIBABLE...
INDESTRUCTIBLE!
NOTHING CAN STOP IT!
THE BLOB
STEVEN McQUEEN ANETA CORSEAUT · EARL ROWE
PRODUCED BY JACK H. HARRIS · DIRECTED BY IRVIN S. YEAWORTH, JR. · SCREENPLAY BY THEODORE SIMONSON AND KATE PHILLIPS
FROM AN IDEA BY IRVINE H. MILLGATE
A TONYLYN PRODUCTION · COLOR BY DE LUXE

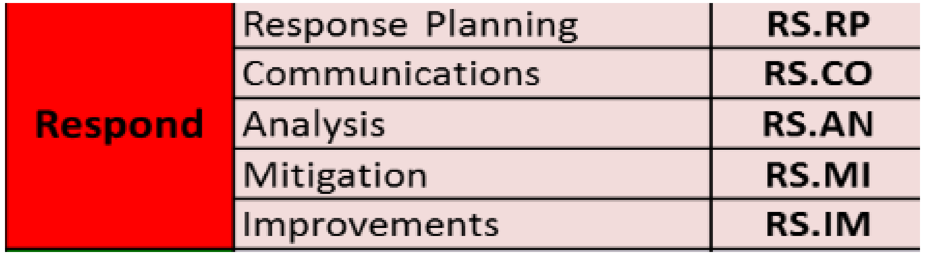


Wanted urgently: People who know a half century-old computer language so states can process unemployment claims

By Alicia Lee, CNN

Two men operating a mainframe computer, circa 1960.



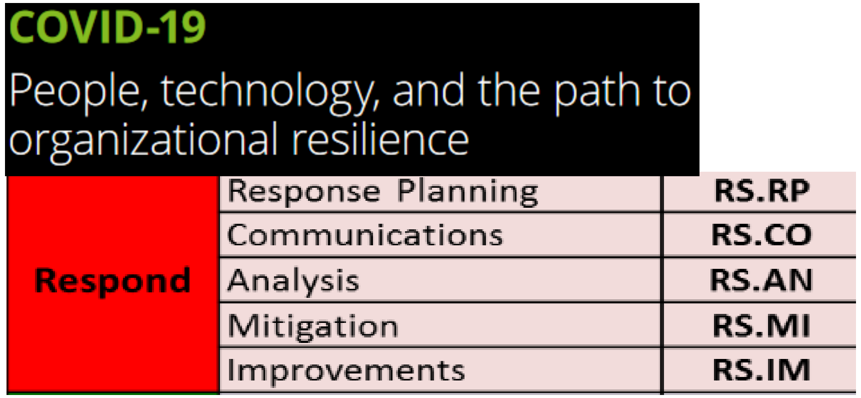


Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM

Cybersecurity risk mitigations	Online resource
Organizational resilience (Deloitte)	https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/about-deloitte/CoronaVirus_POV_People%20Technology%20Path_Central_Europe.pdf
Legacy Software (COBOL) Supporting Financial Systems	https://www.cnn.com/2020/04/08/business/coronavirus-cobol-programmers-new-jersey-trnd/index.html
Fired Americans Send Unemployment Websites Crashing Down	https://www.bloomberg.com/news/articles/2020-03-25/fired-americans-send-state- unemployment-websites-crashing-down

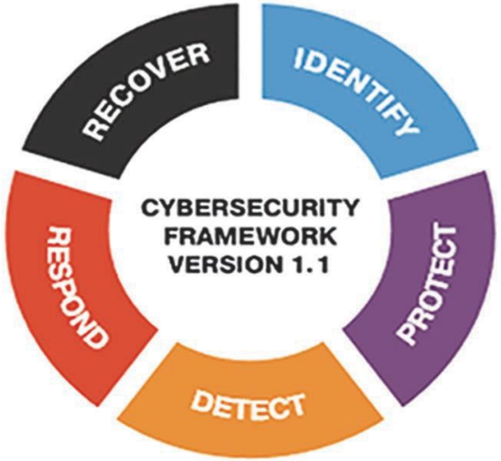
CSF Recover Controls for COVID-19

A HORROR HORDE OF CRAWL-AND-CRUSH GIANTS
CLAWING OUT OF THE EARTH
FROM MILE-DEEP
CATACOMBS!
"THEM"
"This city is under martial law until we annihilate THEM!"
Kill one and two take it's place!
THE AMAZING NEW WARNER BROS. SENSATION!
"THEM!" JAMES WHITMORE . EDMUND GWENN . JOAN WELDON . JAMES ARNESS


COVID-19

People, technology, and the path to organizational resilience

Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM



› **Response strategy:**

- review BC/disaster recovery plans;
- establish a crisis management office;
- develop a communications plan.

› Personnel management (health and safety):

○ - enforce precautionary measures and revisit sick leave policies;

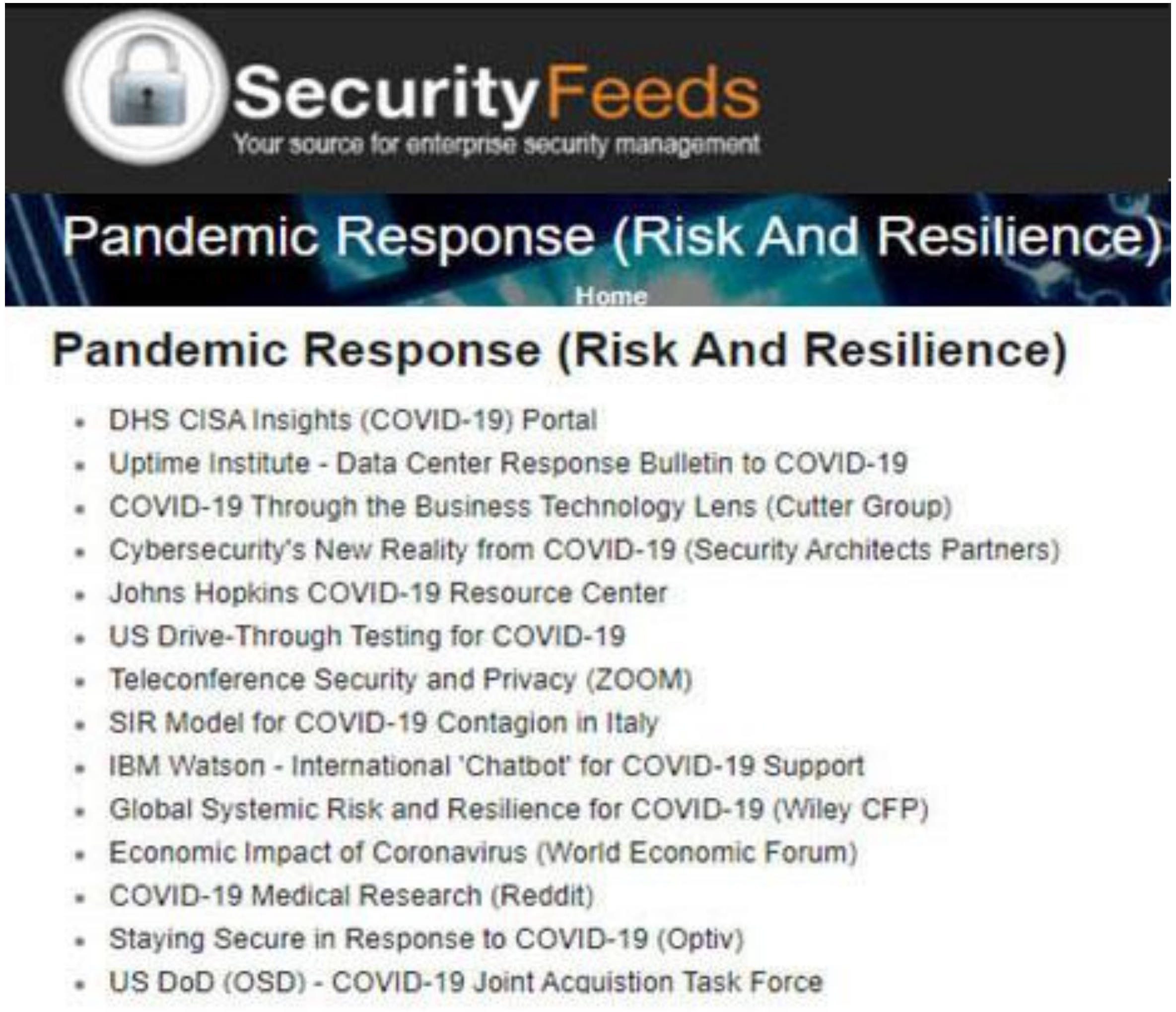
○ - review/amend policies for remote work, including guidelines on travel;

○ plan for absenteeism.

› **Continuity of operation:**

- rationalize technology projects and portfolios;
- equip your connectivity, security, and infrastructure for new traffic and use patterns;
- be ready for disruptions in your business and technology ecosystem.

CSF Recover Controls for COVID-19 – https://www.securityfeeds.us/pandemic-response-risk-and-resilience


SecurityFeeds

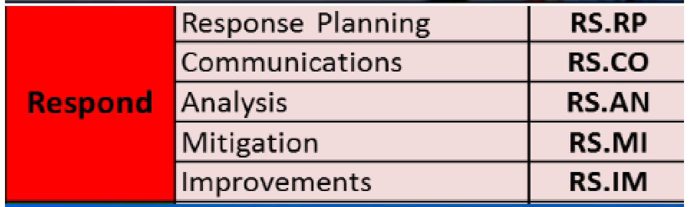
Your source for enterprise security management

Pandemic Response (Risk And Resilience)

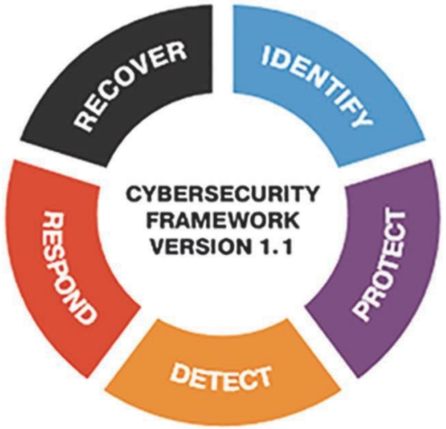
Home

Pandemic Response (Risk And Resilience)

- DHS CISA Insights (COVID-19) Portal
- Uptime Institute - Data Center Response Bulletin to COVID-19
- COVID-19 Through the Business Technology Lens (Cutter Group)
- Cybersecurity's New Reality from COVID-19 (Security Architects Partners)
- Johns Hopkins COVID-19 Resource Center
- US Drive-Through Testing for COVID-19
- Teleconference Security and Privacy (ZOOM)
- SIR Model for COVID-19 Contagion in Italy
- IBM Watson - International 'Chatbot' for COVID-19 Support
- Global Systemic Risk and Resilience for COVID-19 (Wiley CFP)
- Economic Impact of Coronavirus (World Economic Forum)
- COVID-19 Medical Research (Reddit)
- Staying Secure in Response to COVID-19 (Optiv)
- US DoD (OSD) - COVID-19 Joint Acquistion Task Force



Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM

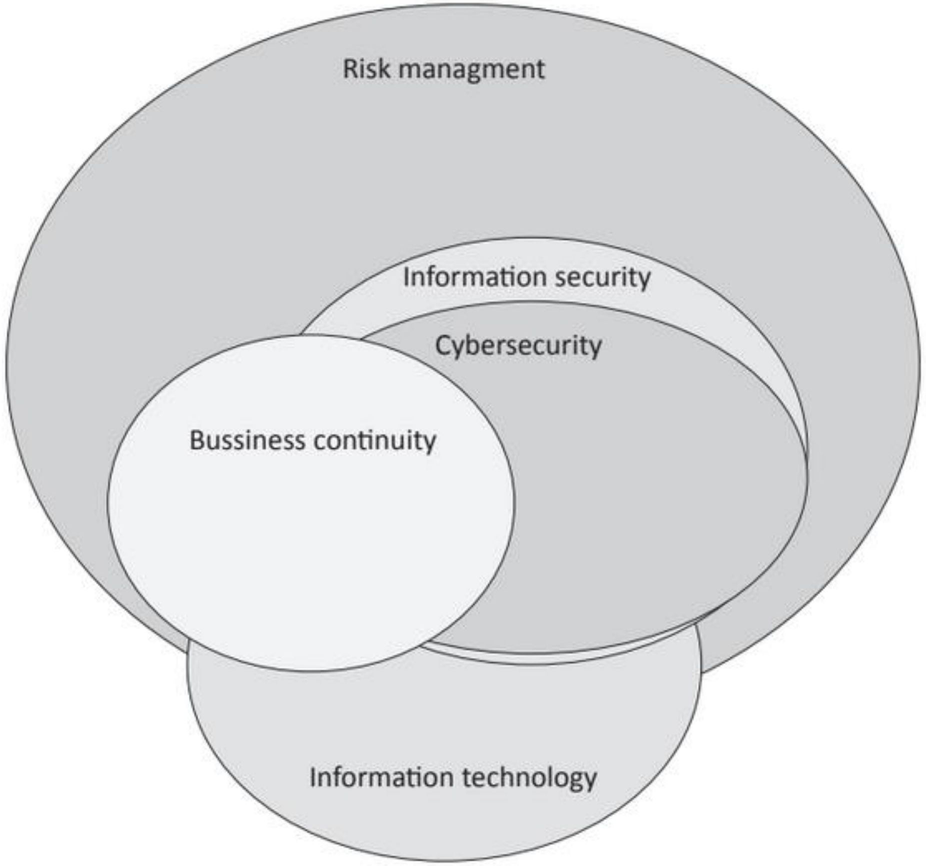


Steve fends off the encroaching Blob with a fire extinguisher, which leads to the discovery that the Blob hates the cold. Steve relays this info to the police, and soon the people of Downingtown band together to take down the Blob.

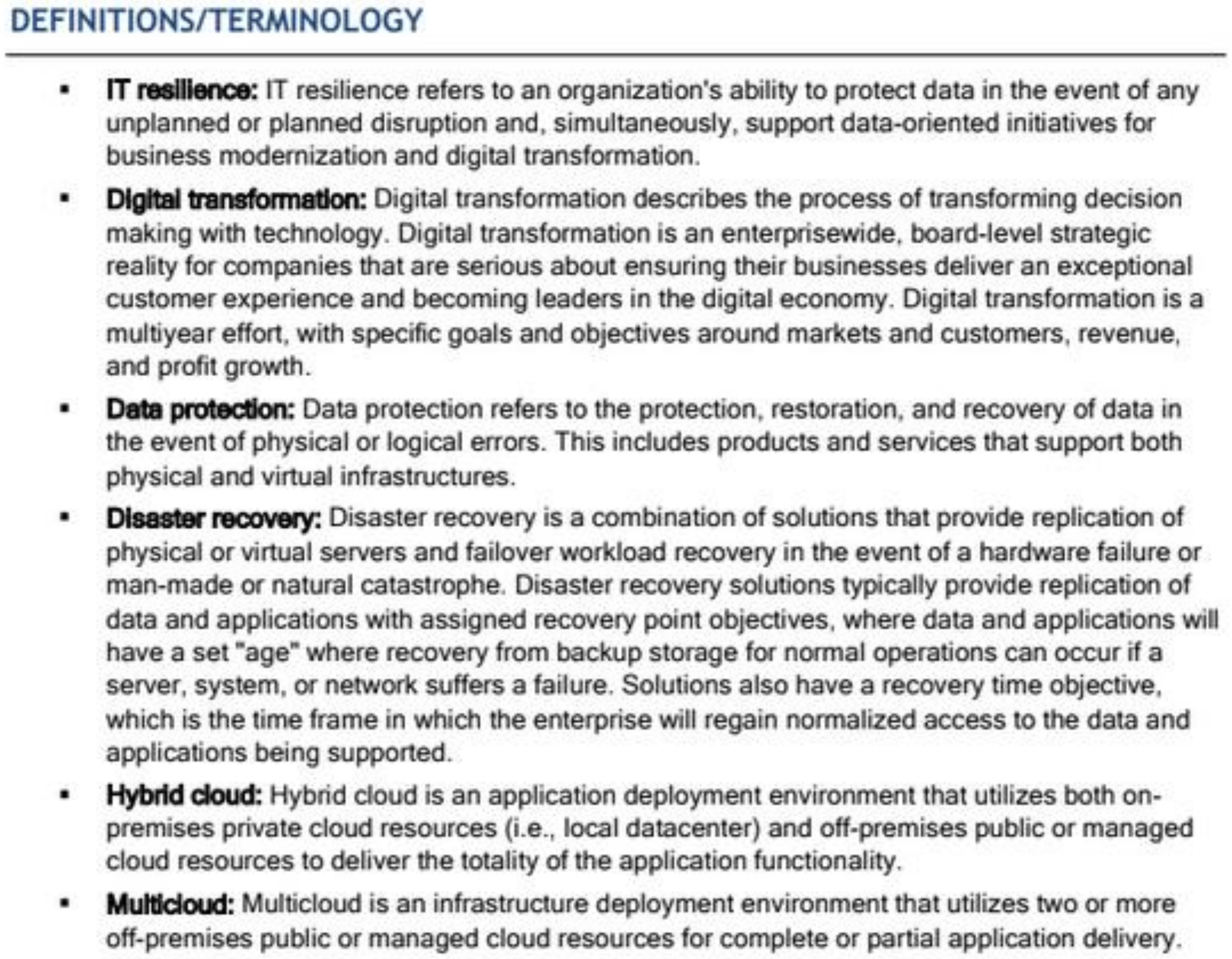
There’s no way to kill the Blob, so the Air Force stuffs it in a giant box and dumps it in the Arctic.

Recovery and Resilience – IT Context for Business Continuity

2.3 Where does business continuity belong?

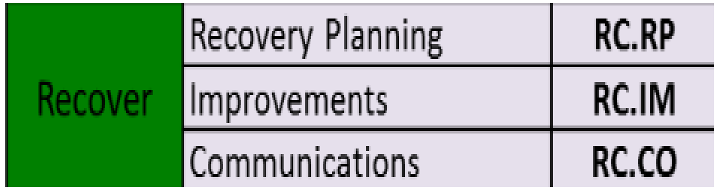


“”Becoming Resilient ” Dejan Kosutic



DEFINITIONS/TERMINOLOGY

- **IT resilience:** IT resilience refers to an organization's ability to protect data in the event of any unplanned or planned disruption and, simultaneously, support data-oriented initiatives for business modernization and digital transformation.
- **Digital transformation:** Digital transformation describes the process of transforming decision making with technology. Digital transformation is an enterprisewide, board-level strategic reality for companies that are serious about ensuring their businesses deliver an exceptional customer experience and becoming leaders in the digital economy. Digital transformation is a multiyear effort, with specific goals and objectives around markets and customers, revenue, and profit growth.
- **Data protection:** Data protection refers to the protection, restoration, and recovery of data in the event of physical or logical errors. This includes products and services that support both physical and virtual infrastructures.
- **Disaster recovery:** Disaster recovery is a combination of solutions that provide replication of physical or virtual servers and failover workload recovery in the event of a hardware failure or man-made or natural catastrophe. Disaster recovery solutions typically provide replication of data and applications with assigned recovery point objectives, where data and applications will have a set "age" where recovery from backup storage for normal operations can occur if a server, system, or network suffers a failure. Solutions also have a recovery time objective, which is the time frame in which the enterprise will regain normalized access to the data and applications being supported.
- **Hybrid cloud:** Hybrid cloud is an application deployment environment that utilizes both on-premises private cloud resources (i.e., local datacenter) and off-premises public or managed cloud resources to deliver the totality of the application functionality.
- **Multicloud:** Multicloud is an infrastructure deployment environment that utilizes two or more off-premises public or managed cloud resources for complete or partial application delivery.



Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

CSF Recover Controls for COVID-19 - https://www.acq.osd.mil/jrac/da2/index.html

Defense Assisted Acquisition (DA2) Cell

The DA2 has assumed the interagency efforts for COVID-19 medical resource acquisition previously coordinated by the DoD's Joint Acquisition Task Force (JATF). Nested within the Joint Rapid Acquisition Cell (JRAC), the DA2 is poised to rapidly respond to the nation's most urgent acquisition needs in current and future national emergencies.

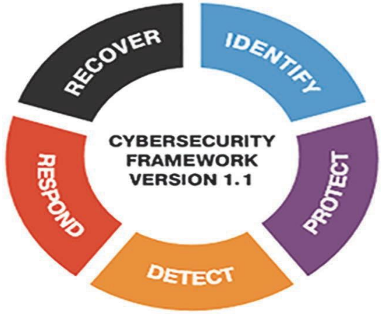
•DOD Awards $231.8 Million Contract to Ellume USA LLC to Increase Domestic Production Capacity and Deliver COVID-19 Home Tests

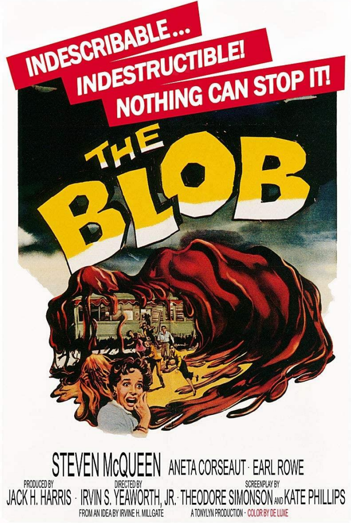
•DOD Awards $69.3 Million Contract to CONTINUUS Pharmaceuticals to Develop US-based Continuous Manufacturing Capability for Critical Medicines

•DOD Awards $110 Million Firm Fixed Price Contract Action to Puritan Medical Products to Increase Domestic Production Capacity of Foam Tip Swabs

•DOD Awards $15 Million Firm Fixed Price Contract to Corning Incorporated to Increase Domestic Production Capacity of Robotic Pipette Tips

•DOD Awards $4.8 Million Indefinite Delivery/Indefinite Quantity to a Calibre Scientific Subsidiary, Anatrace, to Increase Domestic Production Capacity of COVID-19 Testing Reagents

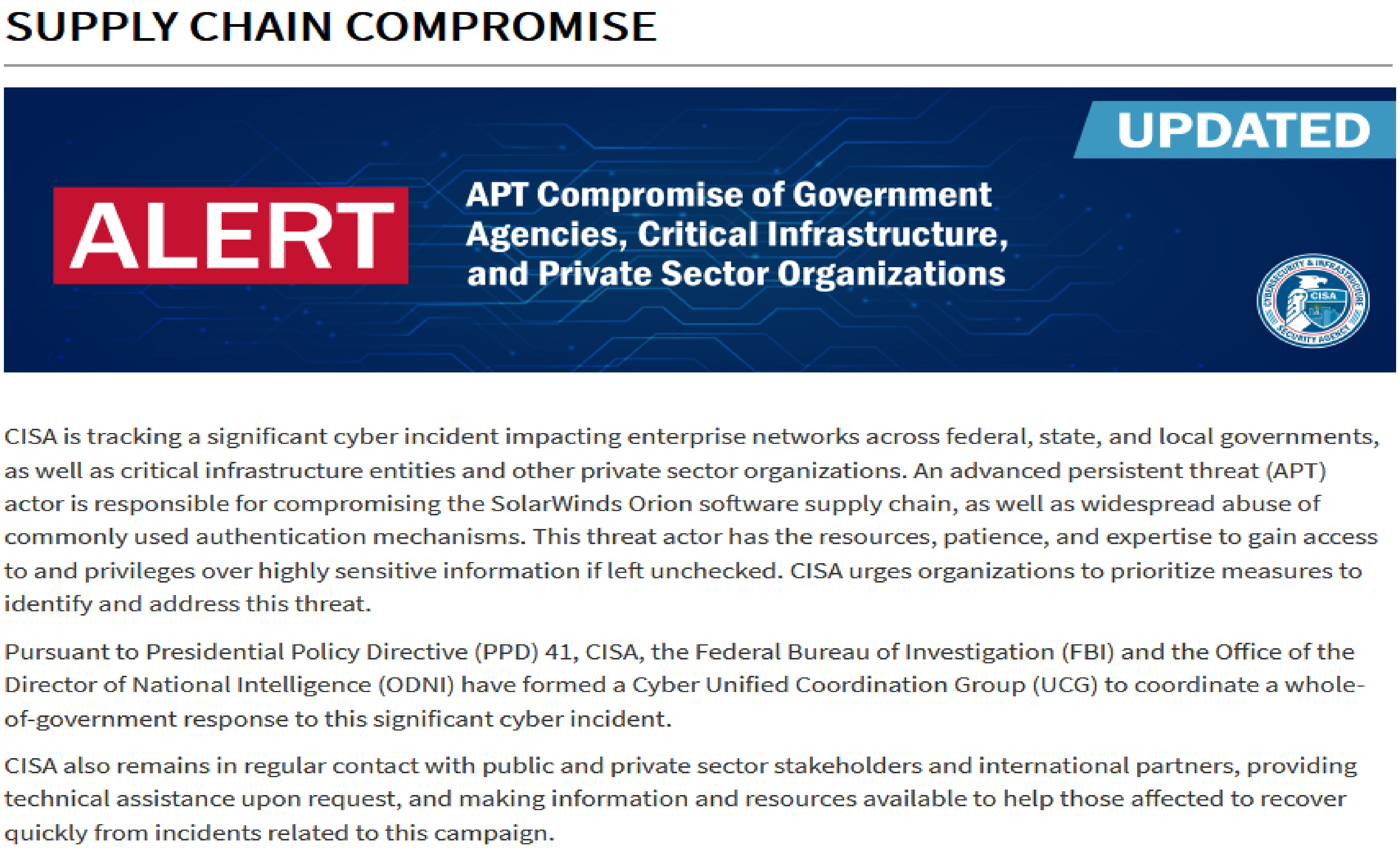



INDESCRIBABLE...
INDESTRUCTIBLE!
NOTHING CAN STOP IT!
THE BLOB
STEVEN McQUEEN ANETA CORSEAUT · EARL ROWE
PRODUCED BY JACK H. HARRIS · DIRECTED BY IRVIN S. YEAWORTH, JR. · SCREENPLAY BY THEODORE SIMONSON AND KATE PHILLIPS
FROM AN IDEA BY IRVINE H. MILLGATE
A TONYLYN PRODUCTION · COLOR BY DE LUXE

A HORROR HORDE OF CRAWL-AND-CRUSH GIANTS
CLAWING OUT OF THE EARTH
FROM MILE-DEEP
CATACOMBS!
"THEM!"
"This city is under martial law until we annihilate THEM!"
Kill one and two take it's place!
THE AMAZING NEW WARNER BROS. SENSATION!
"THEM!" JAMES WHITMORE . EDMUND GWENN . JOAN WELDON . JAMES ARNESS

Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

SUNBURST - Solar Winds ORION NMS APT Attack (2019 - 2021) - Oops



SUPPLY CHAIN COMPROMISE

UPDATED

ALERT

APT Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

CISA is tracking a significant cyber incident impacting enterprise networks across federal, state, and local governments, as well as critical infrastructure entities and other private sector organizations. An advanced persistent threat (APT) actor is responsible for compromising the SolarWinds Orion software supply chain, as well as widespread abuse of commonly used authentication mechanisms. This threat actor has the resources, patience, and expertise to gain access to and privileges over highly sensitive information if left unchecked. CISA urges organizations to prioritize measures to identify and address this threat.

Pursuant to Presidential Policy Directive (PPD) 41, CISA, the Federal Bureau of Investigation (FBI) and the Office of the Director of National Intelligence (ODNI) have formed a Cyber Unified Coordination Group (UCG) to coordinate a whole-of-government response to this significant cyber incident.

CISA also remains in regular contact with public and private sector stakeholders and international partners, providing technical assistance upon request, and making information and resources available to help those affected to recover quickly from incidents related to this campaign.

https://www.cisa.gov/supply-chain-compromise

No One Knows How Deep Russia's Hacking Rampage Goes

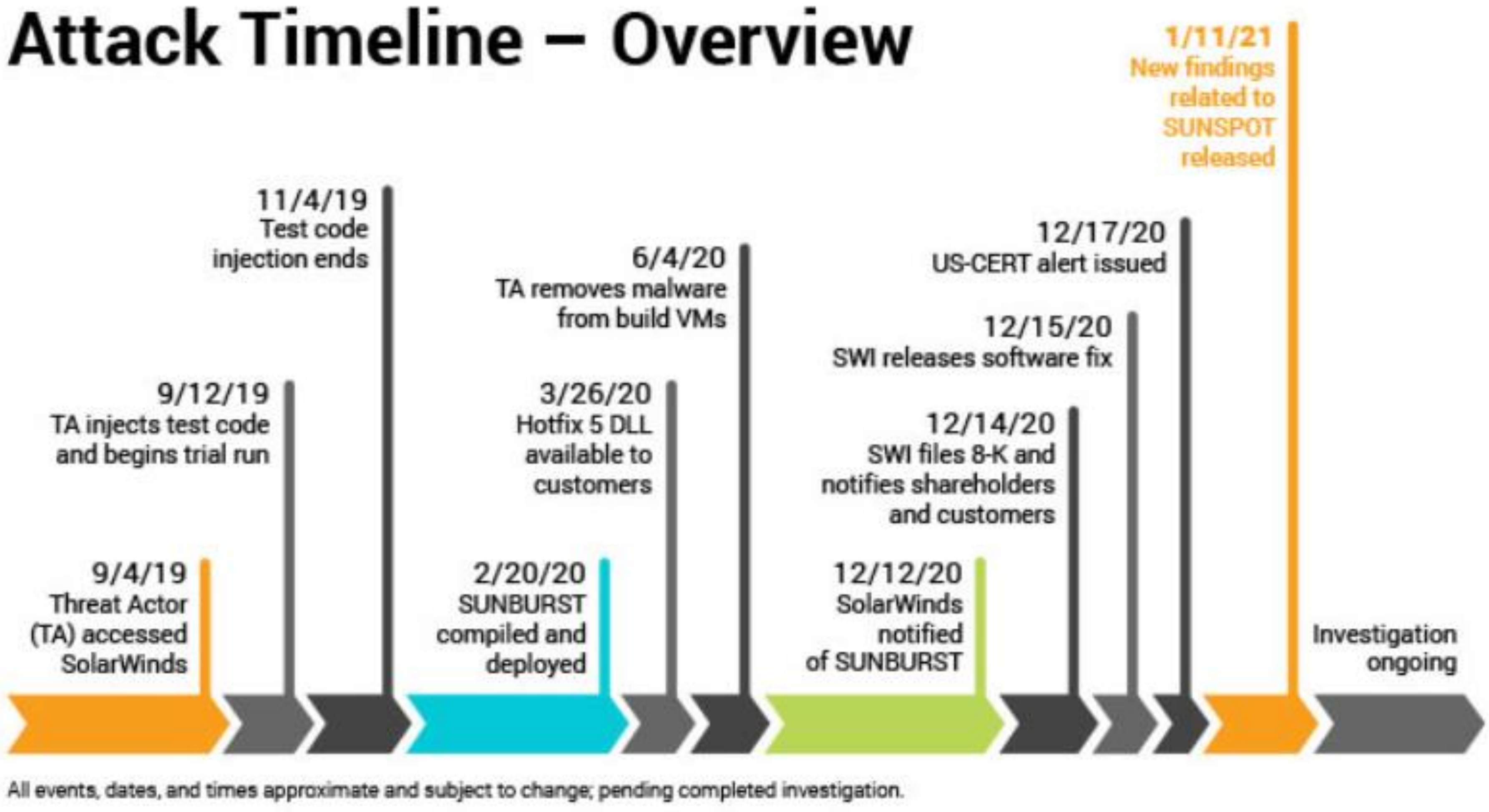
A supply chain attack against IT company SolarWinds has exposed as many as 18,000 companies to Cozy Bear's attacks.

- **SANS Bulletin - Threat Actors Behind SolarWinds Used Multiple Attack Vectors** - **(January 29 & February 1, 2021)**

- The *acting director of the US Cybersecurity and Infrastructure Security Agency (CISA)* says that “significant numbers of both the private-sector and government victims linked to this campaign had no direct connection to SolarWinds.” The threat actors multiple attack vectors. (Please note that the WSJ story is behind a paywall.)

- **Read more in:**
  - **www.securityweek.com**: CISA Says Many Victims of SolarWinds Hackers Had No Direct Link to SolarWinds
  - **www.scmagazine.com**: Does SolarWinds change the rules in offensive cyber? Experts say no, but offer alternatives
  - **www.scmagazine.com**: As SolarWinds spooks tech firms into rechecking code, some won’t like what they find
  - **www.zdnet.com**: SolarWinds attack is not an outlier, but a moment of reckoning for security industry, says Microsoft exec
  - **www.wsj.com**: Suspected Russian Hack Extends Far Beyond SolarWinds Software, Investigators Say (paywall)
  - **arstechnica.com**: 30% of “SolarWinds hack” victims didn’t actually use SolarWinds

SUNBURST - Solar Winds ORION NMS APT Attack (2019 - 2021) - Oops



Attack Timeline – Overview

9/4/19
Threat Actor (TA) accessed SolarWinds

9/12/19
TA injects test code and begins trial run

11/4/19
Test code injection ends

2/20/20
SUNBURST compiled and deployed

3/26/20
Hotfix 5 DLL available to customers

6/4/20
TA removes malware from build VMs

12/12/20
SolarWinds notified of SUNBURST

12/14/20
SWI files 8-K and notifies shareholders and customers

12/15/20
SWI releases software fix

12/17/20
US-CERT alert issued

1/11/21
New findings related to SUNSPOT released

Investigation ongoing

All events, dates, and times approximate and subject to change; pending completed investigation.

https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details

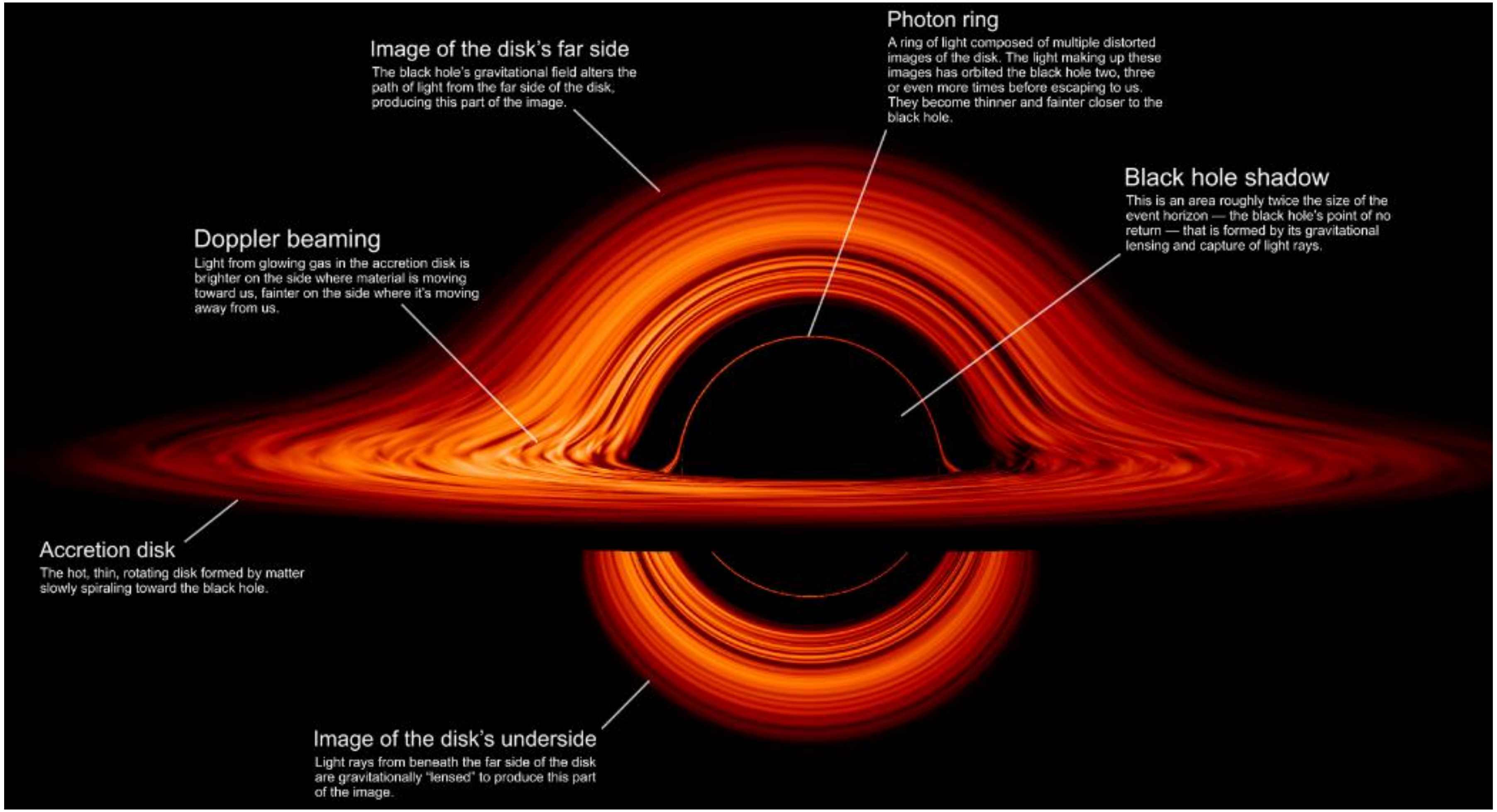


Image of the disk's far side
The black hole's gravitational field alters the path of light from the far side of the disk, producing this part of the image.
Photon ring
A ring of light composed of multiple distorted images of the disk. The light making up these images has orbited the black hole two, three or even more times before escaping to us. They become thinner and fainter closer to the black hole.
Black hole shadow
This is an area roughly twice the size of the event horizon — the black hole's point of no return — that is formed by its gravitational lensing and capture of light rays.
Doppler beaming
Light from glowing gas in the accretion disk is brighter on the side where material is moving toward us, fainter on the side where it's moving away from us.
Accretion disk
The hot, thin, rotating disk formed by matter slowly spiraling toward the black hole.
Image of the disk's underside
Light rays from beneath the far side of the disk are gravitationally "lensed" to produce this part of the image.

NASA Visualization Shows a Black Hole's Warped World

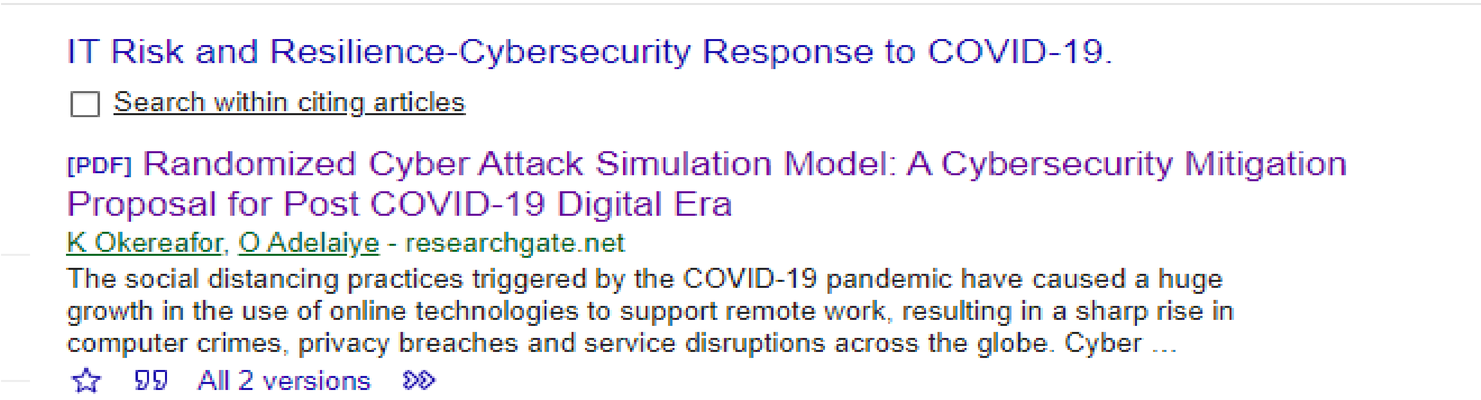
This new visualization of a black hole illustrates how its gravity distorts our view, warping its surroundings as if seen in a carnival mirror. The visualization simulates the appearance of a black hole where infalling matter has collected into a thin, hot structure called an accretion disk. The black hole's extreme gravity skews light emitted by different regions of the disk, producing the misshapen appearance.

https://www.nasa.gov/feature/goddard/2019/nasa-visualization-shows-a-black-hole-s-warped-world

Table of Contents

- Cyberspace – Our Point of Departure
- Information Security Management Models
- Frameworks for Risk Management
- COVID Smackdown – NIST CSF vs Big Scary Monsters
- Random Cybersecurity Attack Simulation Model (RCSM)
- References + Q&A

1st Citation for ‘IT Risk and Resilience – Cybersecurity Response to COVID-19’



IT Risk and Resilience-Cybersecurity Response to COVID-19.

☐ Search within citing articles

[PDF] Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era

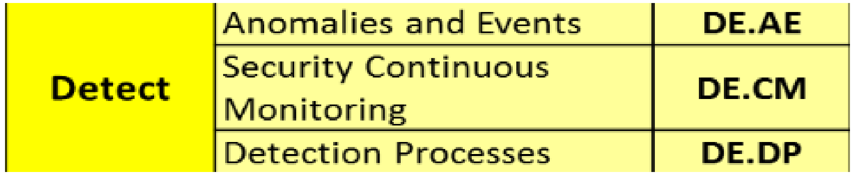
[PDF] researchgate.net

K Okereafor, O Adelaiye - researchgate.net

The social distancing practices triggered by the COVID-19 pandemic have caused a huge growth in the use of online technologies to support remote work, resulting in a sharp rise in computer crimes, privacy breaches and service disruptions across the globe. Cyber ...

☆ 99 All 2 versions »

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
CYBERSECURITY FRAMEWORK VERSION 1.1

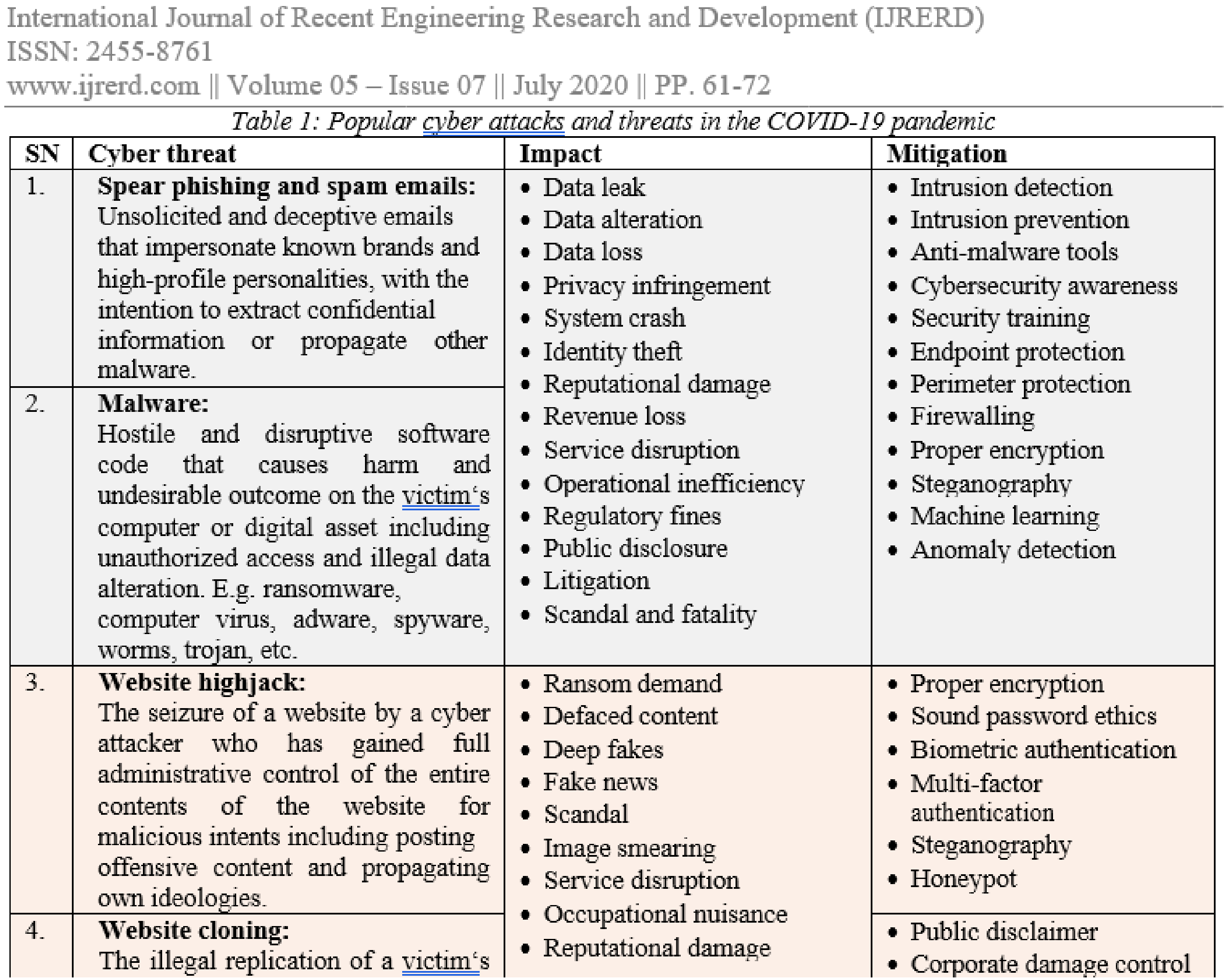


Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP

- Cyber attackers are taking advantage of COVID-19 anxiety to launch email scams, misinform and mislead unsuspecting targets, and propagate harmful software using various threats. The trend beckons for a more proactive cybersecurity approach to detect, prevent, and mitigate potential computer crimes. This paper proposes **a Randomized Cyberattack Simulation Model (RCSM),** an enhanced cyber attack readiness checklist for tackling computer crimes in advance. The RCSM extends traditional incident response and offers **a pre-forensic guide as a precursor to the redefinition of cybersecurity in the post COVID-19 digital era.**

- Cyber attack incidents have been on a steady increase, with their impacts including rising financial implications [4] and millions of dollars [5] in tangential losses. Most attacks occur even in the midst of traditional mitigation methods, using obfuscation to evade [6] detection and gain persistence in the system [7]. **Most recent cyber attacks use un-identified attack methods, which make signature-based detection grossly ineffective** [8], including the recovery approach proposed by ***Weil and Murugesan [9]***.

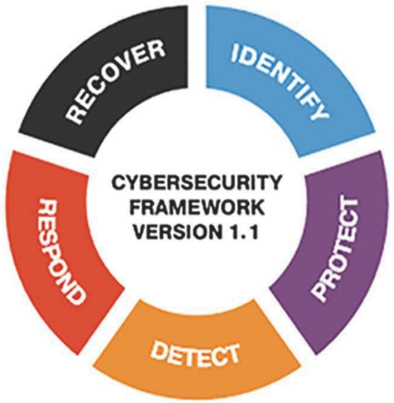
Global transformation caused by COVID-19

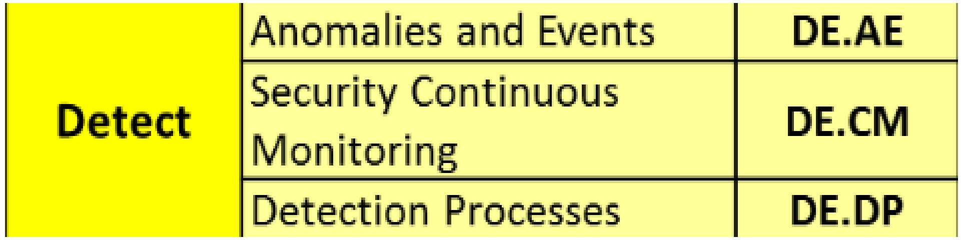


International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 05 – Issue 07 || July 2020 || PP. 61-72

Table 1: Popular cyber attacks and threats in the COVID-19 pandemic

SN	Cyber threat	Impact	Mitigation
1.	**Spear phishing and spam emails:** Unsolicited and deceptive emails that impersonate known brands and high-profile personalities, with the intention to extract confidential information or propagate other malware.	• Data leak • Data alteration • Data loss • Privacy infringement • System crash • Identity theft • Reputational damage • Revenue loss • Service disruption • Operational inefficiency • Regulatory fines • Public disclosure • Litigation • Scandal and fatality	• Intrusion detection • Intrusion prevention • Anti-malware tools • Cybersecurity awareness • Security training • Endpoint protection • Perimeter protection • Firewalling • Proper encryption • Steganography • Machine learning • Anomaly detection
2.	**Malware:** Hostile and disruptive software code that causes harm and undesirable outcome on the victim‘s computer or digital asset including unauthorized access and illegal data alteration. E.g. ransomware, computer virus, adware, spyware, worms, trojan, etc.		
3.	**Website highjack:** The seizure of a website by a cyber attacker who has gained full administrative control of the entire contents of the website for malicious intents including posting offensive content and propagating own ideologies.	• Ransom demand • Defaced content • Deep fakes • Fake news • Scandal • Image smearing • Service disruption • Occupational nuisance • Reputational damage	• Proper encryption • Sound password ethics • Biometric authentication • Multi-factor authentication • Steganography • Honeypot
4.	**Website cloning:** The illegal replication of a victim‘s		• Public disclaimer • Corporate damage control





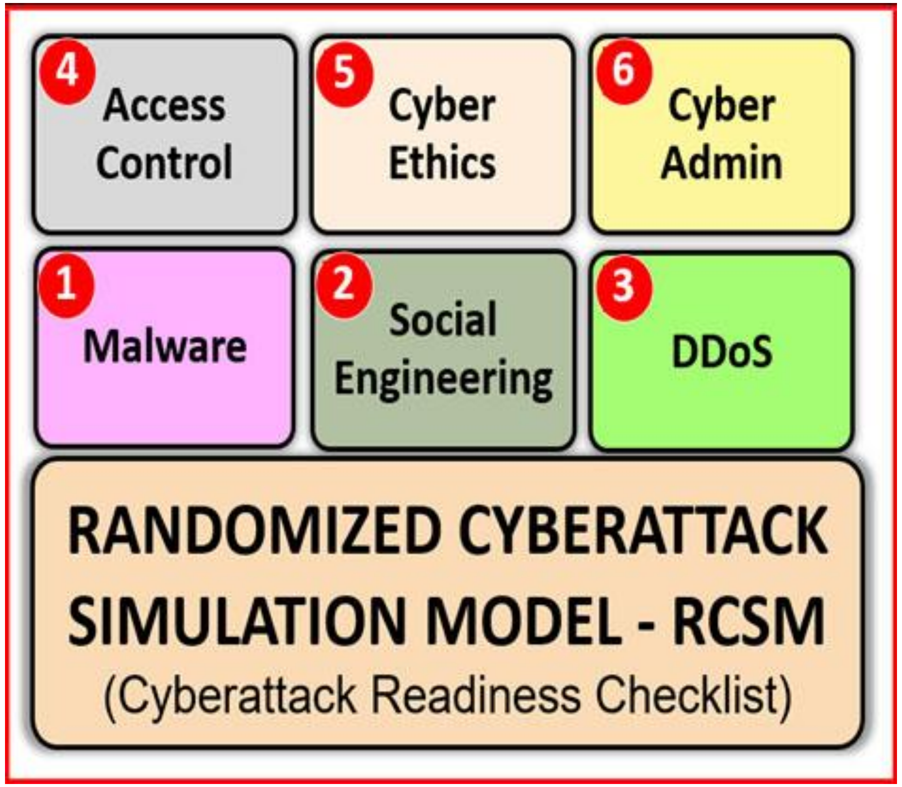
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP

Cyber attacks during COVID-19

- Spear phishing and SPAM email
- Malware
- Website highjack
- Website cloning
- Cyber espionage

Okereafor, Kenneth & Adelaiye, Oluwasegun. (2020). Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. 05. 61-72.

Global transformation caused by COVID-19



4 Access Control

5 Cyber Ethics

6 Cyber Admin

1 Malware

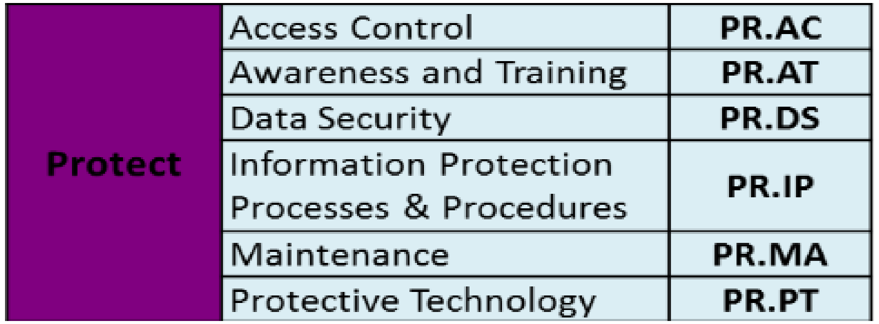
2 Social Engineering

3 DDoS

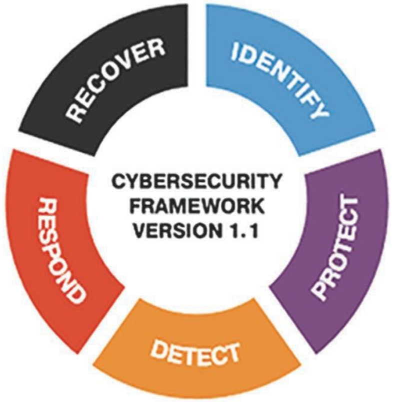
RANDOMIZED CYBERATTACK SIMULATION MODEL - RCSM

(Cyberattack Readiness Checklist)

Okereafor, Kenneth & Adelaiye, Oluwasegun. (2020). Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. 05. 61-72.

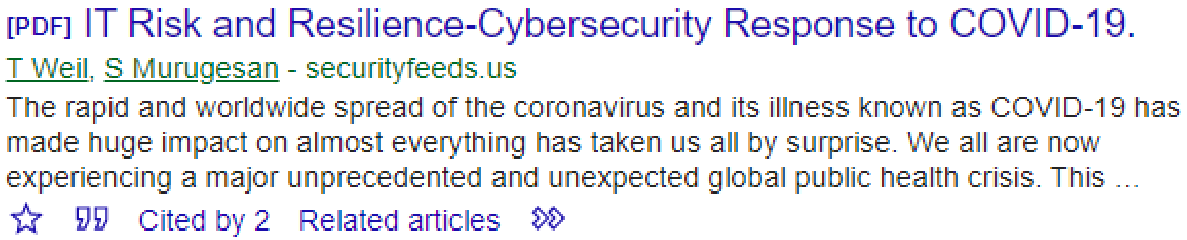


Protect	Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & Procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**



The RCSM provides an easy-to-reference set of best practices for incident response teams to evaluate and assess, in advance, the IT infrastructure‘s resilience and preparedness to neutralize malicious activities and resist spontaneous cyber attacks. As a novel cyber attack simulation approach, it is designed to offer an instantaneous checklist for the cyber defence preparedness of the organization, with the following key features:

1. Proactively analyses the scope of vulnerabilities in critical applications.
2. Appraises the strengths and capabilities of existing controls.
3. Strengthens the organization‘s pre-forensic and cybersecurity functions.
4. Differs from a pre-scheduled vulnerability and penetration testing.
5. Deployed rather spontaneously in a typical security drill fashion.
6. Detects weak controls that must be compulsorily fixed in advance.
7. Evaluates how incident responders truly react to unexpected attacks.



[PDF] IT Risk and Resilience-Cybersecurity Response to COVID-19.

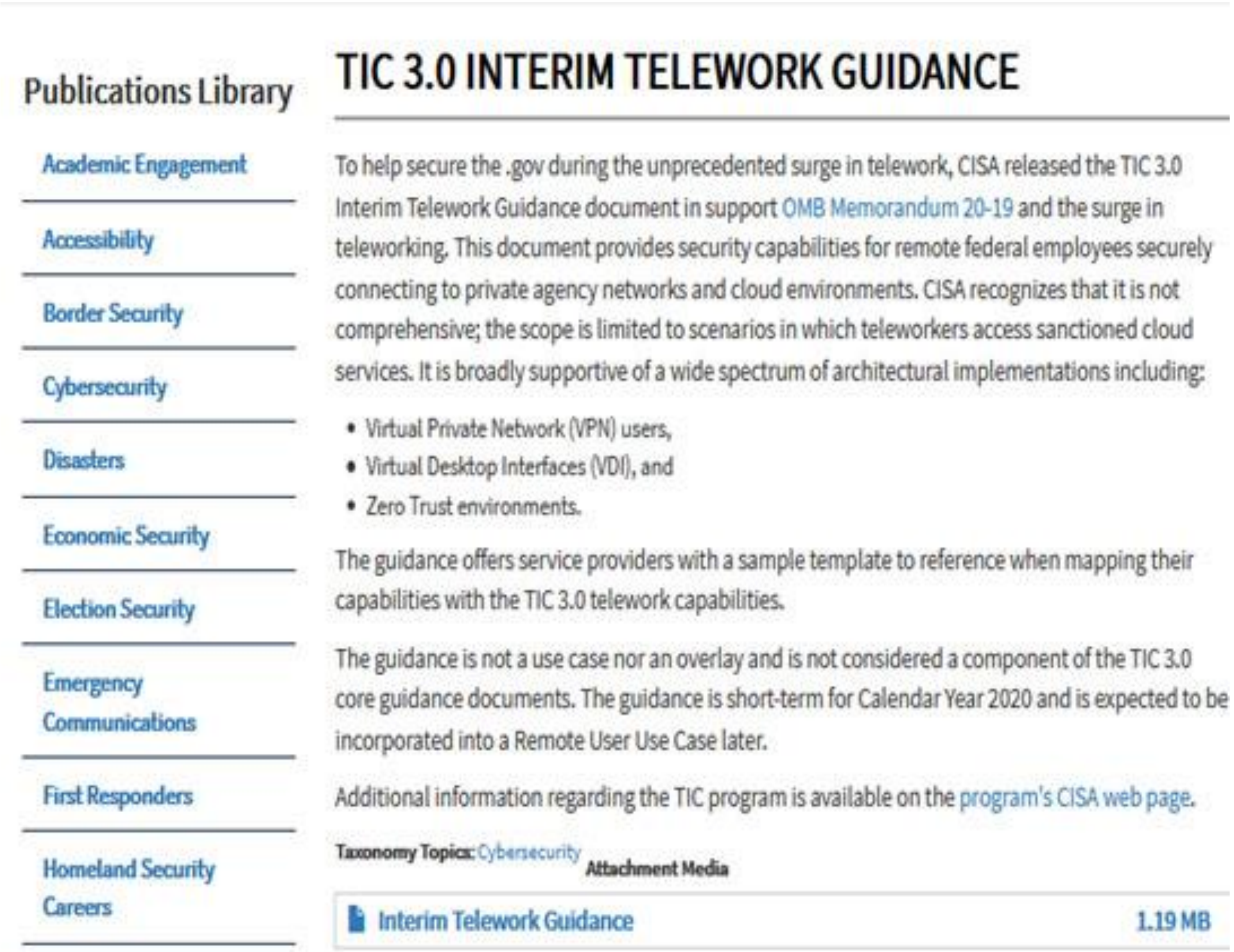
T Weil, S Murugesan - securityfeeds.us

The rapid and worldwide spread of the coronavirus and its illness known as COVID-19 has made huge impact on almost everything has taken us all by surprise. We all are now experiencing a major unprecedented and unexpected global public health crisis. This ...

☆ 99 Cited by 2 Related articles »

Global transformation caused by COVID-19

https://www.cisa.gov/publication/tic-30-interim-telework-guidance



Publications Library

- Academic Engagement
- Accessibility
- Border Security
- Cybersecurity
- Disasters
- Economic Security
- Election Security
- Emergency Communications
- First Responders
- Homeland Security Careers

TIC 3.0 INTERIM TELEWORK GUIDANCE

To help secure the .gov during the unprecedented surge in telework, CISA released the TIC 3.0 Interim Telework Guidance document in support OMB Memorandum 20-19 and the surge in teleworking. This document provides security capabilities for remote federal employees securely connecting to private agency networks and cloud environments. CISA recognizes that it is not comprehensive; the scope is limited to scenarios in which teleworkers access sanctioned cloud services. It is broadly supportive of a wide spectrum of architectural implementations including:

- Virtual Private Network (VPN) users,
- Virtual Desktop Interfaces (VDI), and
- Zero Trust environments.

The guidance offers service providers with a sample template to reference when mapping their capabilities with the TIC 3.0 telework capabilities.

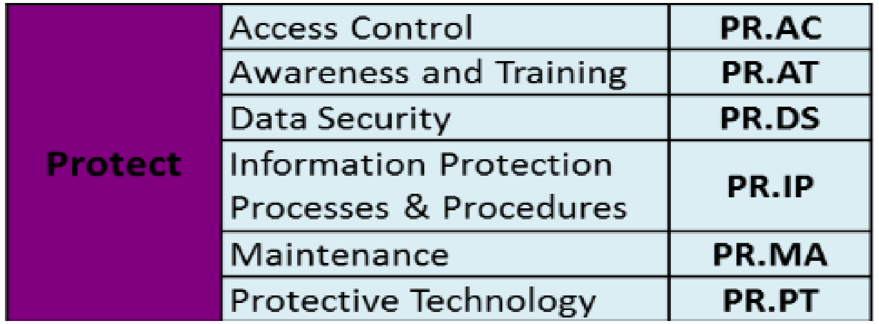
The guidance is not a use case nor an overlay and is not considered a component of the TIC 3.0 core guidance documents. The guidance is short-term for Calendar Year 2020 and is expected to be incorporated into a Remote User Use Case later.

Additional information regarding the TIC program is available on the program's CISA web page.

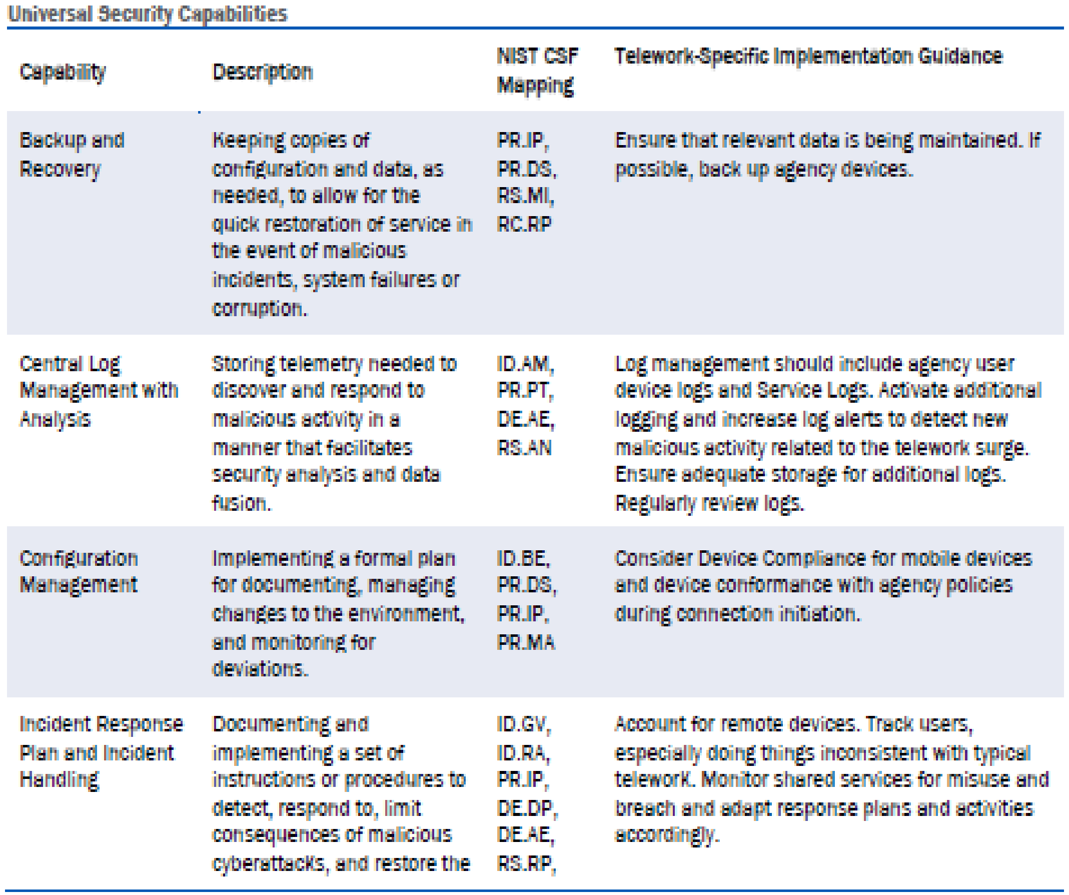
Taxonomy Topics: Cybersecurity

Attachment Media

Interim Telework Guidance 1.19 MB



Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT



Universal Security Capabilities

Capability	Description	NIST CSF Mapping	Telework-Specific Implementation Guidance
Backup and Recovery	Keeping copies of configuration and data, as needed, to allow for the quick restoration of service in the event of malicious incidents, system failures or corruption.	PR.IP, PR.DS, RS.MI, RC.RP	Ensure that relevant data is being maintained. If possible, back up agency devices.
Central Log Management with Analysis	Storing telemetry needed to discover and respond to malicious activity in a manner that facilitates security analysis and data fusion.	ID.AM, PR.PT, DE.AE, RS.AN	Log management should include agency user device logs and Service Logs. Activate additional logging and increase log alerts to detect new malicious activity related to the telework surge. Ensure adequate storage for additional logs. Regularly review logs.
Configuration Management	Implementing a formal plan for documenting, managing changes to the environment, and monitoring for deviations.	ID.BE, PR.DS, PR.IP, PR.MA	Consider Device Compliance for mobile devices and device conformance with agency policies during connection initiation.
Incident Response Plan and Incident Handling	Documenting and implementing a set of instructions or procedures to detect, respond to, limit consequences of malicious cyberattacks, and restore the	ID.GV, ID.RA, PR.IP, DE.DP, DE.AE, RS.RP,	Account for remote devices. Track users, especially doing things inconsistent with typical telework. Monitor shared services for misuse and breach and adapt response plans and activities accordingly.

Assessing Cybersecurity Response to COVID-19 – Blue Sky or Rain?

Table of Contents

- Cyberspace – Our Point of Departure
- Information Security Management Models
- Frameworks for Risk Management
- COVID Smackdown – NIST CSF vs Big Scary Monsters
- Random Cybersecurity Attack Simulation Model (RCSM)
- References + Q&A

IT Pro Special Issue on Communications Recovery and Resilience

https://www.computer.org/csdl/magazine/it/2020/06/09250314/1oxkJTuIsMg

IT Pro Special Issue on Communications Recovery and Resilience - Editor's Column" by Tim Weil, Bhuvan Unhelkar, John Callahan, Jason W. Rupe, Keith Sherringham

Recovery and resilience are two sides worth exploring here: 1) the needs and challenges with recovering from disasters of all types, and 2) how to enhance the resiliency of communication networks to provide better support in these difficult operations
https://doi.org/10.1109/MITP.2020.3031443 https://www.computer.org/csdl/magazine/it/2020/06/09250314/1oxkJTuIsMg

A Design for Resilient Datacenter Networks by Alan H. Karp, Paul L. Borrill

A key design goal is the ability to recover from network failures so fast that applications perceive an unbreakable network.

https://doi.org/10.1109/MITP.2020.3013511

The IT Challenges in Disaster Relief: What We Learned From Hurricane Harvey by Yun Wan, Qi Zhu

We also observed that organizations used ad hoc technology solutions to accommodate different relief project needs; an integrated open-source system would not only save cost but also improve the overall productivity.
https://doi.org/10.1109/MITP.2020.3005675

Resilience in Smart City Applications: Faults, Failures, and Solutions by Jawwad. A. Shamsi

The paper concludes that for a cost-effective and feasible solution, an adaptive model is needed, which can enable resilience measures as per the needs of an application. https://doi.org/10.1109/MITP.2020.3016728

IT Pro Special Issue on Communications Recovery and Resilience

https://www.computer.org/csdl/magazine/it/2020/06/09250314/1oxkJTuIsMg

Enhancing Artificial Intelligence Decision Making Frameworks to Support Leadership During Business Disruptions by Bhuvan Unhelkar, Tad Gonsalves
This article discusses enhancing the DLE with human experience resulting in a business disruption prediction framework.
https://doi.org/10.1109/MITP.2020.3031312

Preference Biased Edge Weight Assignment for Connectivity-Based Resilience Computation in Telecommunication Networks" by Uthpala Subodhani Premarathne
Preference values bias the selection of node and edge-related attributes to compute the level of connectivity.
https://doi.org/10.1109/MITP.2020.3015961

Resiliency by Retrograded Communication-the Revival of Shortwave as a Military Communication Channel" by Jan Kallberg, Stephen S. Hamilton
The concept of retrograding could give an operational advantage and create the ability to sustain communication in EW saturated environment**.** https://doi.org/10.1109/MITP.2020.3029944

Resilience in Smart City Applications: Faults, Failures, and Solutions by Jawwad. A. Shamsi
The paper concludes that for a cost-effective and feasible solution, an adaptive model is needed, which can enable resilience measures as per the needs of an application. https://doi.org/10.1109/MITP.2020.3016728

Elastic Resilience for Software-Defined Satellite Networking: Challenges, Solutions, and Open Issues by Bohao Feng, Zhewei Cui, Yunxue Huang, Huachun Zhou, Shui Yu
We also discuss several key open issues to be urgently addressed, hoping to shed some light on this promising land.
https://doi.org/10.1109/MITP.2020.3019435

References – IT Risk and Resilience – Cybersecurity Response to COVID-19

- T. Weil and S. Murugesan, "IT Risk and Resilience—Cybersecurity Response to COVID-19," in IT Professional, vol. 22, no. 3, pp. 4-10, 1 May-June 2020, doi: 10.1109/MITP.2020.2988330. https://ieeecs-media.computer.org/media/marketing/cedge_digital/ce-oct20-final.pdf

- Okereafor, Kenneth & Adelaiye, Oluwasegun. (2020). Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. 05. 61-72.

- M. Reeves, et al., “Sensing and shaping the post-COVID era,” Boston Consulting Group, Apr. 3, 2020. [Online]. Available: https://www.bcg.com/publications/2020/8-ways-companies-can-shap-reality-post-covid-19.aspx

- “Five functions of the cybersecurity framework,” NIST. Apr. 2018. [Online]. Available: Cybersecurity framework,” NIST. Apr. 2018. [Online]. Ahttps://www.nist.gov/cyberframework/online-learning/five-functions

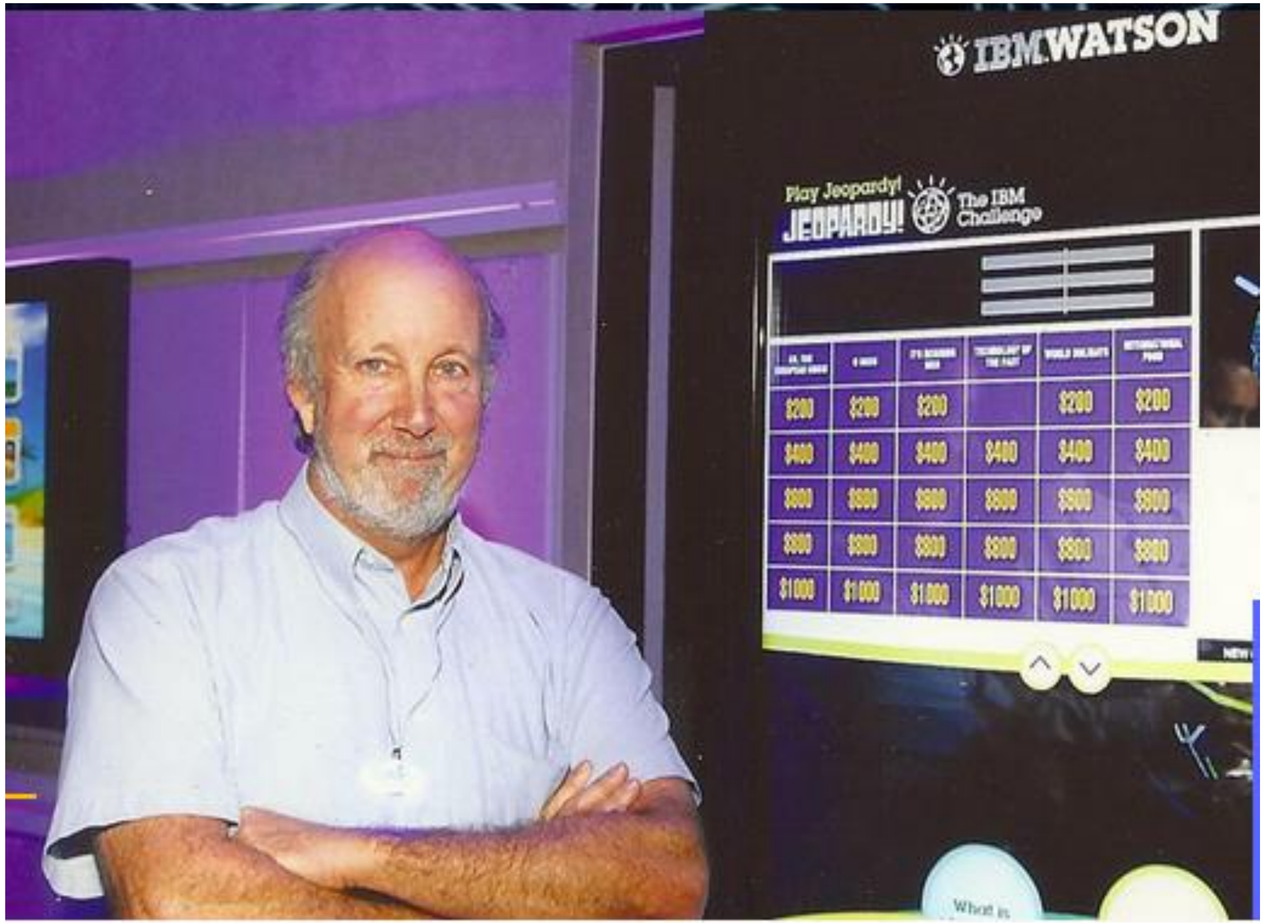
- vailable: http://www.nist.gov/cyberframework

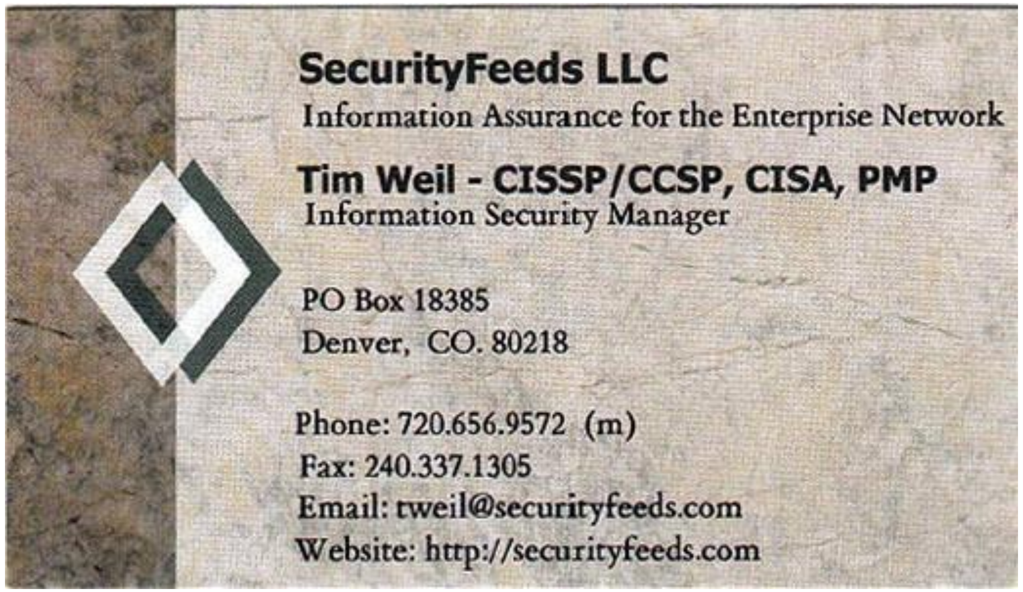
- “CISA INSIGHTS:TRUSTED INTERNET CONNECTIONS 3.0 INTERIM TELEWORK GUIDANCE: https://www.cisa.gov/publication/tic-30-interim-telework-guidance

- “CISA INSIGHTS: Risk Management for Novel Coronavirus (COVID-19),” CISA. Mar. 18, 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf

ICT - Science & Engineering Journalism – 1984 - 2020

Thank you for joining us!





SecurityFeeds LLC
Information Assurance for the Enterprise Network

Tim Weil - CISSP/CCSP, CISA, PMP
Information Security Manager

PO Box 18385
Denver, CO. 80218

Phone: 720.656.9572 (m)
Fax: 240.337.1305
Email: tweil@securityfeeds.com
Website: http://securityfeeds.com

SecurityFeeds LLC provides IT Management Consulting services

- Communications and Security Engineering
- Data Processing (Systems Engineering)
- Project and Program Management
- Risk Management (ISO 27001)

Our expertise includes Enterprise Security Architecture, Cloud Security, Program Management, and Network Engineering.

"RISK is a four-letter word"

http://www.securityfeeds.com - trweil@ieee.org