SecurityFeeds
Yor source for enterprise security management

IT Professional
Technology Solutions for the Enterprise

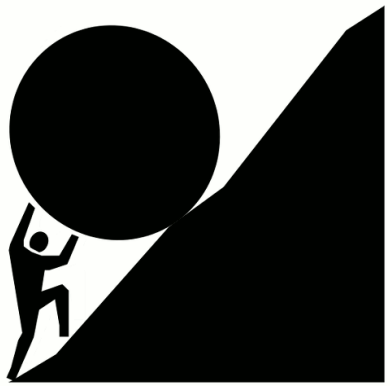
Technology, Cybersecurity and Policy (TCP)

Roadmaps for Risk Management

Tim Weil – IEEE Senior Member
CU-Boulder TCP Seminar
https://www.colorado.edu/cs/

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

Resilience and Reliability



Invited Talk
Boulder, CO
Oct. 17, 2022

Objectives of this Presentation

Cyberspace – Out Point of Departure

-- A Writer's Life

-- Risk Landscape Evaluation

-- Cloud Computing Model (NIST)

-- NIST Risk Management Framework

-- ISO 27001

Information Security Management Models

-- FISMA and FedRamp

-- Center for Internet Security (CIS) Top 18 Controls

-- NIST Cybersecurity Frameworks

Global transformation caused by COVID-19

-- Global transformation of Information Technology Services

-- COVID Smackdown – NIST CSF vs Big Scary Monsters

-- Attack on US Government Systems (2019-2021)

-- MITRE Att%ck Taxonomies and Methods

Emerging Road Maps for Risk Management

-- Project Management Institute (PMBOK)

-- Rational Cybersecurity for Business (Blum) vs Cybersecurity Management (Kshetri)

-- Information Security Management Systems (ISO 27001)

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 institutions 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.2020.2968330

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

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

Guest Editors' Introduction

VOLUME 22, NUMBER 6 NOVEMBER/DECEMBER 2(

Resilience and Reliability

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

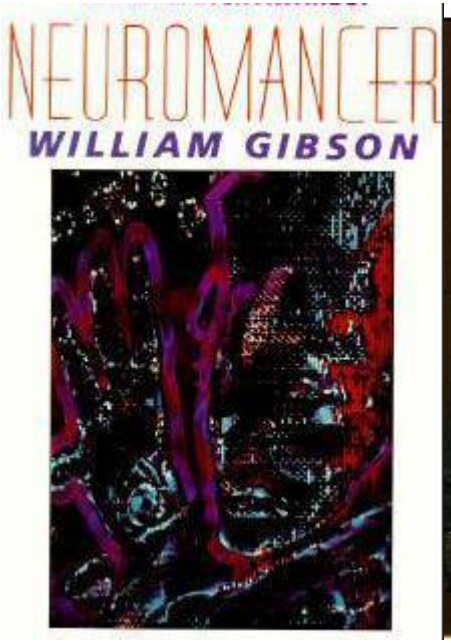
Four papers focus on improving communication networks to make them more resilient, which are as follows.

- 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

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

26 YEARS AFTER GIBSON, PENTAGON DEFINES 'CYBERSPACE'

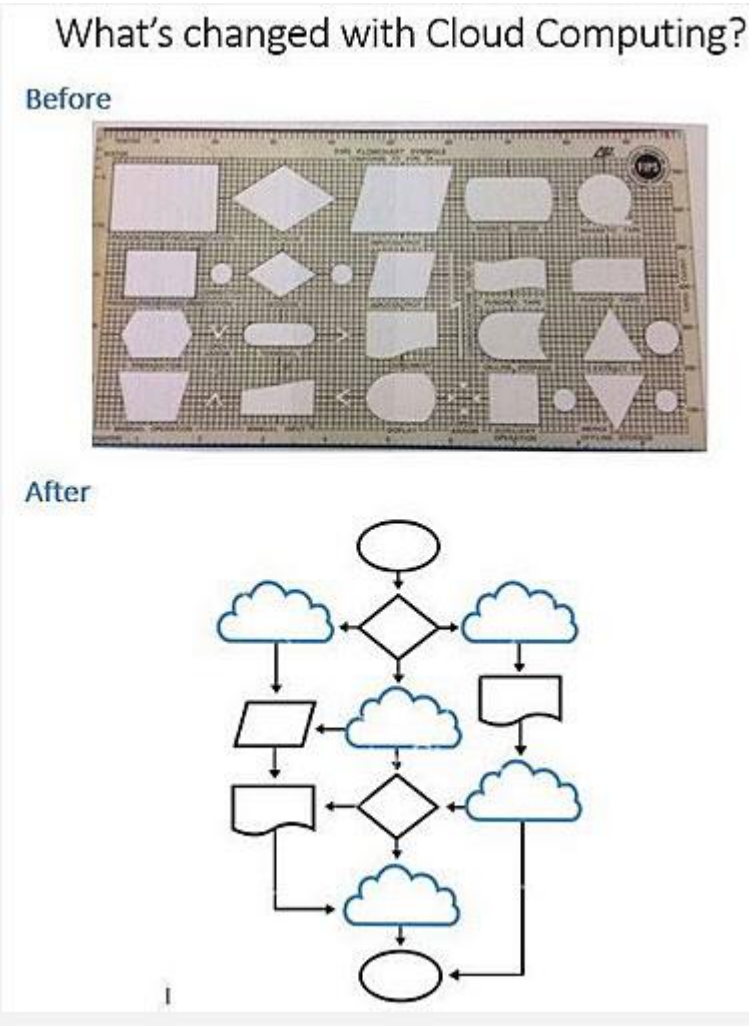


"More than two decades after novelist William Gibson coined the term cyberspace as a 'consensual hallucination' of data... the Pentagon has come up with its own definition,"* *Inside Defense reports. "A May 12 'for official use only' memo signed by Deputy Defense Secretary Gordon England... offers a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

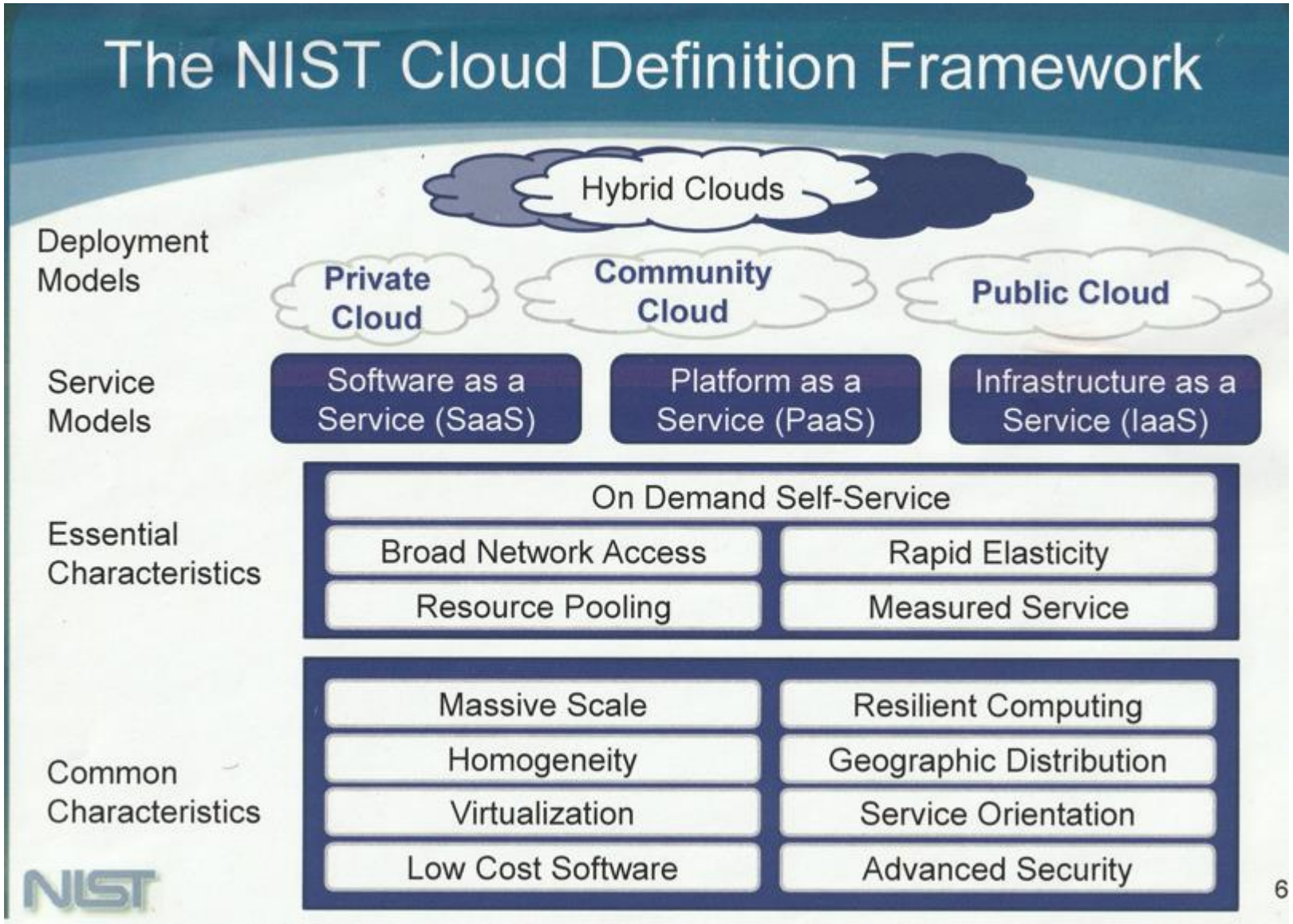
Cyberspace, England writes, is “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” *

*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.”

How we got to the cloud

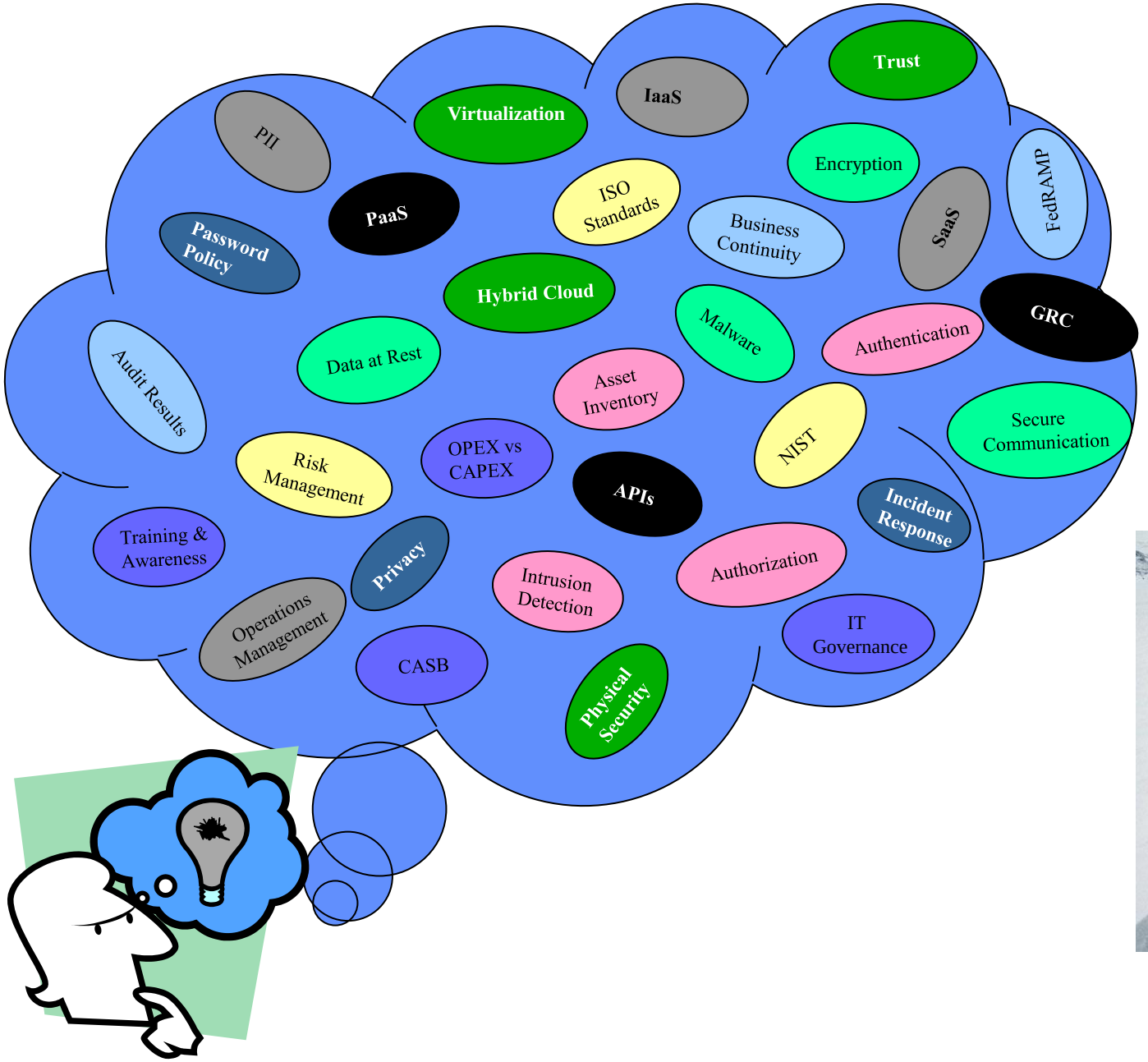


NIST Cloud Computing Model



https://securityfeeds.us/cloud-security

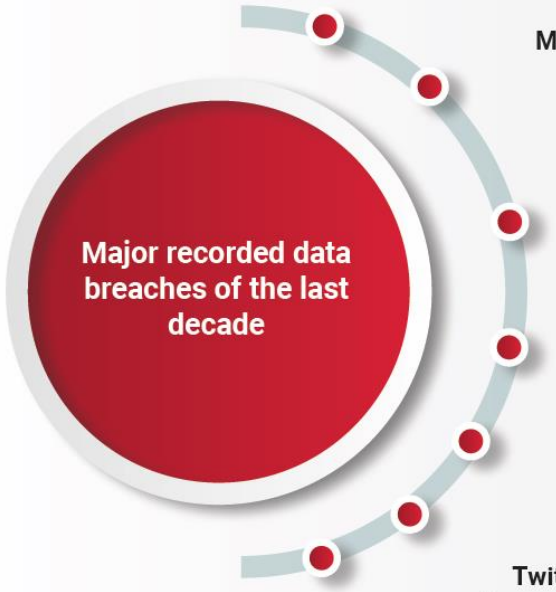
Now What? (Lessons learn from Enterprise Risk Assessment of the National Science Foundation's US Antarctic Program)



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
- **Manage Information Security & Privacy Risk**
- Improve Continuous Monitoring Process

FACTS ON SOME MAJOR RECORDED DATA BREACHES AROUND THE WORLD



Equifax: 143,000,000
Over 143 million credit reports of American citizens with sensitive personal data were leaked.

Marriot: 383,000,000
In 2018, Sheraton, Regis, W Hotels were hacked and sensitive customers' information, such as credit card and passport details were exposed.

American businesses hack: 160,000,000
Between 2005 and 2012, payment processors, chain stores and banks were targeted by hackers. More than 160 million credit and debit card numbers were stolen. This included businesses such as JC Penny, Visa Jordan, Dow Jones, 7-Eleven, JetBlue, etc.

Ebay: 154,000,000
In 2014, hackers targeted some of Ebay's employees and stole their login credentials. They used these credentials to access a database of all users' personal identifiable information.

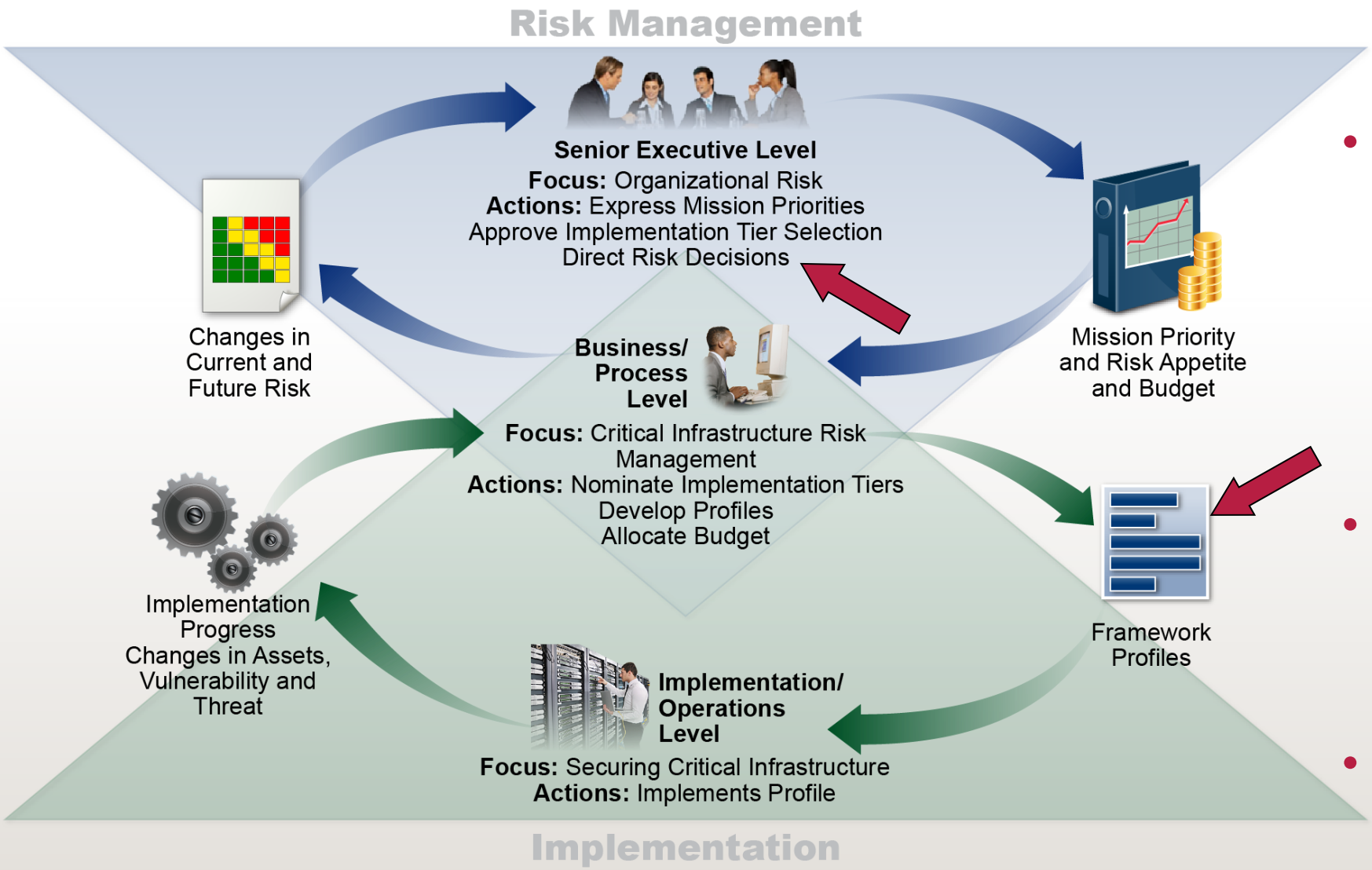
Facebook: 50,000,000
Cambridge Analytica managed to harvest over 50 million Facebook profiles' information in 2014. This data was then utilized to target US voters with political ads.

Twitter: 330,000,000
Due to a mishap, personal information such as passwords was stored in a readable text.

MangoDB: 275,265,298
Indian citizens' personal identifiable information was left unprotected on the Internet for more than two weeks.

PECB

Table of Contents



- 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

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

The FISMA Risk Management Framework.

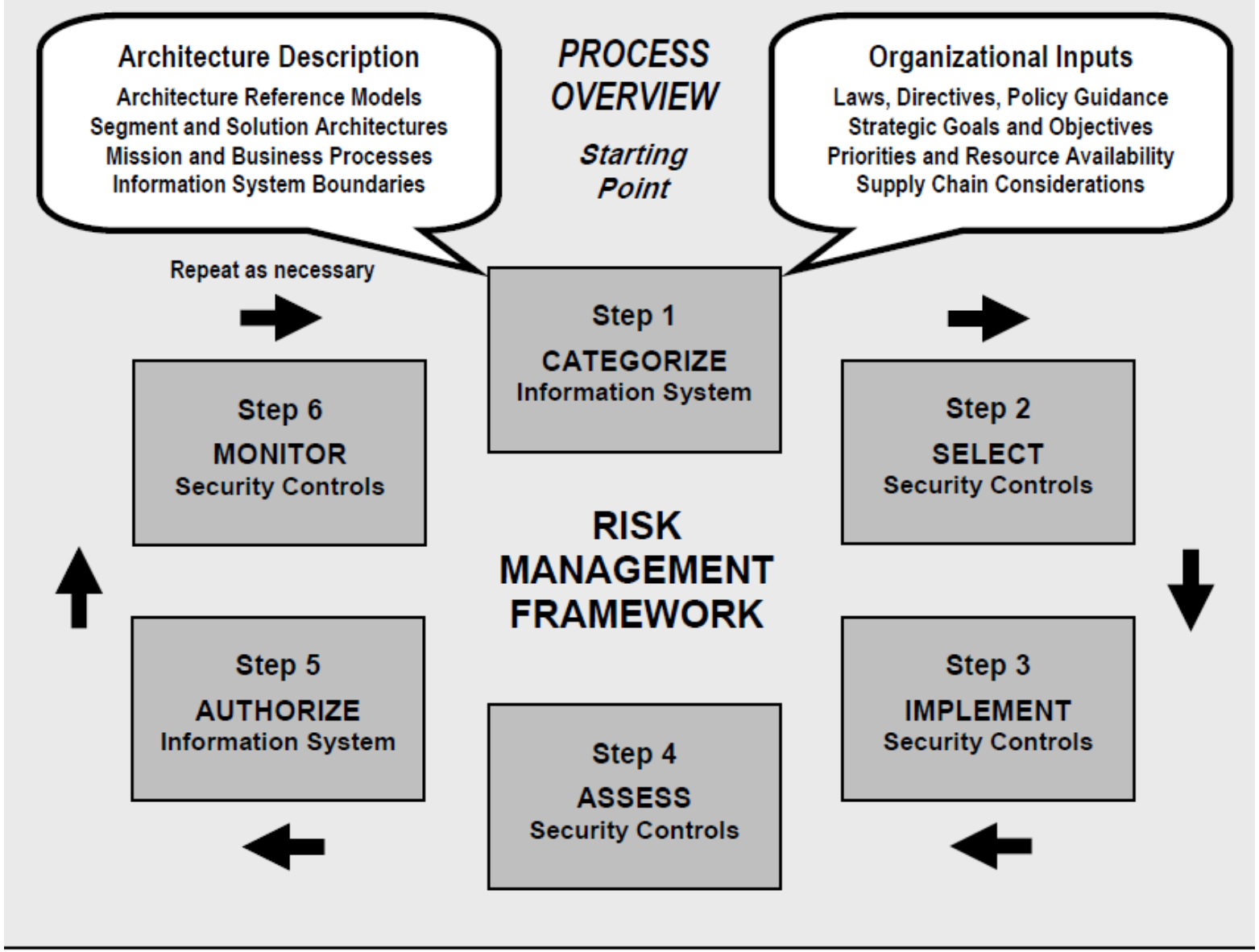


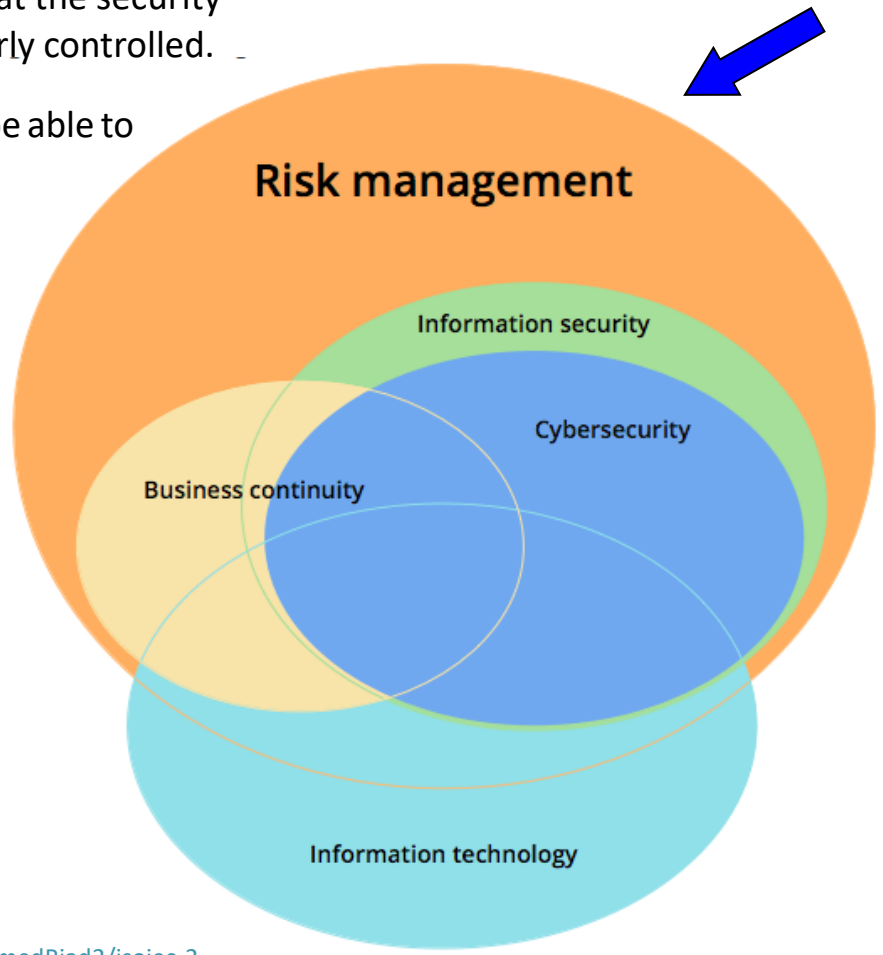
FIGURE 2-2: RISK MANAGEMENT FRAMEWORK

Benefits of ISO 27001 - ISO /IEC 27001:2013 Structure and Content

ISO/IEC 27001:2013 Implementation, Certification from a certification body demonstrates that the security of organization information has been addressed, valuable data and information assets properly controlled.

Also there is List of benefits By achieving certification to ISO/IEC 27001:2013 organization will be able to acquire numerous benefits including:

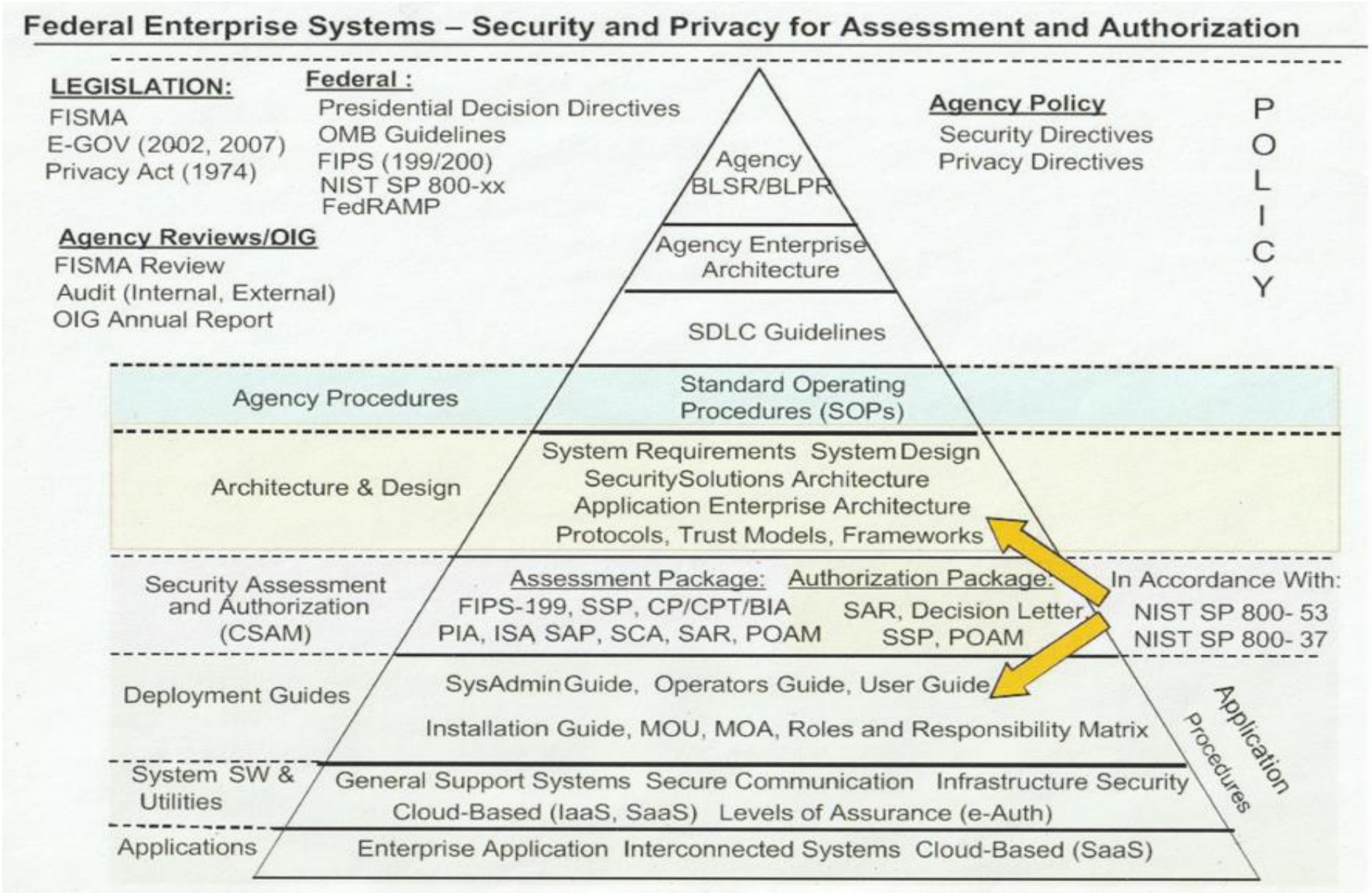
- Keeps confidential information secure
- Provides customers and stakeholders with confidence in how you manage risk
- Secure exchange of information
- Provide Organization with a competitive advantage
- Enhanced customer satisfaction
- Consistency in the delivery of your service or product
- Manages and minimises risk exposure
- Builds a culture of security
- Protects the Organization assets, shareholders and Customers
- Protects the company, assets, shareholders and directors



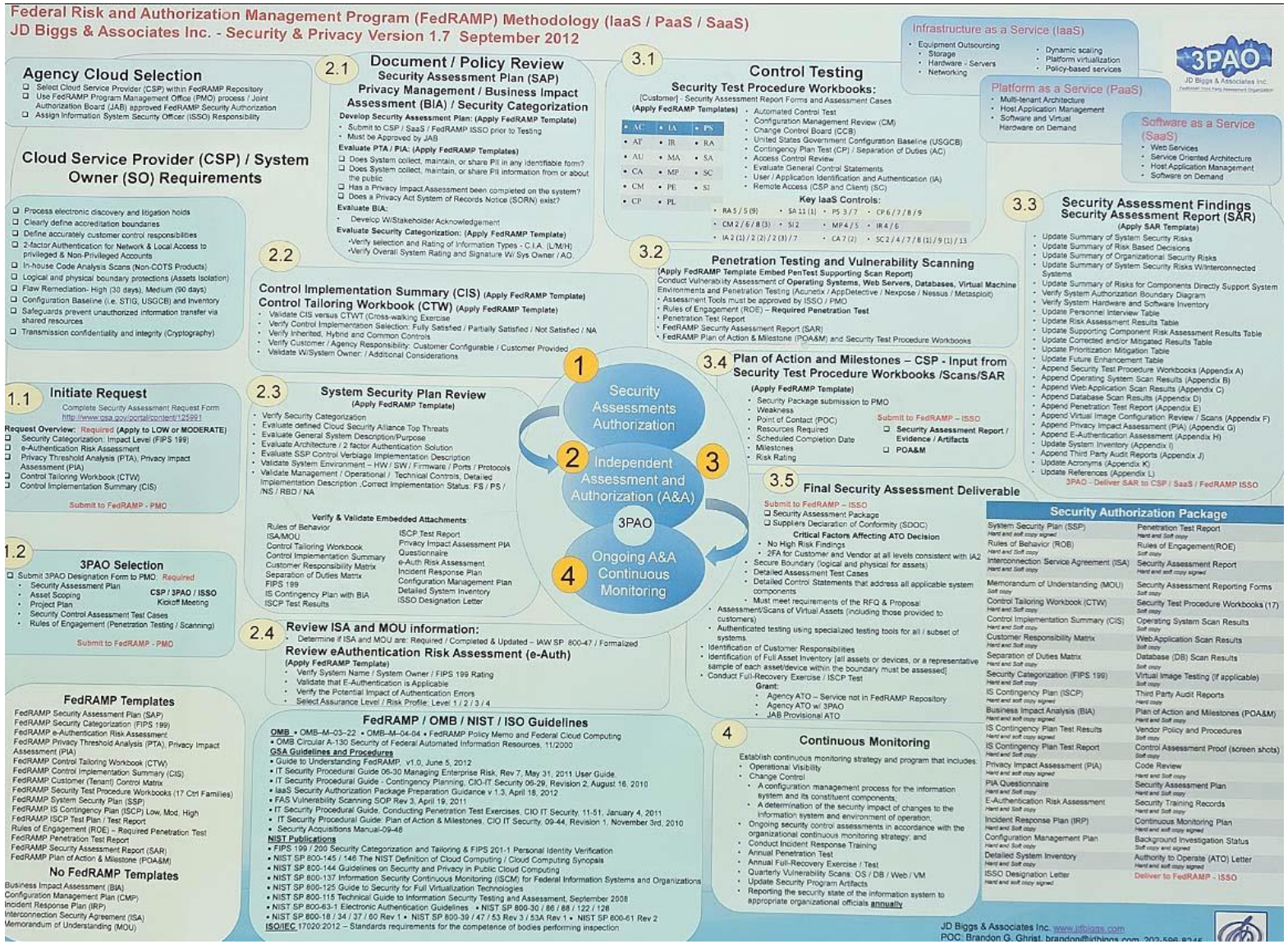
Ahmed Riad, BlueKaizen Magazine, Benefits of ISO 27001- https://www.slideshare.net/AhmedRiad2/isoiec-https://www.slideshare.net/AhmedRiad2/isoiec-2

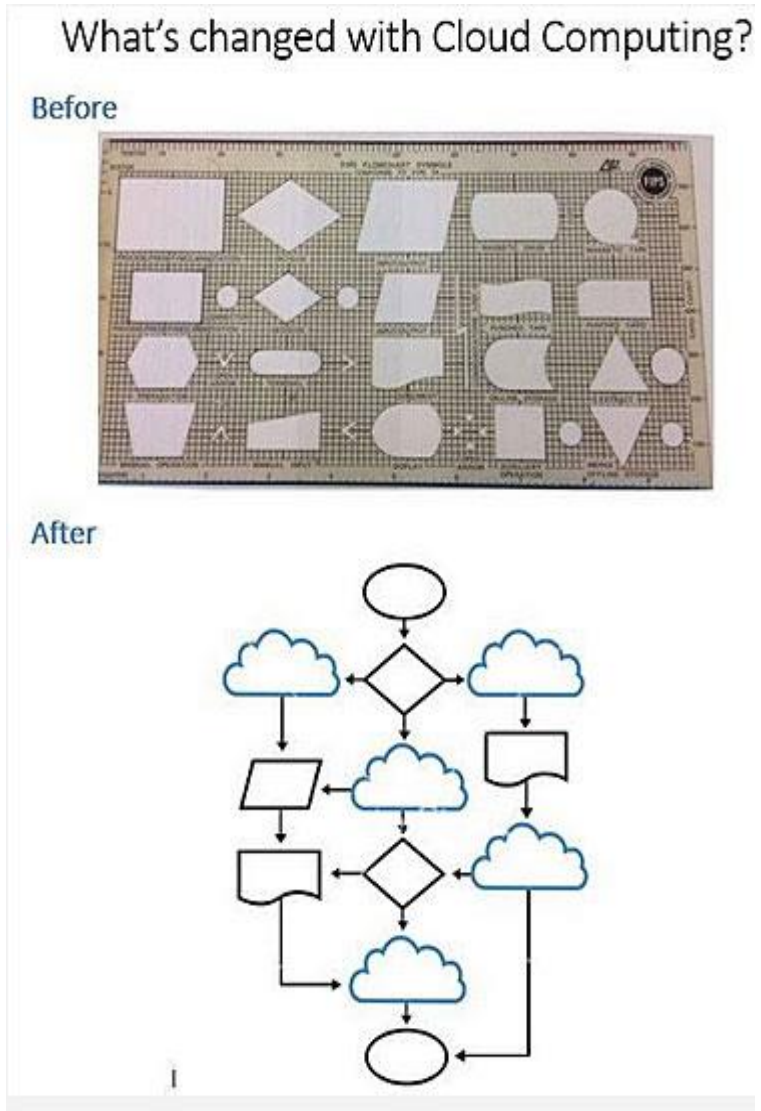
Table of Contents

FISMA Model - For Assessment and Authorization



FEDRAMP Model - For Assessment and Authorization

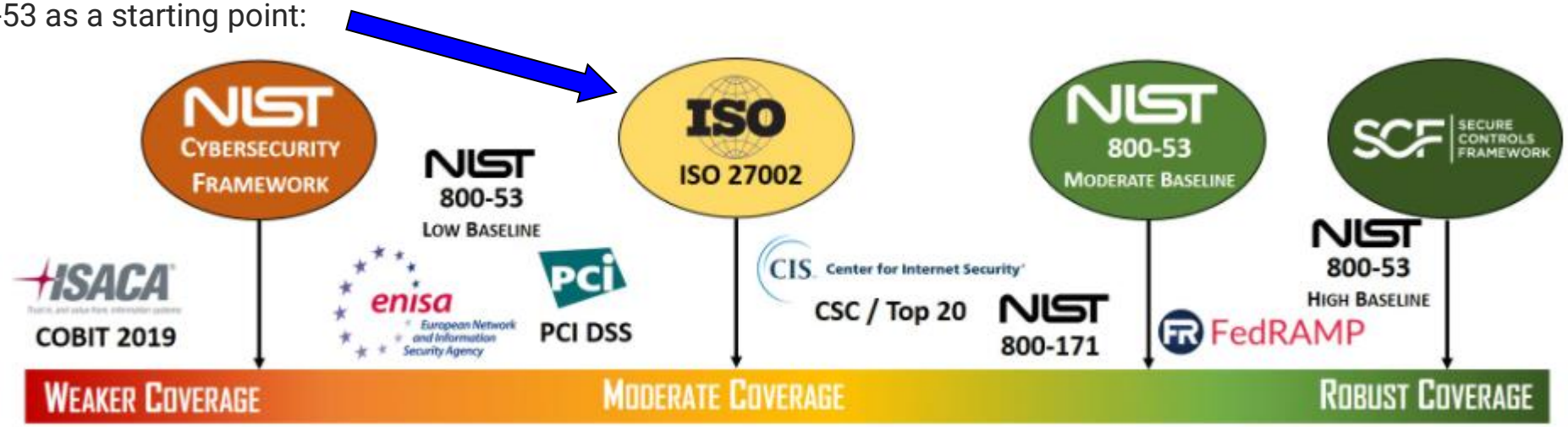




Which framework is right for my business?

- **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

Which framework is right for my business?

The 18 CIS Critical Security Controls

Formerly the SANS Critical Security Controls (SANS Top 20) these are now officially called the CIS Critical Security Controls (CIS Controls).

CIS Controls Version 8 combines and consolidates the CIS Controls by activities, rather than by who manages the devices. Physical devices, fixed boundaries, and discrete islands of security implementation are less important; this is reflected in v8 through revised terminology and grouping of Safeguards, resulting in a decrease of the number of Controls from 20 to 18.

Click on the individual CIS Control for more information:

CIS Control 1: Inventory and Control of Enterprise Assets

CIS Control 2: Inventory and Control of Software Assets

CIS Control 3: Data Protection

CIS Control 4: Secure Configuration of Enterprise Assets and Software

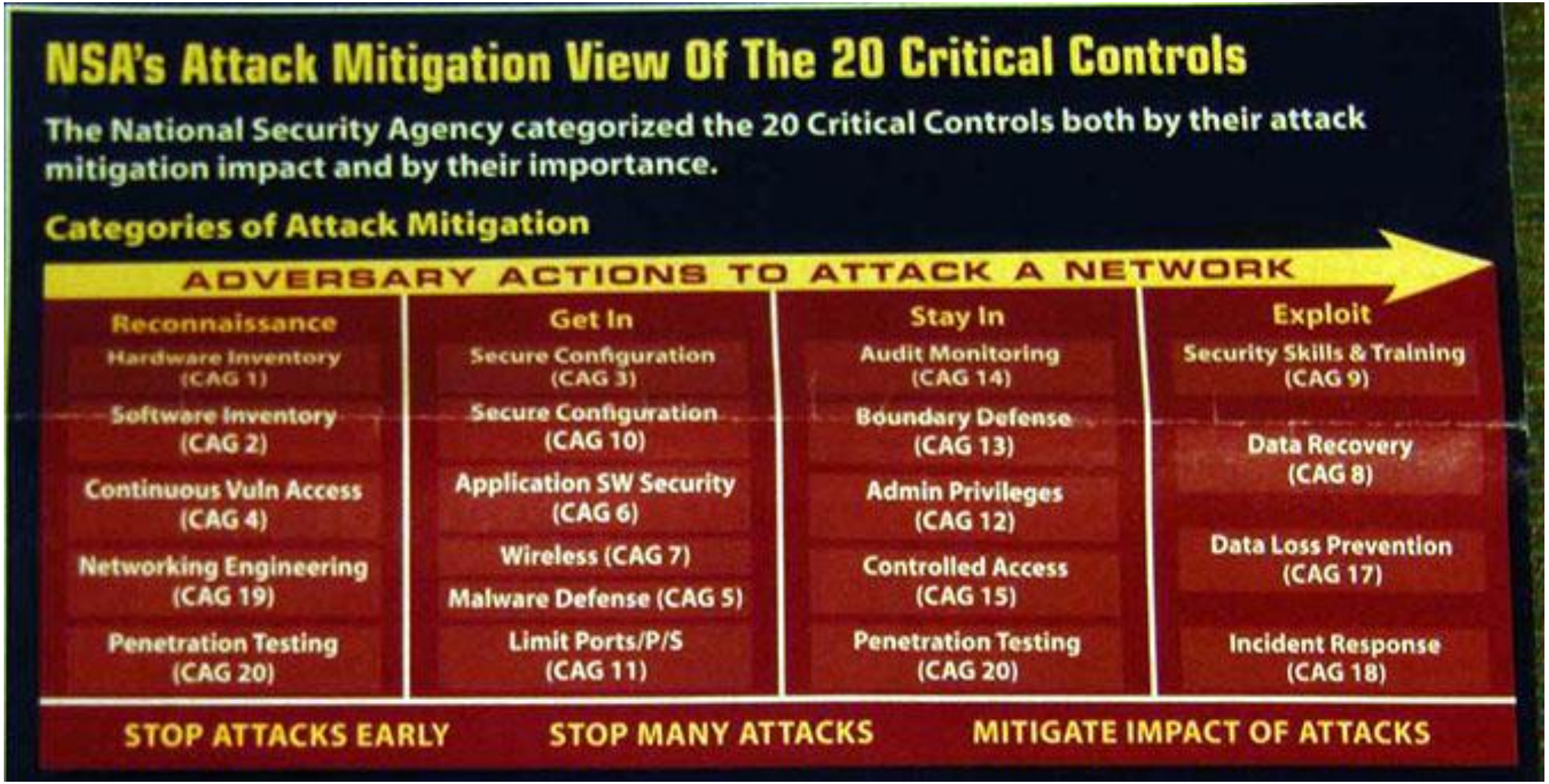
CIS Control 5: Account Management

CIS Center for Internet Security®

Creating Confidence in the Connected World.™

https://www.cisecurity.org/controls/cis-controls-list/

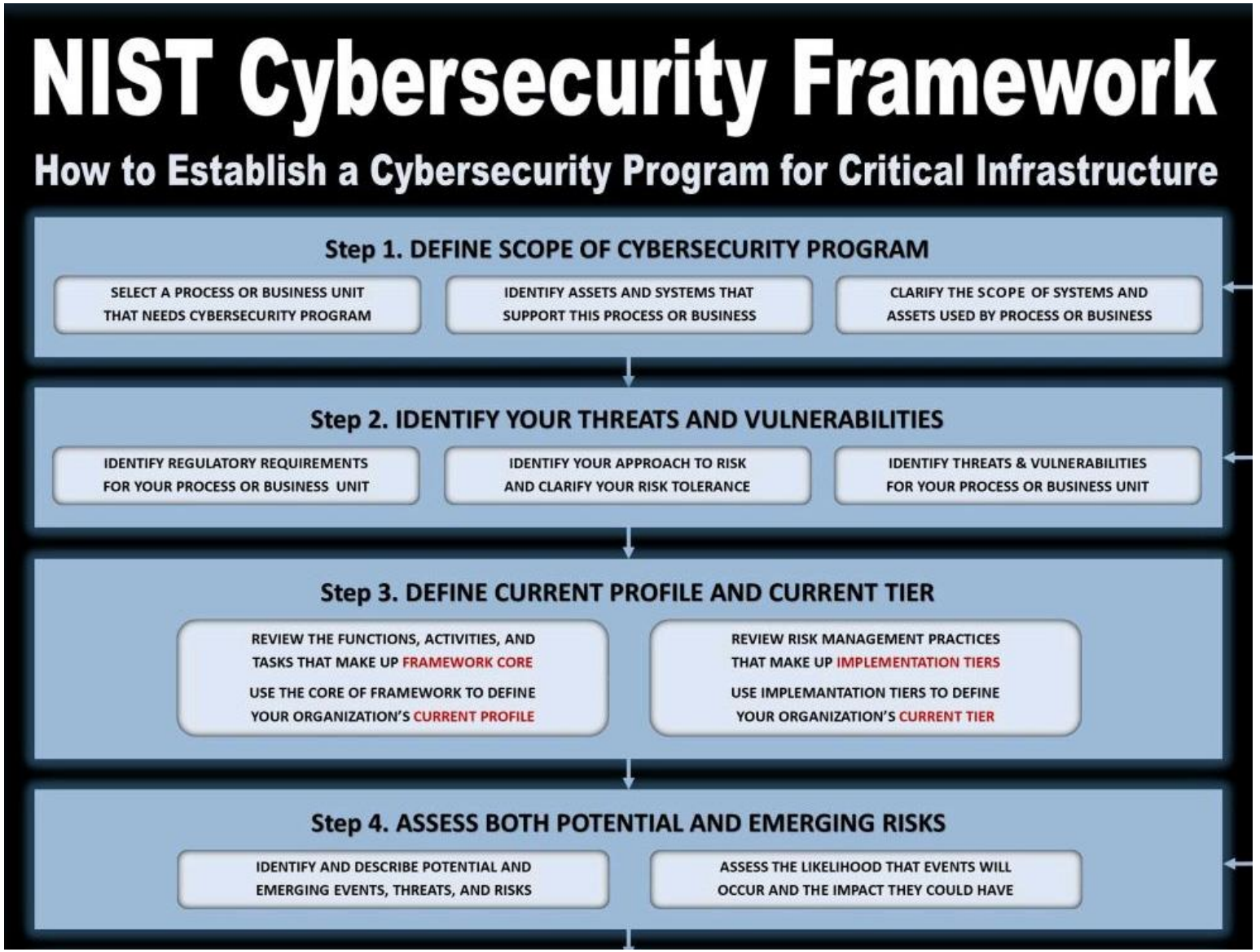
Which framework is right for my business?



NIST Cybersecurity Framework –

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.

NIST Cybersecurity Framework – https://www.praxiom.com



NIST Cybersecurity Framework – https://www.praxiom.com

Step 5. DESCRIBE TARGET PROFILE AND TARGET TIER

REVIEW THE FUNCTIONS, ACTIVITIES, AND TASKS THAT MAKE UP FRAMEWORK CORE

USE THE CORE OF FRAMEWORK TO DEFINE YOUR ORGANIZATION'S TARGET PROFILE

USE INPUT FROM STAKEHOLDERS TO REFINE YOUR TARGET PROFILE

REVIEW RISK MANAGEMENT PRACTICES THAT MAKE UP IMPLEMENTATION TIERS

USE IMPLEMANTATION TIERS TO DEFINE YOUR ORGANIZATION'S TARGET TIER

USE INPUT FROM STAKEHOLDERS TO REFINE YOUR TARGET TIER

Step 6. IDENTIFY GAPS IN YOUR CYBERSECURITY ACTIVITIES

IDENTIFY FRAMEWORK GAPS BY COMPARING CURRENT & TARGET PROFILES

PRIORITIZE FRAMEWORK GAPS BY CONSIDERING RISKS, COSTS, AND BENEFITS

IDENTIFY IMPLEMENTATION GAPS BY COMPARING CURRENT & TARGET TIERS

PRIORITIZE IMPLEMENATION GAPS BY CONSIDERING RISKS, COSTS, AND BENEFITS

Step 7. EXECUTE PLAN TO ESTABLISH CYBERSECURITY PROGRAM

CONSIDER HIGH PRIORITY GAPS

CONSIDER HIGH PRIORITY FRAMEWORK GAPS

CONSIDER HIGH PRIORITY IMPLEMENTATION GAPS

CREATE PLAN TO ADDRESS GAPS

DEFINE STEPS TO ADDRESS HIGH PRIORITY FRAMEWORK GAPS

DEFINE STEPS TO ADDRESS HIGH PRIORITY IMPLEMENTATION GAPS

EXECUTE PLAN TO ADDRESS GAPS

TAKE STEPS TO ADDRESS HIGH PRIORITY FRAMEWORK GAPS

TAKE STEPS TO ADDRESS HIGH PRIORITY IMPLEMENTATON GAPS

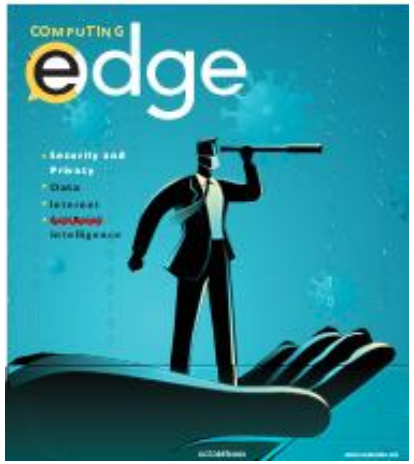
For more informatiion, see https://www.praxiom.com/cybersec.htm

Table of Contents

Global transformation caused by COVID-19

Artificial Intelligence (AI) in Agriculture

IEEE COMPUTER SOCIETY



Download PDF | View References | Generate 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

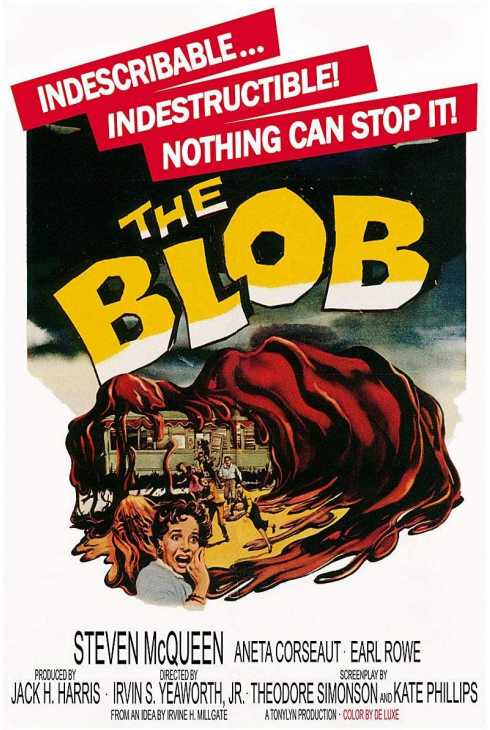
Abstract

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

Big Scary Monsters - Global transformation caused by COVID-19



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

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.

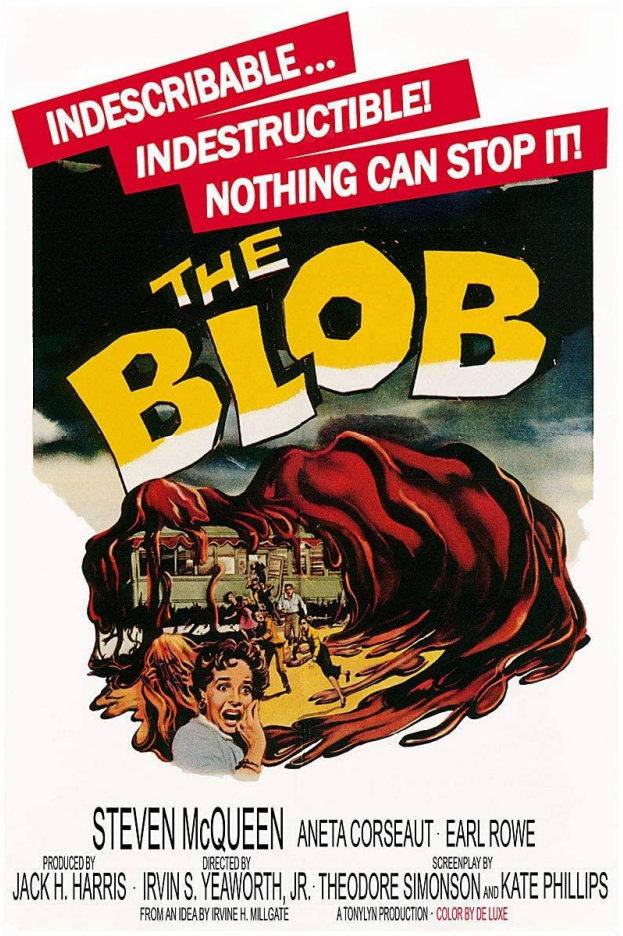
The FUD Factor – Fear, Uncertainty and Doubt

CSF Identify Categories related to COVID-19

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

US Cybersecurity and Infrastructure Security Agency (CISA)



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 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

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

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

SUPPLY CHAIN COMPROMISE

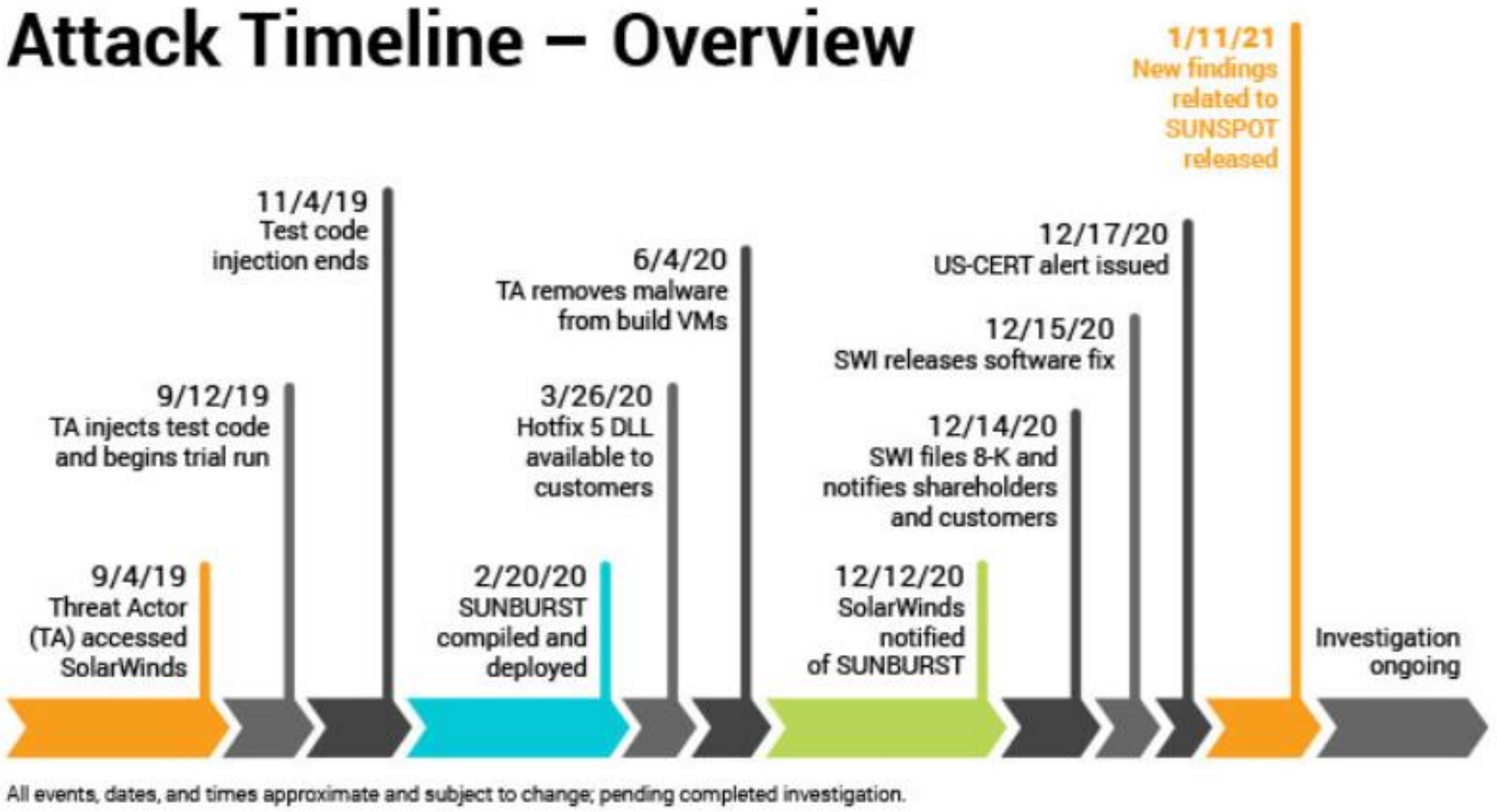
CISA is tracking a significant cyber incident impacting enterprise networks across federal, state, and local governments, as well as critical infrastructure entities and other private sector organizations. An advanced persistent threat (APT) actor is responsible for compromising the SolarWinds Orion 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

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



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

Taxonomy of Cloud Security Attacks

MITRE | ATT&CK

Matrices Tactics Techniques

Search

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK®

Getting Started | Take a Tour

Contribute | Blog

FAQ | Random Page

https://attack.mitre.org/

Cloud Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the following platforms: Azure AD, Office 365, Google Workspace, SaaS, IaaS.

View on the ATT&CK Navigator

Version Permalink

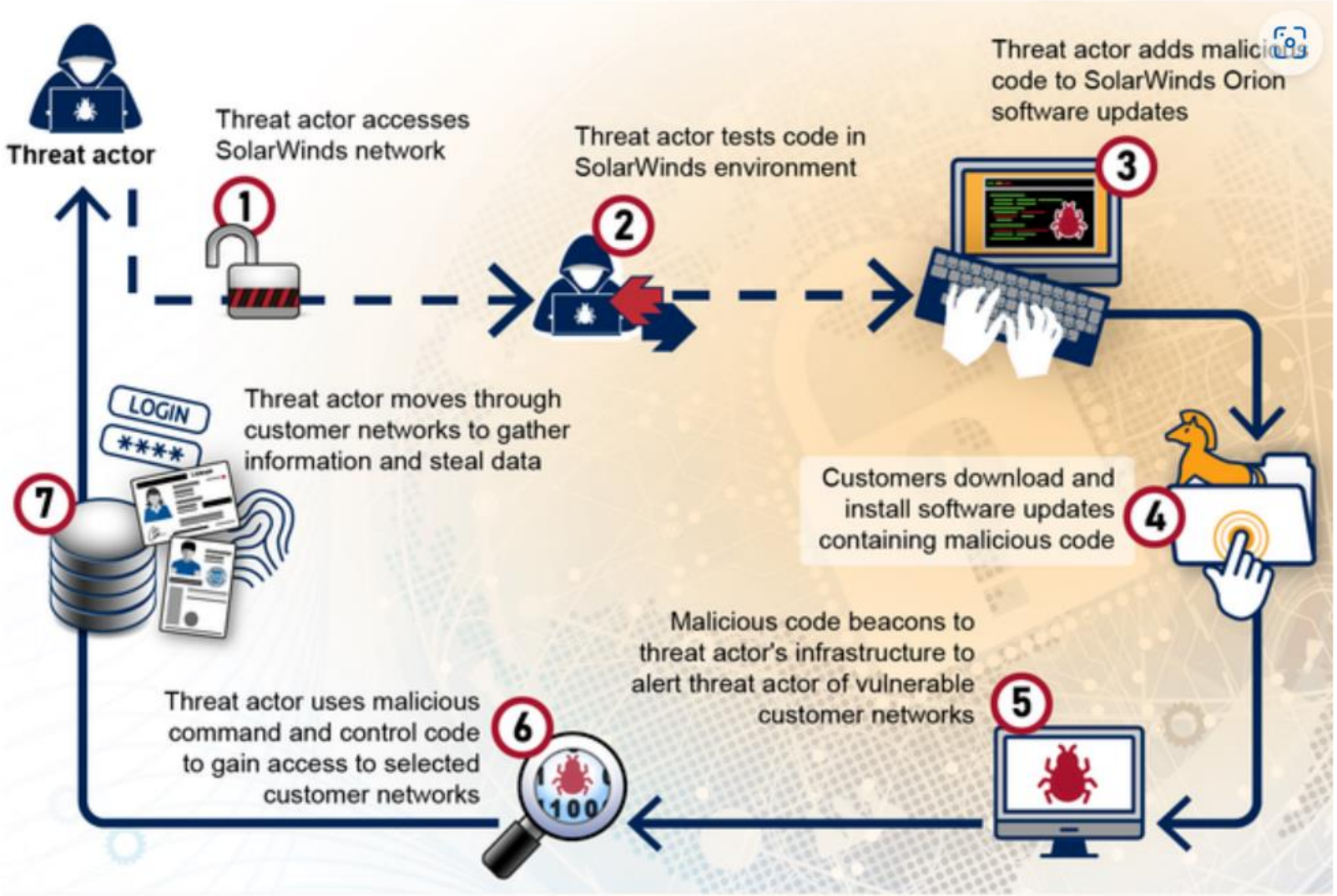
layout: side

show sub-techniques | hide sub-techniques | help

Initial Access (5 techniques)	Execution (1 techniques)	Persistence (5 techniques)	Privilege Escalation (2 techniques)	Defense Evasion (7 techniques)	Credential Access (5 techniques)	Discovery (12 techniques)
Drive-by Compromise	User Execution (1)	Account Manipulation (3)	Domain Policy Modification (1)	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)
Exploit Public-Facing Application		Create Account (1)	Valid Accounts (2)	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Infrastructure Discovery
Phishing (1)		Implant Internal Image		Impair Defenses (3)	Steal Application Access Token	Cloud Service Dashboard
Trusted Relationship		Office Application Startup (6)		Modify Cloud Compute Infrastructure (4)	Steal Web Session Cookie	Cloud Service Discovery
Valid Accounts (2)		Valid Accounts (2)		Unused/Unsupported Cloud Regions	Unsecured Credentials (2)	Cloud Storage Object Discovery
				Use Alternate Authentication Material (2)		
				Valid Accounts (2)		

SUNBURST - Solar Winds ORION NMS APT Attack (2019 - 2021) – GAO Report

Figure 1: Analysis of How a Threat Actor Exploited SolarWinds Orion Software



Source: GAO analysis of documentation from publicly released private industry and federal agency reports; images: kras99/stock.adobe.com, anna_leni/stock.adobe.com. | GAO-22-104746

No One Knows How Deep Russia's Hacking Rampage Goes

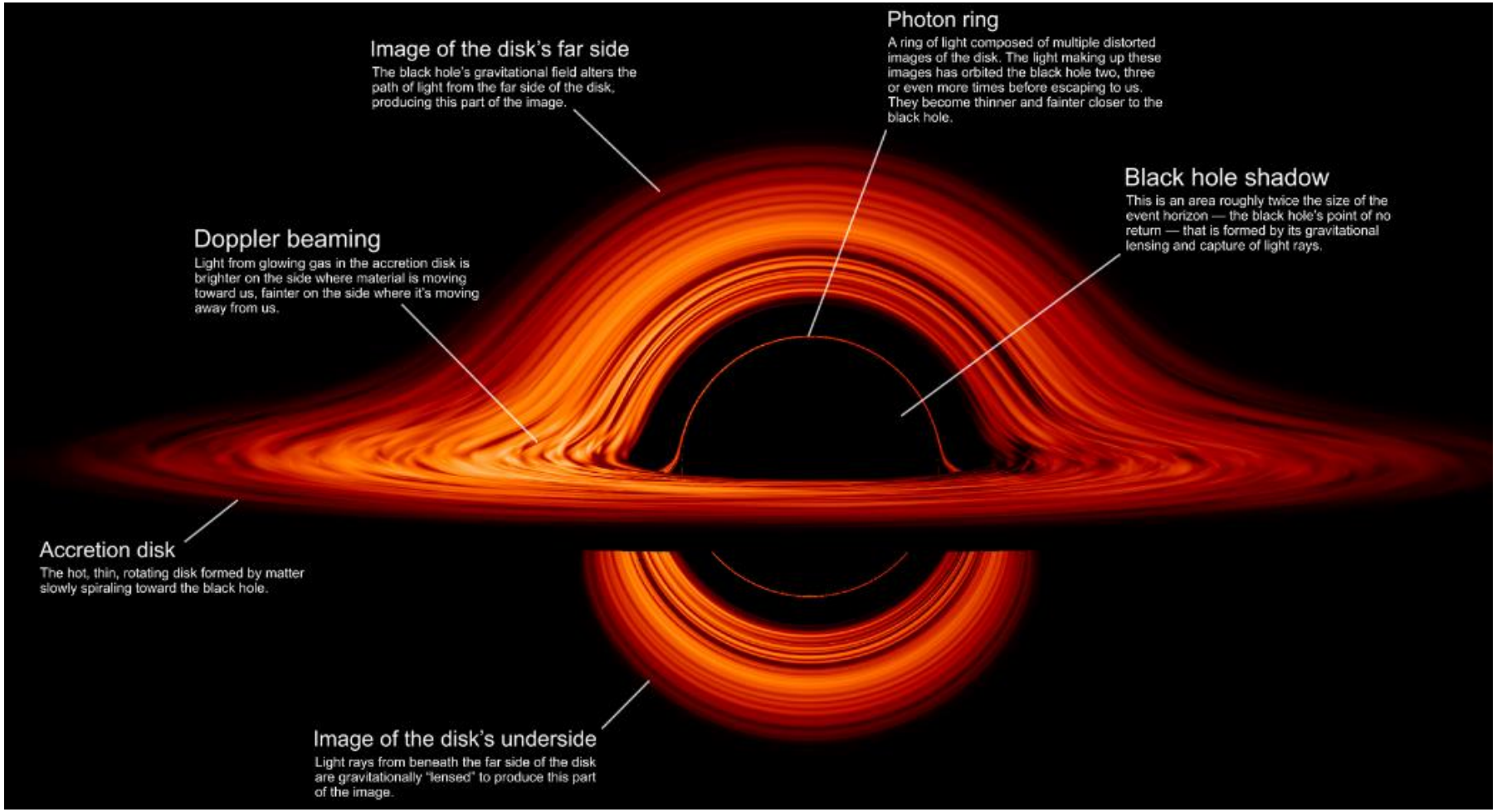
A supply chain attack against IT company SolarWinds has exposed as many as 18,000 companies to Cozy Bear's attacks.

- **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

- **Cleaning up SolarWinds hack may cost as much as $100 billion.** Government agencies, private corporations will spend months and billions of dollars to root out the Russian malicious code

- **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



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

Practical Risk Management Methods (PMI PMBOK)

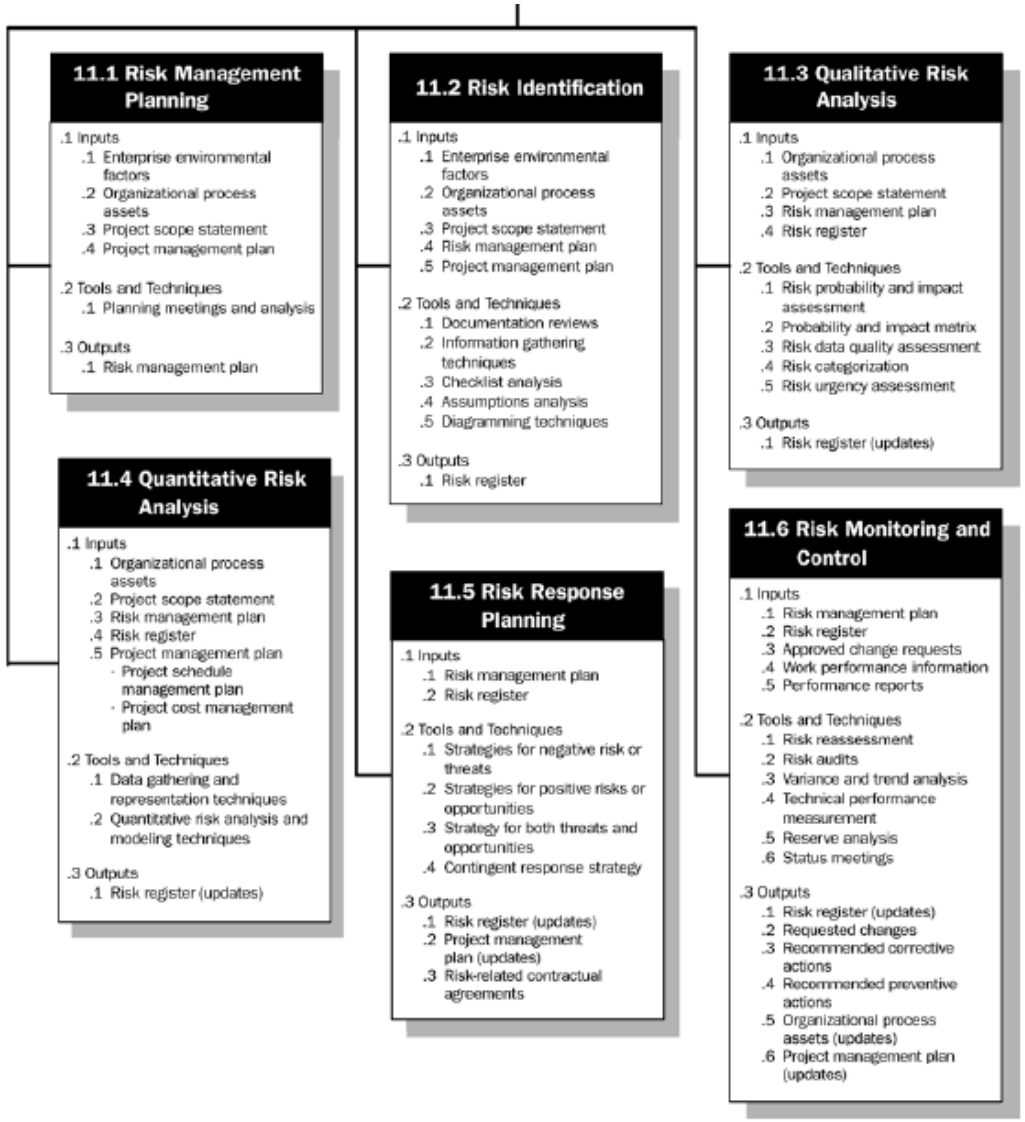


Figure 11-1. Project Risk Management Overview

A Guide to the
Project Management Body of Knowledge
Third Edition
(PMBOK® Guide)

Project Risk Management

Project Risk Management includes the processes concerned with conducting risk management planning, identification, analysis, responses, and monitoring and control on a project; most of these processes are updated throughout the project. The objectives of Project Risk Management are to increase the probability and impact of positive events, and decrease the probability and impact of events adverse to the project. Figure 11-1 provides an overview of the Project Risk Management processes, and Figure 11-2 provides a process flow diagram of those processes and their inputs, outputs, and other related Knowledge Area processes. The Project Risk Management processes include the following:

11.1 Risk Management Planning – deciding how to approach, plan, and execute the risk management activities for a project.

11.2 Risk Identification – determining which risks might affect the project and documenting their characteristics.

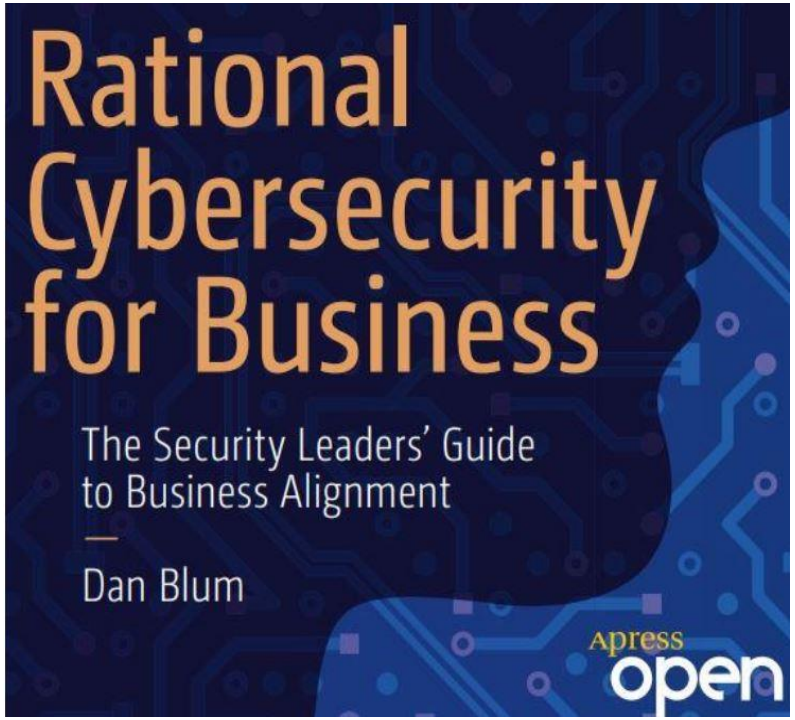
11.3 Qualitative Risk Analysis – prioritizing risks for subsequent further analysis or action by assessing and combining their probability of occurrence and impact.

11.4 Quantitative Risk Analysis – numerically analyzing the effect on overall project objectives of identified risks.

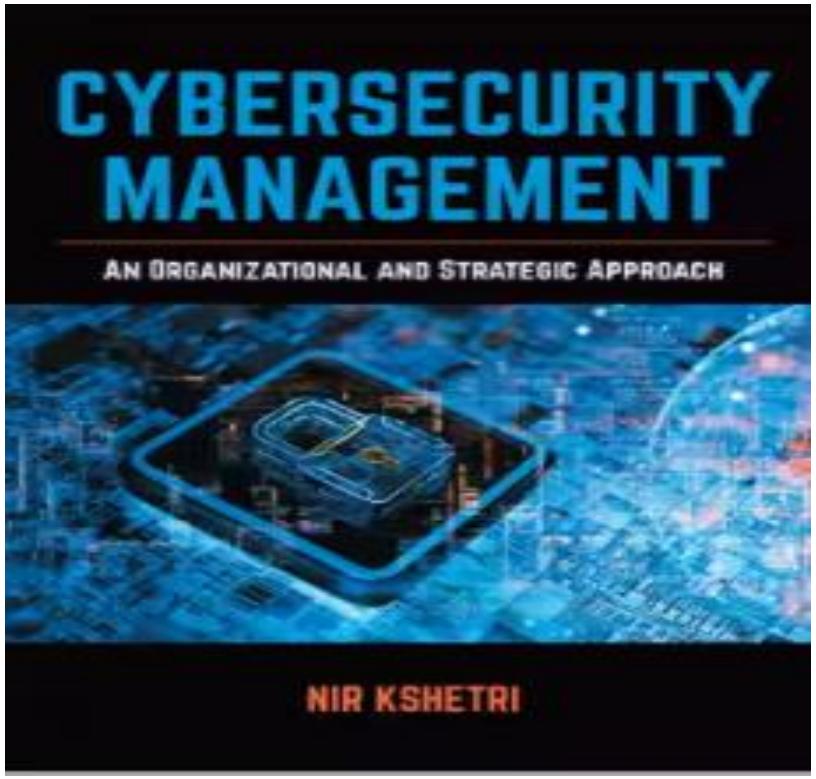
11.5 Risk Response Planning – developing options and actions to enhance opportunities, and to reduce threats to project objectives.

11.6 Risk Monitoring and Control – tracking identified risks, monitoring residual risks, identifying new risks, executing risk response plans, and evaluating their effectiveness throughout the project life cycle.

Taking Risk Management to the Boardroom

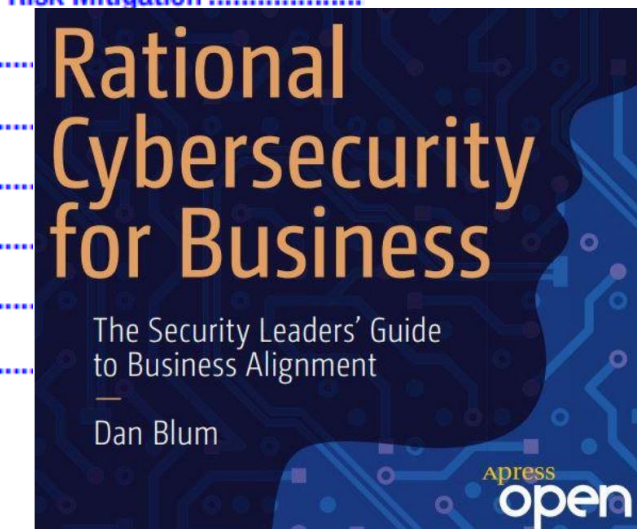


The first comprehensive field guide to cybersecurity-business alignment. Focuses on six areas to maximize the effectiveness of your cybersecurity program: risk management, control baseline, security culture, IT rationalization, access control, and cyber-resilience
•Includes more than 50 keys to alignment and advice on how to scale them for businesses of different types and sizes

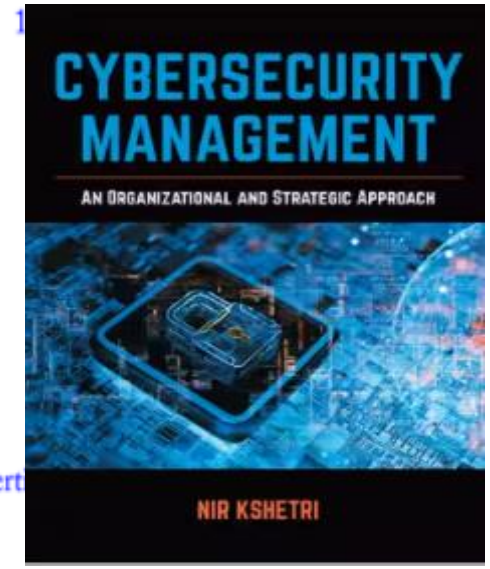


Cyberthreats are among the most critical issues facing the world today. *Cybersecurity Management* draws on case studies to analyze cybercrime at the macro level, and evaluates the strategic and organizational issues connected to cybersecurity. Cross-disciplinary in its focus, orientation, and scope, this book looks at emerging communication technologies that are currently under development to tackle emerging threats to data privacy.

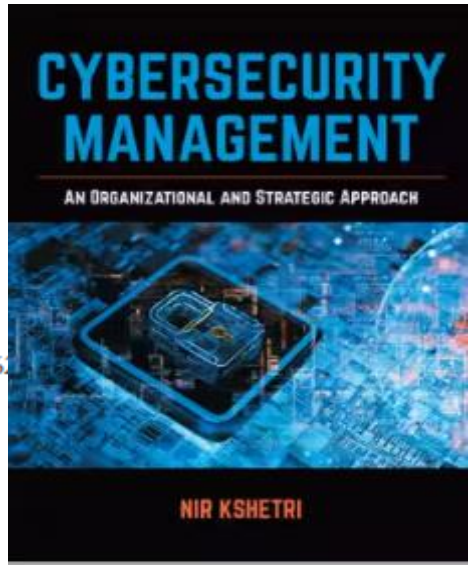
Rational Cybersecurity for Business – Dan Blum



Cybersecurity Management – Nir Kshetri



Cybersecurity Management – Nir Kshetri



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
- Tracking non-conformities and resolution
- Continuous improvement

Annex A deals with:
114 Optional controls for risk mitigation

ISO/IEC 27001 Controls v2022 vs 2013

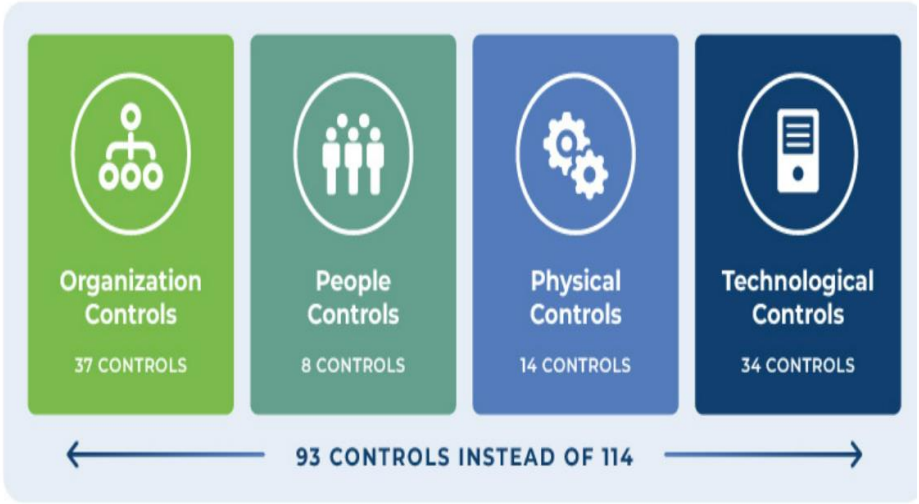
Information security policies	Organisation of information security	Human resources security	Asset management
Access control	Cryptography	Physical and environmental security	Operations security
Communications security	System acquisition, development and maintenance	Supplier relationships	Incident management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

What has changed in Annex A of ISO/IEC 27001?

- The updated Annex A of ISO/IEC 27001 based on ISO/IEC 27002 standard contains a list of possible information security controls. Annex A provides only information security controls and does not provide the control objective as in ISO/IEC 27001:2013.
- Annex A introduces 11 new information security controls, 58 updated controls, and 24 controls that have been merged with the existing controls. These controls are grouped into four categories.

A.5	A.6	A.7	A.8
Organizational controls	**People controls**	**Physical controls**	**Technological controls**
A.5.1-A.5.37	A.6.1-A.6.8	A.7.1-A.7.14	A.8.1-A.8.34

ISO 27002:2022 vs :2013 https://www.advantio.com/blog/whats-new-in-iso/iec-27002-2022-updates



To consolidate the increased number of controls in this version, 11 new controls have been added. Only 1 control from the previous version has been removed, and 57 controls that had similar objectives have been merged into 24 new controls.

Control	Type of control
5.7 Threat intelligence	Organizational
5.23 Information security for use of cloud services	Organizational
5.30 ICT readiness for business continuity	Organizational
7.4 Physical security monitoring	Physical
8.9 Configuration management	Technological
8.10 Information deletion	Technological
8.11 Data masking	Technological
8.12 Data leakage prevention	Technological
8.16 Monitoring activities	Technological
8.23 Web filtering	Technological
8.28 Secure coding	Technological

A Line of Business for a Certification Company (ISO 27001)

All Press Releases for January 30, 2015

Coalfire Receives Accreditation from ANAB as ISO 27001 Certification Body

Coalfire, a leading global provider of cyber risk management and compliance solutions, announced accreditation of its subsidiary, Coalfire ISO, Inc.

DENVER, CO, January 30, 2015 **/24-7PressRelease/** -- Coalfire, a leading global provider of cyber risk management and compliance solutions, announced accreditation of its subsidiary, Coalfire ISO, Inc. by the ANSI-ASQ National Accreditation Board (ANAB) to certify organizations to the ISO 27001 Information Security Standard. Coalfire is one of less than a handful of North American organizations that have achieved this prestigious accreditation from ANAB.

ANAB is an internationally-recognized U.S. accreditation body for information security management systems. ISO 27001 provides the blueprint for a risk-based information security management framework. ISO 27001 can be valuable as an operating framework for a growing organization laying the basic groundwork for information security in their business, or complex Fortune 500s designing a highly sophisticated risk-based management framework for all information security in the company.

COALFIRE ISO

CERTIFICATE NUMBER: 2018-012301

CERTIFICATE OF REGISTRATION

Information Security Management System (ISMS) – ISO/IEC 27001:2013

Coalfire ISO, Inc. certifies that the following organization operates an Information Security Management System (ISMS) that conforms to the requirements of ISO/IEC 27001:2013 per the scope and boundaries statement detailed below:

COMPANY:	SailPoint Technologies, Inc.	ADDRESS:	11120 Four Points Drive Suite 100 Austin, TX 78726 United States

Scope:

The certificate scope comprises the Information Security Management System supporting the operations underlying the following products and services offerings:

- IdentityIQ
  - IdentityIQ Compliance Manager
  - IdentityIQ Lifecycle Manager
  - IdentityIQ File Access Manager
  - IdentityIQ File Password Manager
  - Identity Security Integrations

Scope statement continued on the following page

ON BEHALF OF COALFIRE ISO:

COALFIRE ISO 27001 CERTIFIED ISO

ANAB ACCREDITED 9234

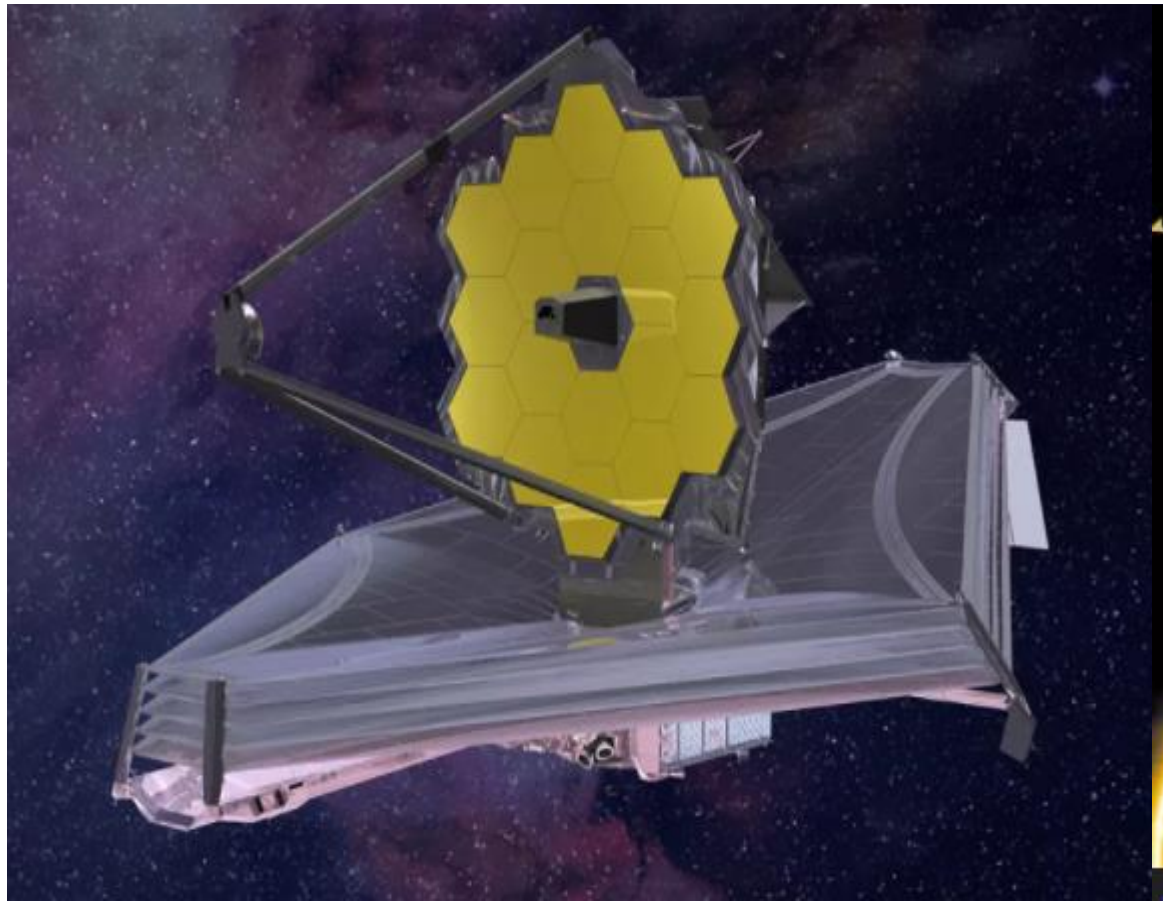
UKAS MANAGEMENT SYSTEMS

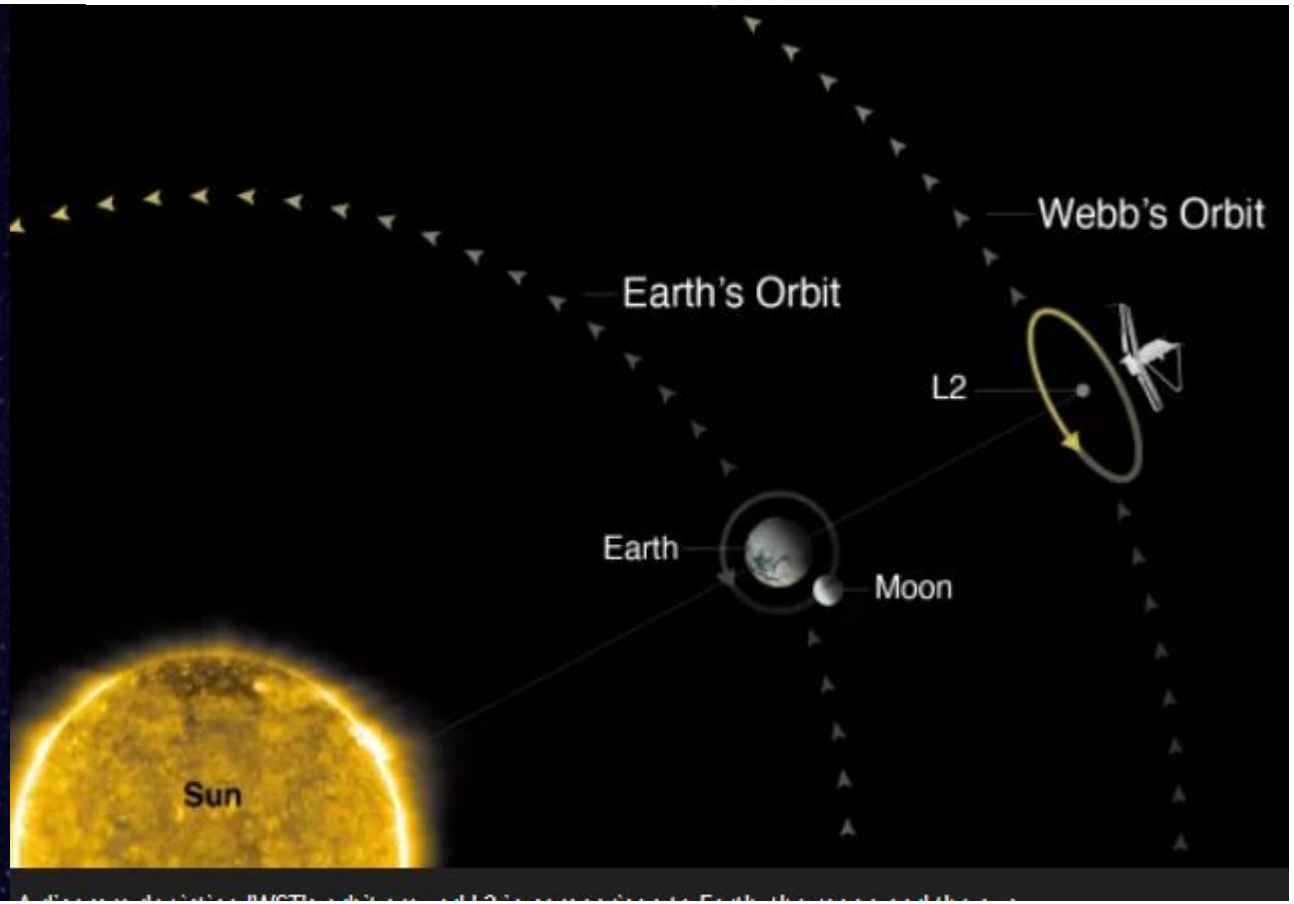
STATEMENT OF APPLICABILITY:
VERSION: 4.0
DATE: September 15, 2021

Original Registration Date:
January 23, 2018

Certificate Issuance Date:
December 17, 2021

Expiration Date:
December 2, 2022





https://www.space.com/james-webb-space-telescope-mission-explained

How the James Webb Space Telescope works in pictures

The James Webb Space Telescope, also known as Webb or JWST, is a high-capability space observatory designed to revolutionize fields of astronomy ranging from star formation to galaxy evolution and from the very first galaxies of the universe to the properties of planetary systems. However, because JWST is a project of unprecedented complexity, the mission has struggled to launch. What had initially been proposed as a $1 billion observatory launching in 2007 has become a $10 billion project launching in 2021.

You don’t need a weatherman to tell which way the wind blows.

Table of Contents

xG Impact on IT and Systems 2022 : xG Impact on Information Technology and Systems

https://www.computer.org/digital-library/magazine/it/cfp-info-tech-systems

Important Dates
Submissions Due: 25 November 2022

Publication: May/June 2023

IT Professional
Technology Solutions for the Enterprise

IT Professional seeks original and novel contributions describing research, cross-domain experimentation and practical case studies on the current and future directions of xG networks. 5G networks are becoming mainstream in the cellular and wireless communications domain requiring rigorous and wide-ranging study of their impact on Information Technologies and Systems. 5G and beyond (xG) is more than simply increase in speed and connecting more devices. xG heralds an era of far- and wide-ranging services, applications and systems that changes business, society and the government. For example, the low latency of xG networks opens up opportunities for data-intense AI applications to be deployed on IoT devices with potential for new business models and customer satisfaction. The need to explore the various impacts of xG networks is of immense contemporary interest. This special issue aims to explore the theory as well as the practice of the impact of 5G, 6G and beyond on IT and Systems. The intersection of xG with Cloud architectures, Network architectures, Convergence, Data science and analytics, Cybersecurity, Business Process optimization, and User experience are topics of interest. Furthermore, the architecture, design and deployment of xG systems that would enable configuration, optimization and recovery are also of interest. The discussions in this special issue should throw fresh lights on expanding network coverage, reducing latency and providing enhanced security. This special issue aspires to advance the body of knowledge on xG networks and their industrial applicability.

In particular, topics of interest include but are not limited to:

Direction of xG network Generations
xG and impact on Cloud architectures (cloud native, metaverse)
Changes in Information Systems development, deployment and operations due to xG
How xG is impacting and impacted by Cybersecurity
xG and challenges to Data Science and Artificial Intelligence
Access network modifications due to xG

When	Jun 11, 2022 - Nov 25, 2022
Where	IT Professional Magazine
Submission Deadline	Nov 25, 2022
Notification Due	Jan 10, 2023
Final Version Due	Feb 10, 2023

Categories 5G 6G

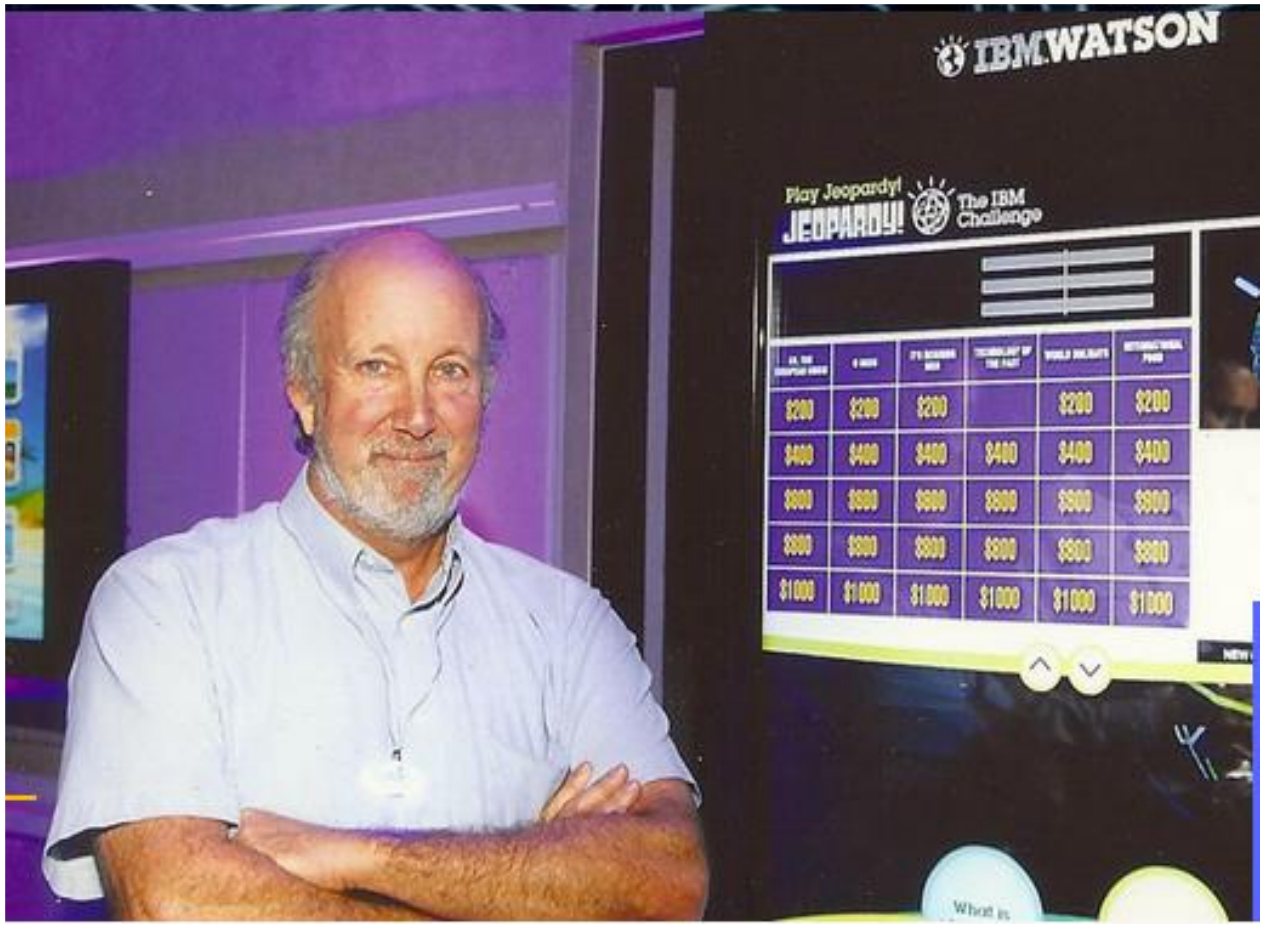
Call For Papers

References – Roadmaps for Risk Management

- IT Pro Special Issue on Communications Recovery and Resilience - Editor's Column" by Tim Weil, Bhuvan Unhelkar, John Callahan, Jason W. Rupe, Keith Sherringham https://www.computer.org/csdl/magazine/it/2020/06/09250314/1oxkJTuIsMg
- 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
- **Cybersecurity Management** by Nir Kshetri, Kshetri, Nir. *Cybersecurity Management: An Organizational and Strategic Approach*, University of Toronto Press. https://www.book2look.com/book/9781487523626
- T. Weil, R. Kuhn, M. Chang https://www.securityfeeds.us/cyberthreats-and-security-ieee-it-professional-special-issue
- **Rational Cybersecurity for Business** by Dan Blum, 2020 | 1st ed.Apress (Verlag), 978-1-4842-5951-1 (ISBN) .https://link.springer.com/content/pdf/10.1007%2F978-1-4842-5952-8.pdf
- 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-shape-reality-post-covid-19
- “Five functions of the cybersecurity framework,” NIST. Apr. 2018. [Online]. Available: Cybersecurity framework,” NIST. Apr. 2018. [Online]. https://www.nist.gov/cyberframework/online-learning/five-functions
- “CISA INSIGHTS: Risk Management for Novel Coronavirus (COVID-19),” CISA. Mar. 18, 2020. [Online]. Available: CISA Insights - Risk Management for Novel Coronavirus https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf
- GAO Federal Response to SolarWinds and Microsoft Exchange Incidents https://www.gao.gov/products/gao-22-104746
- Risk is a Four Letter Word (SecurityFeeds) - https://www.youtube.com/watch?v=hF4VbX6Nmf4

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