Life Sciences & Health Care, Medical Device Manufacturing and Cybersecurity, A Strategy

Presented by:
Robin Basham, CEO, Founder, EnterpriseGRC Solutions

Agenda

EnterpriseGRC Solutions, Inc.

1. Life Science and Health Care (LSHC) – Market, Players, Opportunities
2. Frameworks, Standards & Tools, How CISO's Address MDM Cybersecurity
3. Mapping and Tagging – Unification within GRC and Cybersecurity Risk Management
4. Integration Progress – Facilitated Compliance Management
5. Investment in Licenses and Partners

POLL #1

EnterpriseGRC Solutions, Inc.

Over the last 18 months

A) No change in how I receive Medical Care

B) Some technology - Met via Web with Med Prof

C) Used a device that sent info over Web

D) Implanted a device in my body

1

1 Life Science and Health Care (LSHC) – Market, Players, Opportunities

As Life Science & Health Care Industry is valued at $173 billion -> $208 billion in 2023 – The FDA Faces Increasing Cybersecurity Requirements

EnterpriseGRC Solutions, Inc.

Medtronic	Johnson & Johnson	Philips	GE Healthcare	Siemens Healthineers	Fresenius	Abbott Laboratories	Becton Dickinson	Cardinal Health	Stryker Corporation

FDA U.S. FOOD & DRUG ADMINISTRATION

Home / Medical Devices / Digital Health / Cybersecurity

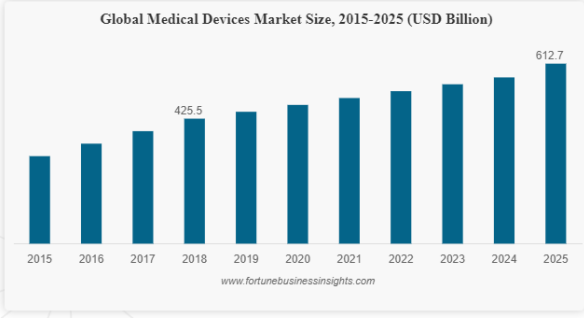
Cybersecurity

All legally-marketed medical devices have benefits and risks. The FDA allows devices to be marketed when there is a reasonable assurance that the benefits to patients outweigh the risks.

Medical devices are increasingly connected to the Internet, hospital networks, and other medical devices to provide features that improve health care and increase the ability of health care providers to treat patients. These same features also increase the risk of potential cybersecurity threats. Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device.

Threats and vulnerabilities cannot be eliminated, therefore, reducing cybersecurity risks is especially challenging. The heath care environment is complex, and manufacturers, hospitals, and facilities must work together to manage cybersecurity risks.

Source: https://www.selectusa.gov/medical-technology-industry-united-states



https://www.fortunebusinessinsights.com/industry-reports/medical-devices-market-100085

Heroes v. Innovators = Cyber-ready v. Closing Up Shop

EnterpriseGRC Solutions, Inc.

Abbott CONSUMERS HEALTHCARE PROFESSIONALS CAREERS ABOUT ABBOTT SEARCH

HOME > NEWSROOM > PRESS RELEASES

PRESS RELEASES

BACK TO PRESS RELEASES

ABBOTT LAUNCHES MOLECULAR POINT-OF-CARE TEST TO DETECT NOVEL CORONAVIR

- The Abbott ID NOW™ COVID-19 test brings rapid testing to the front lines
- Test to run on Abbott's point-of-care ID NOW platform - a portable instrument that can be deployed where testing is needed most
- ID NOW has the largest molecular point-of-care installed base in the U.S. and is available in a wide range of healthcare settings
- Abbott will be making ID NOW COVID-19 tests available next week and expects to ramp up manufacturing to deliver 50,000 tests per da
- This is the company's second test to receive Emergency Use Authorization by the FDA for COVID-19 detection; combined, Abbott expects

Cepheid wins emergency use nod from FDA for bedside coronavirus test

MARCH 23, 2020 BY SEAN WHOOLEY — LEAVE A COMMENT

Danaher Corp. (NYSE:DHR) subsidiary Cepheid announced that it received emergency use authorization from the FDA for its bedside Xpert Xpress SARS-CoV-2 test for detecting the virus causing the COVID-19 outbreak.

The rapid molecular diagnostic test is designed to detect the SARS-CoV-2 virus causing coronavirus while operating on any of Cepheid's GeneXpert systems worldwide, with a detection time of approximately 45 minutes, according to a news release.

Cepheid chief medical & technology officer Dr. David Persing said in the release that, in developing the COVID-19 test, the company used the design of its Xpert Xpress flue/RSV cartridge technology to target the viral genome and provide rapid detection of current and potential variants of SARS-CoV-2. The outcome is a test that offers results in multiple settings where actionable treatment information is required in a timely manner.

A Bloomberg report stated that Sunnyvale, Calif.-based Cepheid's test is the 13th one allowed on the market by the FDA and the first that clinicians can use at the bedside. The report also said that Cepheid plans to begin shipping tests next week. The company is joining in on the trend of companies lending a hand in the search for effective testing for the disease.

"Cepheid currently has nearly 5,000 GeneXpert systems in the U.S. capable of point-of-care testing and for use in hospitals," Cepheid resident Warren Kocmond said in the news release. "Our automated systems do not require users to have specialty training to perform testing — they are capable of running 24/7, with many systems already doing so today."

FILED UNDER: DIAGNOSTICS, FEATURED, FOOD & DRUG ADMINSTRATION (FDA), GENOMICS/MOLECULAR DIAGNOSTICS, REGULATORY/COMPLIANCE
TAGGED WITH: CEPHEID, CORONAVIRUS, COVID-19, DANAHER CORP., FDA

URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication

Safety Communications
- 2020 Safety Communications
- 2019 Safety Communications
- 2018 Safety Communications
- 2017 Safety Communications

Date Issued: October 1, 2019

The U.S. Food and Drug Administration (FDA) is informing patients, health care providers and facility staff, and manufacturers about cybersecurity vulnerabilities that may introduce risks for certain medical devices and hospital networks. The FDA is not aware of any confirmed adverse events related to these vulnerabilities. However, software to exploit these vulnerabilities is already publicly available.

A security firm has identified 11 vulnerabilities, named "URGENT/11." These vulnerabilities may allow anyone to remotely take control of the medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent device function.

These vulnerabilities exist in IPnet, a third-party software component that supports network communications between computers. Though the IPnet software may no longer be supported by the original software vendor, some manufacturers have a license that allows them to continue to use it without support. Therefore, the software may be incorporated into other software applications, equipment, and systems which may be used

Content current as of: 10/01/2019

Regulated Product(s): Medical Devices

Forbes Billionaires Innovation Leadership Money Business Small Business Lifestyle Lis

Topline: Despite the coronavirus weighing heavily on the stock market—
S&P 500 to drop 15% over the last montl
companies are seeing increased demand
rrent environment as more people stay a

stocks that offer compelling opportuniti
ling to analysts from Stifel and Credit Sui

e healthcare space, Credit Suisse recomm
nufacturers like **Medtronic (MDT)** and
), which stand to benefit amid higher d
at the coronavirus pandemic—the stock
hare, respectively.

her top pick from Credit Suisse is **Merck**
largest pharmaceutical companies in th
identifies as an ideal defensive dividend
erse business climate."

the coronavirus causing more people to stay indoors and self-
te, companies like **AdaptHealth Corp. (AHCO)**, one of the
st providers of home medical equipment in the U.S., "can
ately benefit" from the outbreak thanks to higher demand,
rding to Stifel.

- Stifel similarly likes virtual healthcare company **Teladoc (TDOC)**, which facilitates digital doctors visits for remote patients; while the

Biotech

Pfizer, BioNTech strike COVID-19 deal, commit multiple R&D sites to vaccine development

by Nick Paul Taylor | Mar 17, 2020 7:28am

Pfizer and BioNTech have decided not to let financial details hold up their collaboration on a vaccine against COVID-19. (Tracy Staton)

Pfizer has teamed up with BioNTech to co-develop and distribute a mRNA vaccine against COVID-19 outside of China. The partners plan to use multiple R&D sites in the U.S. and Germany to accelerate the progress of a vaccine that is due to begin clinical testing in humans by the end of April.

BioNTech and Pfizer have both referred to talks about a COVID-19 partnership in recent weeks, most recently yesterday when the German mRNA specialist issued a statement on the status of its vaccine and related deal-making. The latest advance in the partnering discussions clears BioNTech and Pfizer to immediately start working together on a vaccine against the novel SARS-CoV-2 coronavirus.

https://www.forbes.com/sites/sergeiklebnikov/2020/03/28/20-more-stock-picks-for-the-coronavirus-economy-according-to-market-experts/#474837ea19f2

GxP Maturity (a.k.a. Good Manufacturing Practices) Makes All The Difference in Rapid Response to Pandemic – but still is not likely to go far enough.

Risk & Cybersecurity Requirements: Recent mandates in the Medical Device Market (MDM) – Under the US FDA

EnterpriseGRC Solutions, Inc.

*"… amongst **healthcare stakeholders** … where **addressing medical device risk has formerly focused on functional safety, and safety-related risk (to the exclusion of cybersecurity) or the protection of data, multiple approaches are now actively addressing the lifecycle risks and potential harm from cybersecurity incidents**.*

*Medical devices manufacturers (MDM) are recommended to undertake a cybersecurity maturity assessment to identify and prioritize areas for improvement. This should include product lifecycle security, stipulated in **emerging assessment schemes**, which will be articulated in **healthcare procurement**. **Mature incident response plans and processes are essential for all healthcare entities**, in anticipation of the inevitable cybersecurity event."*

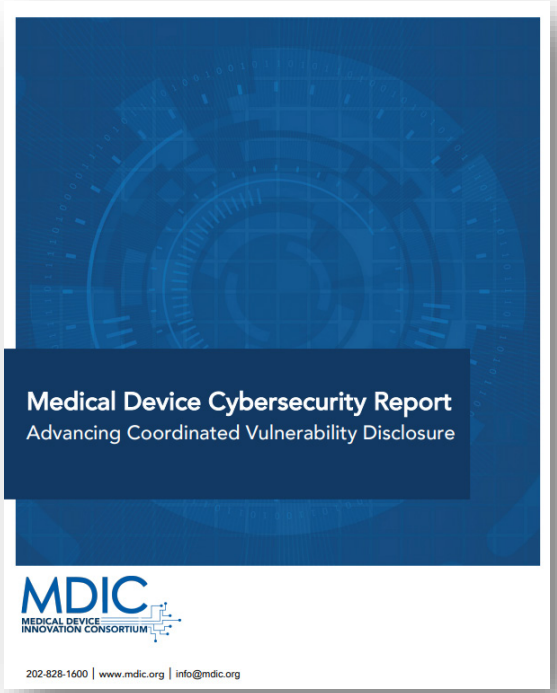
https://www.bsigroup.com/LocalFiles/EN-AU/ISO%2013485%20Medical%20Devices/Whitepapers/White_Paper Cybersecurity_of_medical_devices.pdf

Recent FDA mandates impact Medical Device Security and Extend beyond GxP Good Manufacturing to full Device Lifecycle

EnterpriseGRC Solutions, Inc.

As medical devices and healthcare environments become interconnected … the risk of **cybersecurity vulnerabilities** impacting patient **safety** and **privacy** increases significantly. The Food and Drug Administration (FDA) now takes significant steps to develop policies and guidance to assist medical device manufacturers (MDMs) addressing cybersecurity-related regulatory issues.

Stakeholders in the medical device industry closely examine how they can proactively address product security in an ***ever-changing environment*** to quickly and effectively reduce any risks posed to patients. FDA guidance documents emphasize that medical device cybersecurity concerns must be addressed not only during the design and development of medical devices, but also throughout the device lifecycle as potential cybersecurity vulnerabilities emerge.



*US FDA Cybersecurity Notifications page https://www.fda.gov/medical-devices/digital-health/cybersecurity#risks

https://mdic.org/wp-content/uploads/2018/10/MDIC-CybersecurityReport.pdf

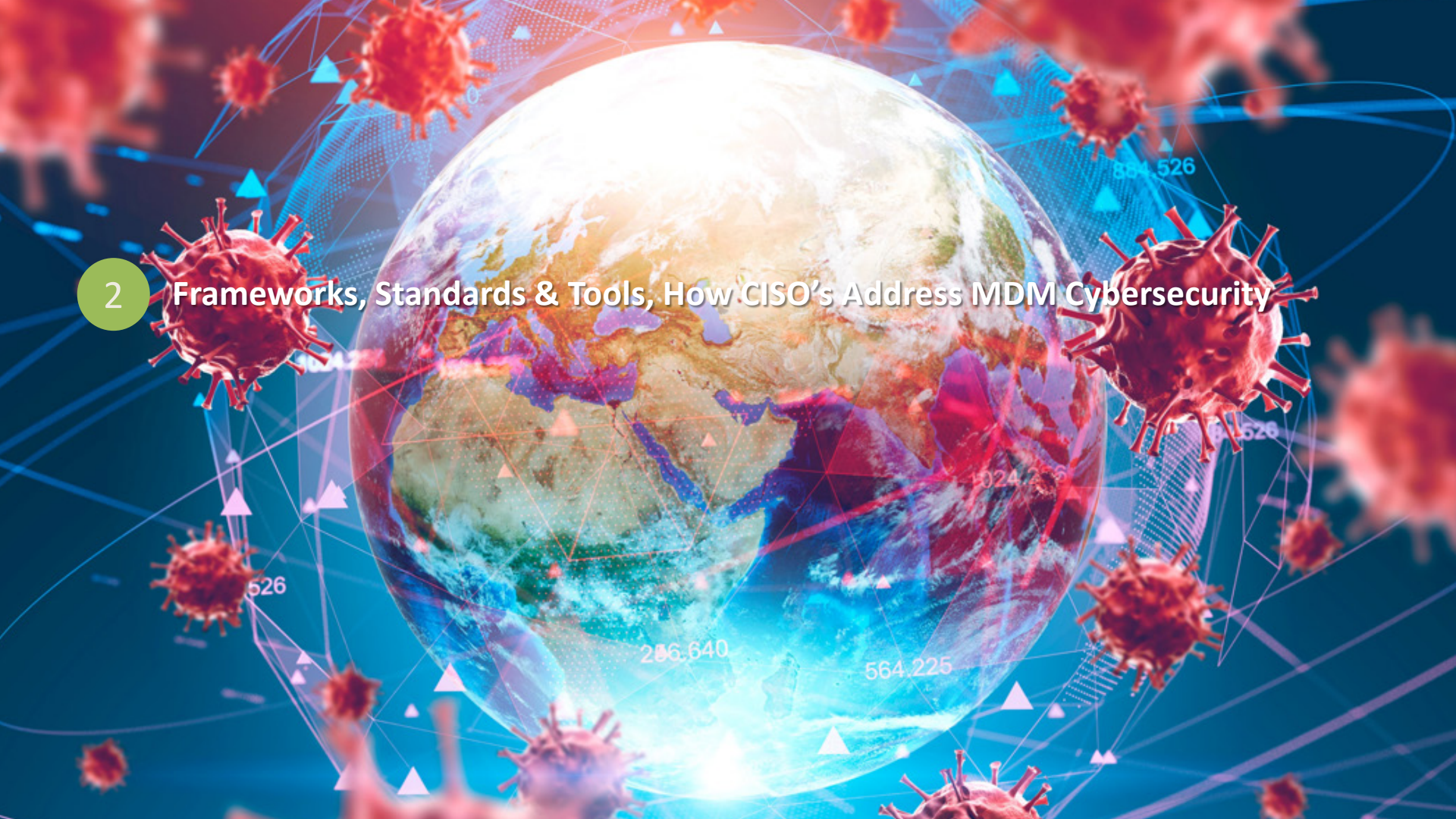
Immediately Required Cyber Security Standards and Laws that Govern or Enable The Medical Device Market (MDM)

EnterpriseGRC Solutions, Inc.

Term	Definition
CFR	Code of Federal Regulations. The CFR is the codification of the general and permanent rules and regulations (sometimes called administrative law) published in the Federal Register by the executive departments and agencies of the federal government of the United States.
GxP	Cumulative term used to refer to the global regulations and guidelines that include, but are not limited to, Good Manufacturing Practice (GMP), Good Laboratory Practice (GLP), Good Clinical Practices (GCP), Good Pharmacovigilance Practices (GPvP) and Good Distribution Practices (GDP) references
GAMP	Good automated manufacturing practice

- **GAMP® 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems***
- **Title 21 CFR Part 11 & Title 21 CFR Part 820 QMS Requirements**
- **Title 45 CFR § 164 HIPAA - HITECH**
- **Eudralex Volume 4 Annex 11 (Others may apply)**
- ISO/IEC 27001:2013 € and ISO/IEC 27002:2013 € or
- **ISO/IEC 27799:2016 € and ISO/IEC 27002:2013 €**
- **ISO 13485:2016 - MEDICAL DEVICES - A PRACTICAL GUIDE FOR MEDICAL DEVICES***
- **ISO 14971:2019 Medical devices — Application of risk management to medical devices***
- **HITRUST v9.3***
- NIST Cybersecurity Framework v1.1

***Associated License Fee and *Necessary* for LSHC**



2 Frameworks, Standards & Tools, How CISO's Address MDM Cybersecurity

Chief Risk, Chief Security, and Chief Information Officer walk into a bar.

EnterpriseGRC Solutions, Inc.

Bartender asks:

- Who ordered policies that control and mitigate the risk lifecycle including all supporting environments?
- Who captures, interprets and provides evidence that a control is operating effectively?
- Who aligns a Vulnerability Program as necessary to operate business and as needed for routine FDA inspection?
- Who establishes technical and manufacturing objectives that meet the needs of the LSHC stakeholders?

Poll #2

EnterpriseGRC Solutions, Inc.

Responsibility for Medical Device Security should be controlled by:

A) IT

B) IT & Security

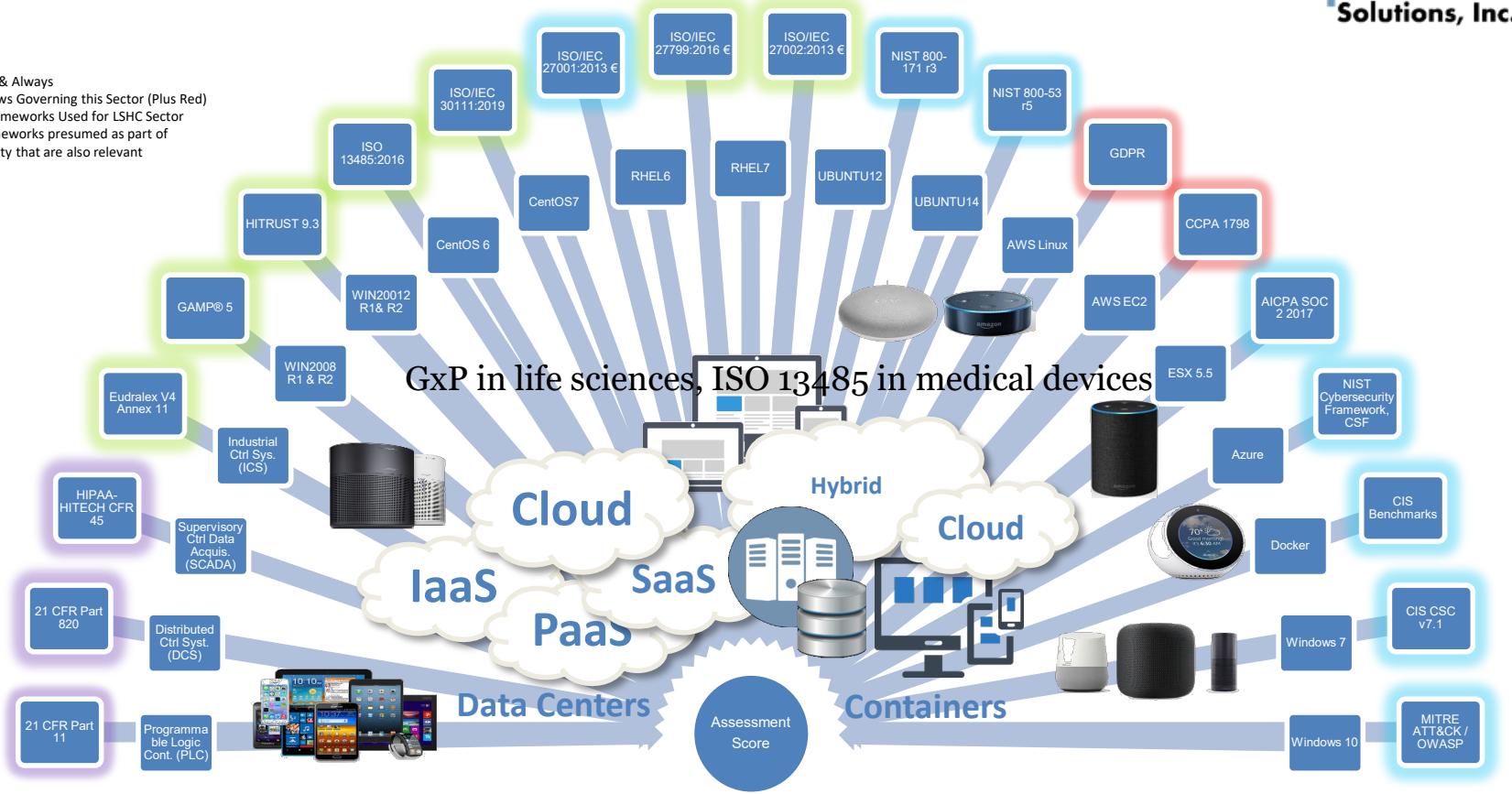
C) Product Engineering

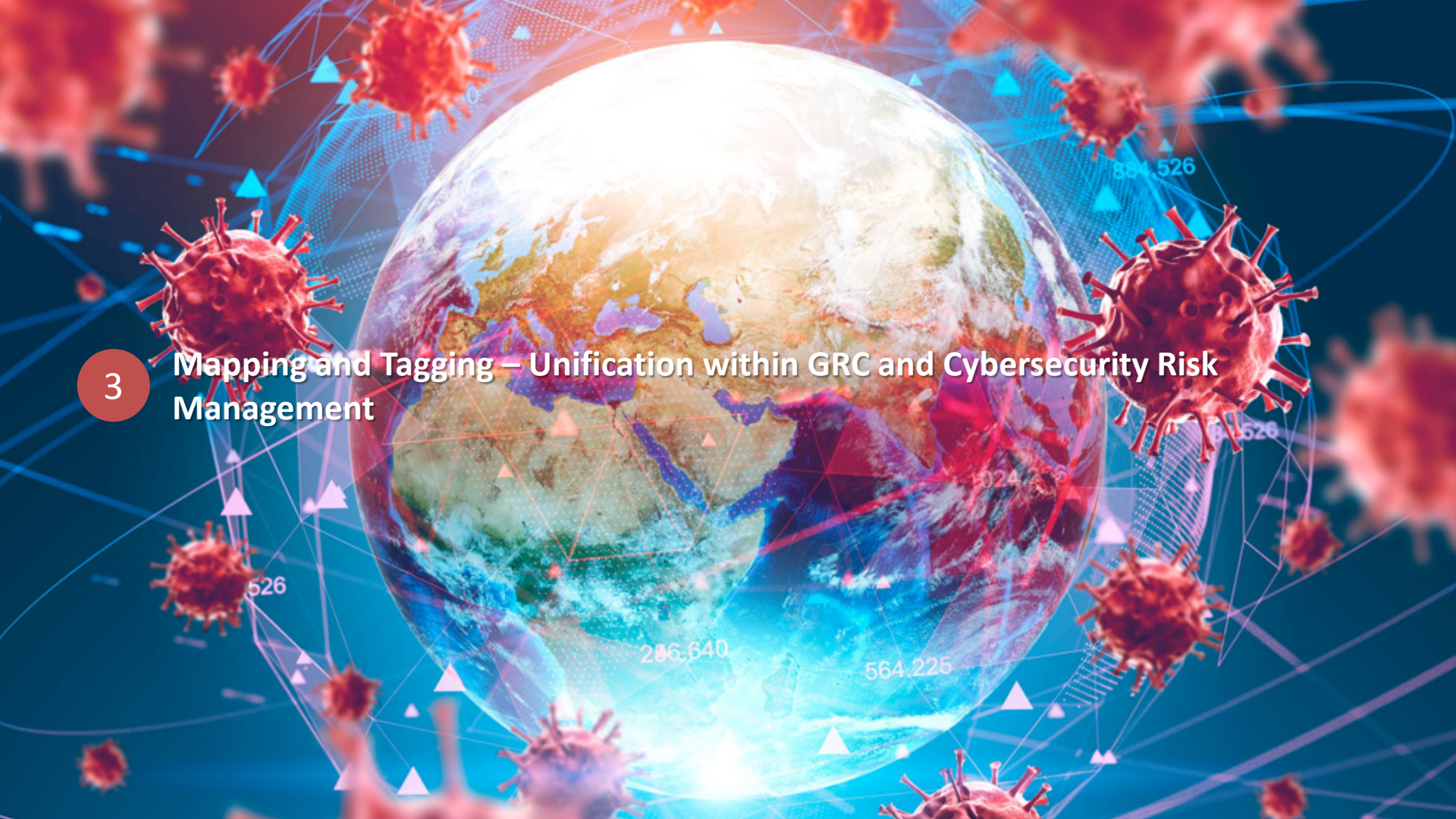
D) Product Engineering, Security and IT

The Universe of Life Science & Health Care

EnterpriseGRC Solutions, Inc.

Red = Now & Always
Purple = Laws Governing this Sector (Plus Red)
Green = Frameworks Used for LSHC Sector
Blue = Frameworks presumed as part of Cybersecurity that are also relevant

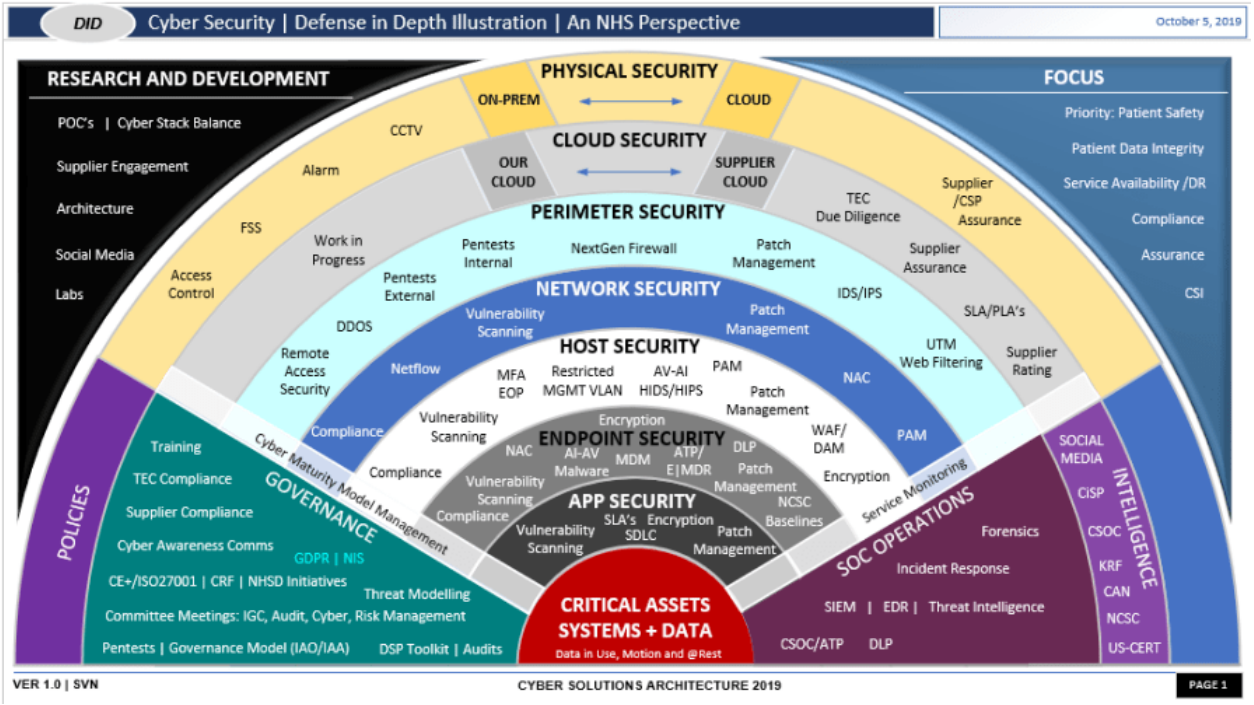




3 Mapping and Tagging – Unification within GRC and Cybersecurity Risk Management

Models Seek to Organize Threats, Technologies, Treatments OR Model Risk Assessment Procedure, but usually not both

EnterpriseGRC Solutions, Inc.

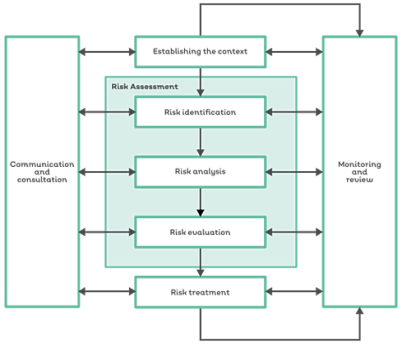


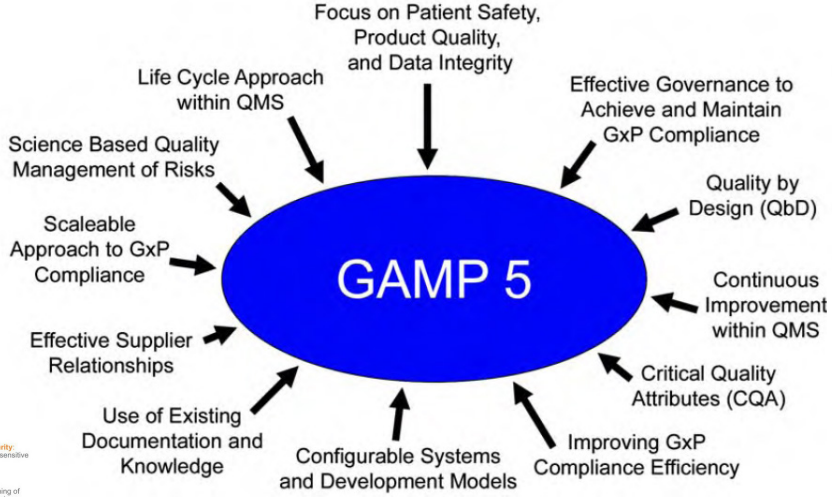
≠

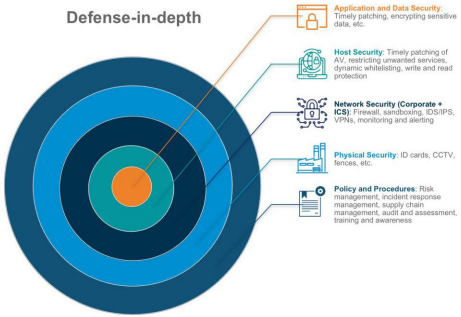
Risk Identification
↓
Business Risk Assessment
↓
Scope & Boundary Definition
↓
Risk Measurement
↓
Risk Action Plan
↓
Risk Acceptance
↓
Safeguard Selection
↓
Risk Assessment Commitment

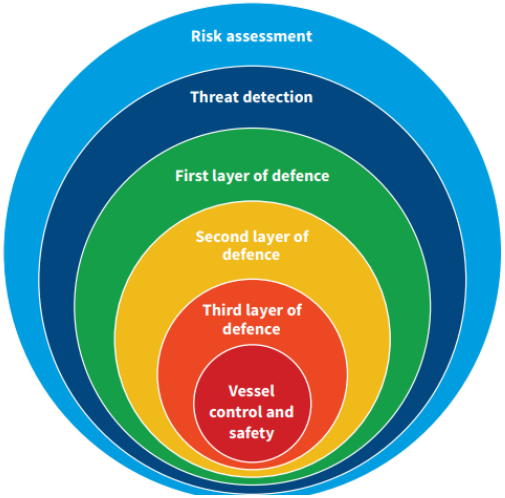
Risk Models Vary by Business Role – Differ on the What, Why & How

EnterpriseGRC Solutions, Inc.









Regulation, Process, Threat, and Assessments Don't Tie Out

EnterpriseGRC Solutions, Inc.

- HIPAA-HITECH CFR 45
- 21 CFR Part 820
- 21 CFR Part 11
- Eudralex V4 Annex 11
- GAMP® 5
- HITRUST 9.3
- ISO 13485:2016
- ISO/IEC 30111:2019
- ISO/IEC 27799:2016 €
- ISO/IEC 27002:2013 €
- GDPR
- CCPA 1798

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE NVD

- General +
- Vulnerabilities +
- Vulnerability Metrics +
- Products +
- Configurations (CCE)
- Contact NVD
- Other Sites +

CVSS/CWE from CVE List now Supported!

CVSS Version 3.1 Official Support!

New NVD CVE/CPE API and Legacy SOAP Service Retirement!

OWASP

MITRE | ATT&CK®

×

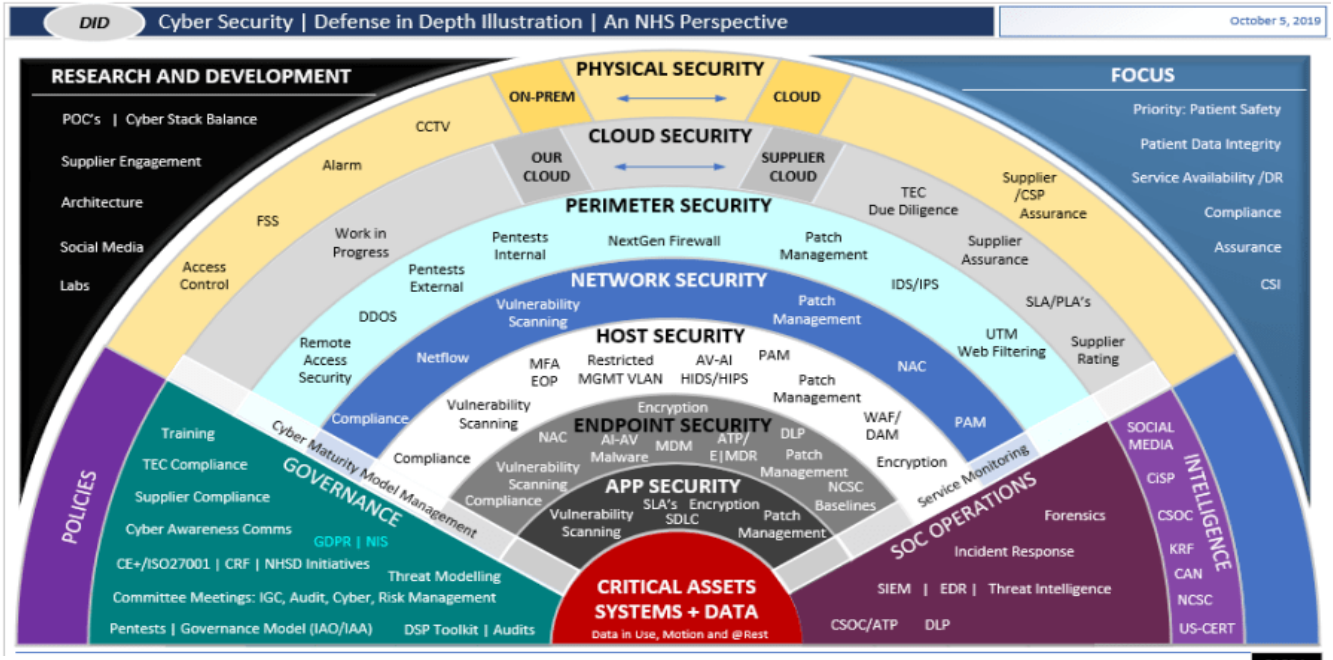
+

- Risk Identification
- Business Risk Assessment
- Scope & Boundary Definition
- Risk Measurement
- Risk Action Plan
- Risk Acceptance
- Safeguard Selection
- Risk Assessment Commitment

Cyber Security – NHS Perspective

EnterpriseGRC Solutions, Inc.

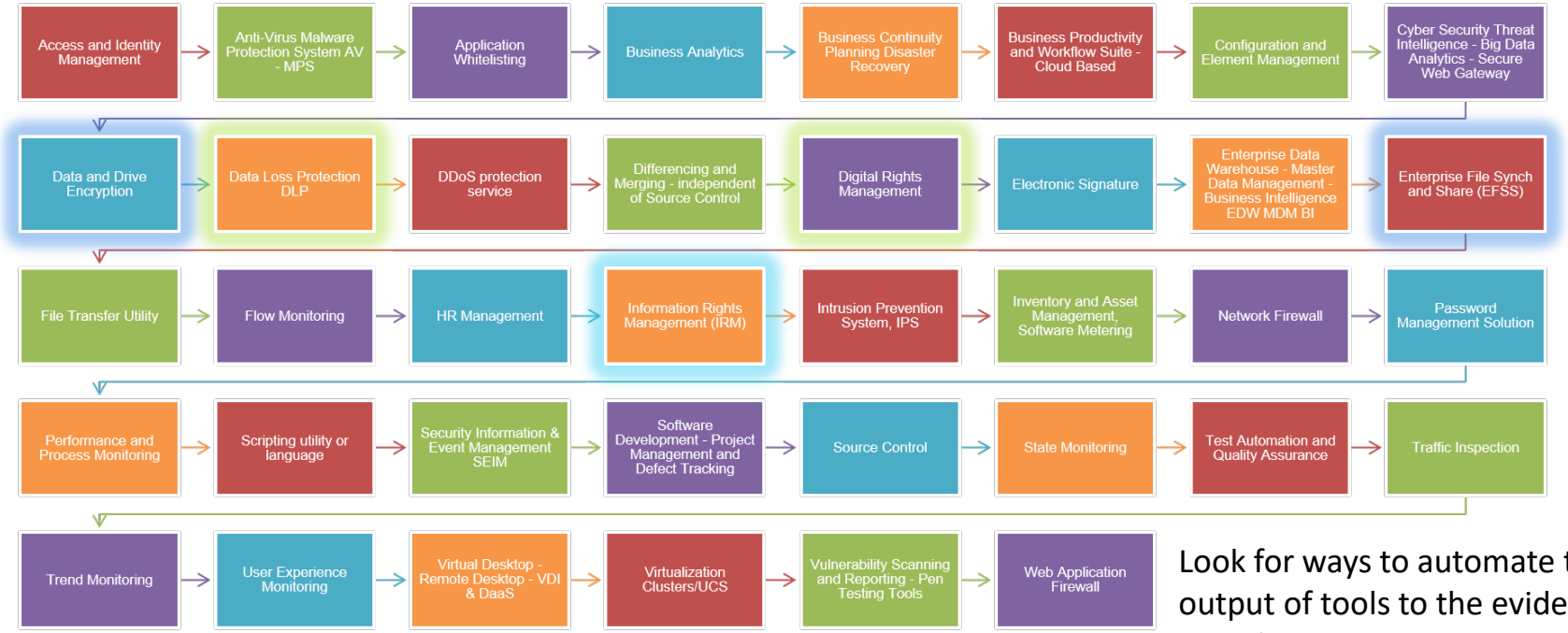
- ISO/IEC 27001:2013 €
- ISO/IEC 27002:2013 €
- NIST 800-171 r3
- NIST 800-53 r5
- AICPA SOC 2 2017
- NIST Cybersecurity Framework, CSF
- CIS Benchmarks
- CIS CSC v7.1
- MITRE ATT&CK / OWASP



National Health Service / National Health Agency

Security Architecture Select Tools Used and Covered in Cyber Security Risk Assessment:

EnterpriseGRC Solutions, Inc.



Look for ways to automate the output of tools to the evidence of compliance

Look to Increase Common Threat Language as Tagging

EnterpriseGRC Solutions, Inc.

- Supply Chain Tampering
- Technology adoption dramatically expands the threat landscape
- IoT leaks
- Algorithms compromise integrity
- Rogue governments use terrorist groups to launch cyberattacks
- APT
- Unmet board expectations
- Researchers silenced to hide security vulnerabilities
- Cyber insurance safety net is pulled away
- Governments become increasingly interventionist

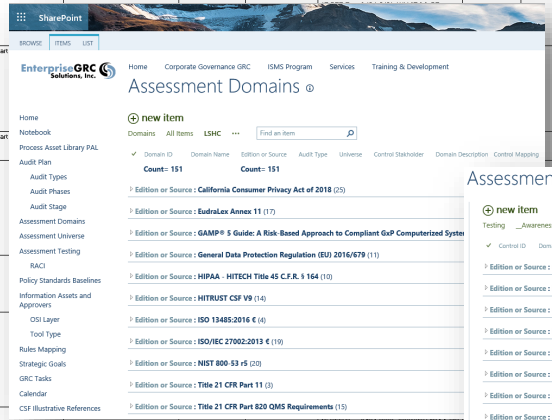
- Regulations fragment the cloud
- Criminal capabilities expand gaps in international policing
- INJECTION
- BROKEN AUTHENTICATION & SESSION MANAGEMENT
- CROSS-SITE SCRIPTING (XSS)
- INSECURE DIRECT OBJECT REFERENCES
- SECURITY MISCONFIGURATIONS
- MISSING FUNCTION LEVEL ACCESS CONTROL
- CROSS-SITE REQUEST FORGERY (CSRF)
- USING COMPONENTS WITH KNOWN VULNERABILITES
- UNVALIDATED REQUESTS AND FORWARDS

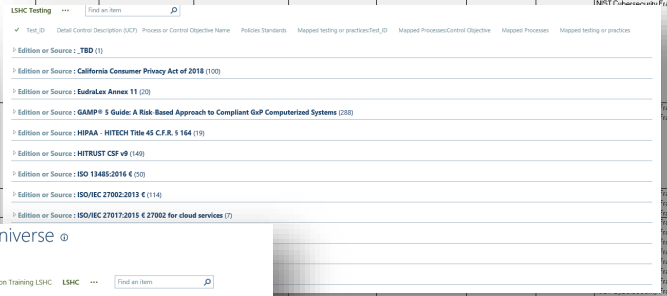
4 Integration Progress – Facilitated Compliance Management

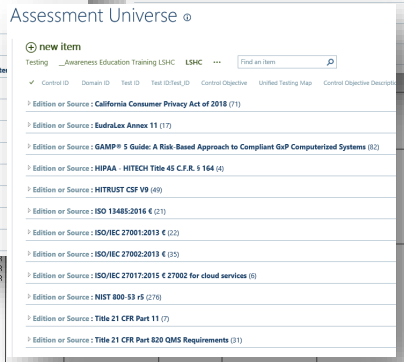
We Leverage Mapping: HITRUST provides recommendations for mapping, which we leverage but do not reproduce commercially

EnterpriseGRC Solutions, Inc.

HITRUST CSF v9.3	21 CFR 11	45 CFR HIPAA.BN	45 CFR HIPAA.GE	45 CFR HIPAA.PR	45 CFR HIPAA.SR	AICPA TSP 100	CCPA 1798	CIS Controls v7.1	EU GDPR	ISO/IEC 27001:2013	ISO/IEC 27002:2013	ISO/IEC 27799:2016	ISO/IEC 29100:2011 – Information technology – Security techniques –	ISO/IEC 29151:2017 – Information technology – Security techniques	NIST Cybersecurity Framework v1.1	NIST SP 800-171r2 (DFARS)	NIST SP 800-53 r4	PCI DSS v3.2.1
01.r Password Management System					45 CFR Part § 164.308(a)(5)(ii)(D) HPAA SR						ISO/IEC 27002:2013 9.2.4 ISO/IEC 27002:2013 9.4.3	ISO/IEC 27799:2016 9.2.4 ISO/IEC 27799:2016 9.4.3			NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.DS-5	NIST SP 800-171R2 3.5.7 NIST SP 800-171R2 3.5.8	NIST SP 800-53 R4 IA-2 NIST SP 800-53 R4 IA-5 NIST SP 800-53 R4 IA-5(1)	PCI DSS v3.2.12.1 PCI DSS v3.2.18.2.1
01.s Use of System Utilities					45 CFR Part § 164.308(a)(3)(ii) HIPAA SR 45 CFR Part § 164.308(a)(3)(ii)(A) HPAA SR 45 CFR Part § 164.308(a)(4)(ii) HPAA SR 45 CFR Part § 164.308(a)(4)(ii)(A) HPAA SR 45 CFR Part § 164.308(a)(4)(ii)(B) HPAA SR 45 CFR Part § 164.308(a)(4)(ii)(C) HPAA SR 45 CFR Part § 164.310(a)(2)(ii) HPAA SR 45 CFR Part § 164.310(b) HPAA SR	AICPA 2017 CC6.1 AICPA 2017 CC6.2					ISO/IEC 27002:2013 9.4.4	ISO/IEC 27799:2016 9.4.4			NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-3		NIST SP 800-53 R4 AC-3 NIST SP 800-53 R4 AC-6 NIST SP 800-53 R4 AU-2 NIST SP 800-53 R4 SC-2	PCI DSS v3.2.12.2.5
01.t Session Time-out	21 CFR Part														Framework v1.1 PR.DS-5 Framework v1.1 PR.PT-4	NIST SP 800-171R2 3.1.10 NIST SP 800-171R2 3.1.11 NIST SP 800-171R2 3.13.5	NIST SP 800-53 R4 AC-11 NIST SP 800-53 R4 AC-11(1) NIST SP 800-53 R4 SC-10 NIST SP 800-53 R4 SC-10	PCI DSS v3.2.112.3.8 PCI DSS v3.2.18.1.8
01.u Limitation of Connection Time	21 CFR Part														Framework v1.1 PR.DS-5 Framework v1.1 PR.PT-3 Framework v1.1 PR.PT-4		NIST SP 800-53 R4 IA-11 NIST SP 800-53 R4 SC-43	
01.v Information Access Restriction															Framework v1.1 PR.AC-1 Framework v1.1 PR.AC-2 Framework v1.1 PR.AC-3 Framework v1.1 PR.AC-4 Framework v1.1 PR.AC-7 Framework v1.1 PR.DS-1 Framework v1.1 PR.DS-5 Framework v1.1 PR.PT-2 Framework v1.1 PR.PT-3		NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-14 NIST SP 800-53 R4 AC-3 NIST SP 800-53 R4 AC-6 NIST SP 800-53 R4 DM-1 NIST SP 800-53 R4 SC-15	PCI DSS v3.2.112.3.10 PCI DSS v3.2.18.7
01.w Sensitive System Isolation											ISO/IEC 27002:2013 9.1.1	ISO/IEC 27799:2016 9.1.1			NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 ID.BE-3 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.AC-5 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.IP-1		NIST SP 800-53 R4 AC-2 NIST SP 800-53 R4 PA-2 NIST SP 800-53 R4 SC-4	
01.x Mobile Computing and Communications											ISO/IEC 27002:2013 6.2.1	ISO/IEC 27799:2016 6.2.1			NIST Cybersecurity Framework v1.1 DE.CM-7 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.IP-1	NIST SP 800-171R2 3.1.18 NIST SP 800-171R2 3.1.19	NIST SP 800-53 R4 AC-19 NIST SP 800-53 R4 AC-19(5) NIST SP 800-53 R4 CM-2(7) NIST SP 800-53 R4 SI-4	PCI DSS v3.2.11.4 PCI DSS v3.2.19.5
01.y Teleworking											ISO/IEC 27002:2013 6.2.1 ISO/IEC 27002:2013 6.2.2	ISO/IEC 27799:2016 6.2.1 ISO/IEC 27799:2016 6.2.2			NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.DS-3 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST Cybersecurity Framework v1.1 PR.IP-5	NIST SP 800-171R2 3.1.13 NIST SP 800-171R2 3.10.6	NIST SP 800-53 R4 AC-17 NIST SP 800-53 R4 AC-17(2) NIST SP 800-53 R4 AC-20 NIST SP 800-53 R4 AC-6 NIST SP 800-53 R4 AT-2 NIST SP 800-53 R4 IA-2 NIST SP 800-53 R4 PE-17 NIST SP 800-53 R4 PL-4	
02.a Roles and Responsibilities					45 CFR Part § 164.308(a)(3)(i) HIPAA SR 45 CFR Part § 164.308(a)(3)(ii) HIPAA SR	AICPA 2017 CC1.4					ISO/IEC 27002:2013 6.1.1 ISO/IEC 27002:2013 7.1.2	ISO/IEC 27799:2016 6.1.1 ISO/IEC 27799:2016 7.1.2			NIST Cybersecurity Framework v1.1 DE.DP-1 NIST Cybersecurity Framework v1.1 ID.AM-6		NIST SP 800-53 R4 PL-4 NIST SP 800-53 R4 PS-1	PCI DSS v3.2.112.4.1







ISO 13845:2016 used to Assess Title 21 CRF Part 820

EnterpriseGRC Solutions, Inc.

REGULATORY COMPLIANCE ASSOCIATES® INC
Wellness for Business®

Correspondence Between ISO 13485:2016 and 21 CFR Part 820 QMS Requirements

https://www.rcainc.com/wp-content/uploads/2017/06/ISO-Comparison-Matrix-jw-mp.pdf

Correspondence Between ISO 13485:2016 and 21 CFR 820 2

ISO 13485:2016	US FDA Quality System Regulation (QSR - 21 CFR 820)
4 Quality Management System **4.1 General Requirements** **4.1.1** The organization shall document a quality management system and maintain its effectiveness in accordance with the requirements of this International Standard and applicable regulatory requirements. The organization shall establish, implement, and maintain any requirement, procedure, activity, or arrangement required to be documented by this International Standard or applicable regulatory requirements. The organization shall document the role(s) undertaken by the organization under the applicable regulatory requirements. **NOTE**. Roles undertaken by the organization can include manufacturer, authorized representative, importer, or distributor. **4.1.2** The organization shall: a) determine the processes needed for the quality management system and the application of these processes throughout the organization taking into account the roles undertaken by the organization; b) apply a risk based approach to the control of the appropriate processes needed for the quality management system; c) determine the sequence and interaction of these processes. **4.1.3** For each quality management system process, the organization shall: a) determine criteria and methods needed to ensure that both the operation and control of these processes are effective; b) ensure the availability of resources and information necessary to support the operation and monitoring of these processes; c) implement actions necessary to achieve planned results and maintain the effectiveness of these processes; d) monitor, measure as appropriate, and analyze these processes;	**Subpart A--General Provisions** **Sec. 820.5 Quality System.** Each manufacturer shall establish and maintain a quality system that is appropriate for the specific medical device(s) designed or manufactured, and that meets the requirements of this part. **Subpart B--Quality System Requirements** **Sec. 820.20 Management Responsibility.** **(a) Quality Policy.** Management with executive responsibility shall establish its policy and objectives for, and commitment to, quality. Management with executive responsibility shall ensure that the quality policy is understood, implemented, and maintained at all levels of the organization. **(b) Organization.** Each manufacturer shall establish and maintain an adequate organizational structure to ensure that devices are designed and produced in accordance with the requirements of this part. **(1) Responsibility and Authority.** Each manufacturer shall establish the appropriate responsibility, authority, and interrelation of all personnel who manage, perform, and assess work affecting quality, and provide the independence and authority necessary to perform these tasks. **(2) Resources.** Each manufacturer shall provide adequate resources, including the assignment of trained personnel, for management, performance of work, and assessment activities, including internal quality audits, to meet the requirements of this part. **(3) Management Representative.** Management with executive responsibility shall appoint, and document such appointment of, a member of management who, irrespective of other responsibilities, shall have established authority over and responsibility for: **(i)** Ensuring that quality system requirements are effectively established and effectively maintained in accordance with this part; and **(ii)** Reporting on the performance of the quality system to management with executive responsibility for review. **(c) Management Review.** Management with executive responsibility shall review the suitability and effectiveness of the quality system at defined intervals and with sufficient frequency according to established procedures to ensure that the quality system satisfies the requirements of this part and the manufacturer's established quality policy and objectives.

Leverage Mapping: HITRUST, NIST800-53r5 – where we start

EnterpriseGRC Solutions, Inc.

Assessment Universe

new item

Testing __Awareness Education Training LSHC **LSHC** ... Find an item

Control ID	Domain ID	Test ID	Test ID:Test_ID	Control Objective	Unified Testing Map	Control Objective Description	Unified Universe Mapping	Unified Testing Map:Test_ID	Unified Universe Mapping:Control Objective
Edition or Source : California Consumer Privacy Act of 2018 (71)									
Edition or Source : EudraLex Annex 11 (17)									
Edition or Source : GAMP® 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems (82)									
Edition or Source : HIPAA - HITECH Title 45 C.F.R. § 164 (4)									
Edition or Source : HITRUST CSF V9 (49)									
HT_00.01	HT_0.0 InfoSecManProg	HT_0.a	0.a Information Security Management Program	0.01 Information Security Management Program	A.5.1.1; A.5.1.2; A.6.1.1; A.6.1.2; A.6 A.6.1.4; A.6.1.5; A.6.2.1; A.6.2.2; A.7 A.7.2.2; A.7.2.3; A.8.1.1; A.8.1.2; A.8 A.8.1.4; A.12.2.1; A.12.4.1; A.12.4.2; A.12.4.3; A.12.4.4; A.12.6.1; A.12.6.2 A.16.1.1; A.16.1.2; A.16.1.3; A.16.1.4 A.16.1.5; A.16.1.6; A.16.1.7; A.18.2.1 A.18.2.2; A.18.2.3; IR-3.1; IR-3.2; IR GMP5_ADX_O11-4.3.1; GMP5_ADX_O11-4.3.2; GMP5_ADX_O11-4.3.3; GMP5_ADX_O11-4.3.4					
HT_01.01	HT_01.0 AccCon	HT_1.a	01.a Access Control Policy	01.01 Business Requirement for Access Control	11.300(a); 11.300(b); 11.300(c); 11. (d); 11.300(e); A.9.1.1; A.9.1.2; A.9.2 A.9.2.2; A.9.2.3; A.9.2.4; A.9.2.5; A.9 A.9.3.1; A.9.4.1; A.9.4.2; A.9.4.3; A.9 A.9.4.5; A.10.1.1; A.10.1.2; AC-11.1; 11.2; AC-12.1; AC-12.2; AC-12.3; A 16.1; AC-16.10; AC-16.11; AC-16.2 16.3; AC-16.4; AC-16.5; AC-16.6; A 16.7; AC-16.8; AC-16.9; AC-17.1; A 17.2; AC-17.3; AC-17.4; AC-17.6; A 17.9; AC-18.1; AC-18.3; AC-18.4; A 18.5; AC-19.4; AC-19.5; AC-2.1; AC-2.10; AC-2.11; AC-2.12; AC-2.1 AC-2.14; AC-2.15; AC-2.2; AC-2.3; AC-2.4; AC-2.5; AC-2.6; AC-2.7; AC-2.8; AC-2.9; AC-20.1; AC-20.2; AC-20.3; AC- 20.4; AC-21.1; AC-21.2; AC-24.1; AC- 24.2; AC-3.10; AC-3.11; AC-3.12; AC-3.13; AC-3.2; AC-3.3; AC-3.4; AC-3.5; AC-3.7; AC-3.8; AC-3.9; AC-4.1; AC-4.10; AC-4.11; AC-4.12; AC-4.13; AC-4.14; AC-4.15; AC-4.17; AC-4.19; AC-4.2; AC-4.20; AC-4.21; AC-4.22; AC-4.3; AC-4.4; AC-4.5; AC-4.6; AC-4.7; AC-4.8; AC-4.9; AC-6.1; AC-6.10; AC-6.2; AC-6.3; AC-6.4; AC-6.5; AC-6.6; AC-6.7; AC-6.8; AC-6.9; AC-7.2; AC-7.3; AC-7.4; AC-9.1; AC-9.2; AC-9.3; AC-9.4; EU11_12.1_SEC-PrevAcc; EU11_12.3_SEC; GMP5_ADX_D1-3.3.3.1					

Edition or Source : California Consumer Privacy Act of 2018 (71)

Edition or Source : EudraLex Annex 11 (17)

Edition or Source : GAMP® 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems (82)

Edition or Source : HIPAA - HITECH Title 45 C.F.R. § 164 (4)

Edition or Source : HITRUST CSF V9 (49)

Edition or Source : ISO 13485:2016 € (21)

Edition or Source : ISO/IEC 27001:2013 € (22)

Edition or Source : ISO/IEC 27002:2013 € (35)

Edition or Source : ISO/IEC 27017:2015 € 27002 for cloud services (6)

Edition or Source : NIST 800-53 r5 (276)

Edition or Source : Title 21 CFR Part 11 (7)

CFR_11-Sec. 11.10	Subpart B--ER	11.10(a); 11.10(b); 11.10(c); 11.10(d); 11.10(e); 11.10(f); 11.10(g); 11.10(h); 11.10(i); 11.10(j); 11.10(k)	21 CFR Part 11.10(a) Validation ensures accuracy record integrity; 21 CFR Part 11.10(b) Accurate complete copy of records; 21 CFR Part 11.10(c) Record protection and retention; 21 CFR Part 11.10(d) - Limiting system access to authorized individuals; 21 CFR Part 11.10(e) - Changes shall not obscure; 21 CFR Part 11.10(f) Operating systems checks; 21 CFR Part 11.10(g) Authorized authority of individual checks; 21 CFR Part 11.10(h) Terminal check for valid data input; 21 CFR Part 11.10(i) qualification education training; 21 CFR Part 11.10(j) adhere to written policies; 21 CFR Part 11.10(k) system documentation and change control	Sec. 11.10 Controls for closed systems	HT_1.b; HT_1.d; HT_1.f; HT_1.k; HT_1.r; HT_1.u; HT_1.v; HT_1.w; HT_10.d; HT_10.i; HT_2.f; HT_2.g; HT_6.d; HT_8.c; HT_9.aa; HT_9.ab; A.12.2.1; A.14.2.1; A.14.2.2; A.14.2.3; A.14.2.6; A.18.1.3	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of **electronic records**, and to ensure that the **signer cannot readily repudiate** the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. (b) The **ability to generate accurate and complete copies of records** in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any	HT_10.01; HT_10.02; HT_10.03; HT_10.04; A.9.2; A.9.3; A.12.1; A.12.2; A.12.7; A.14.1; A.14.2; A.12.4; A.18.1	01.b User Registration; 01.d User Password Management; 01.f Password Use; 01.k Equipment Identification in Networks; 01.r Password Management System; 01.u Limitation of Connection Time; 01.v Information Access Restriction; 01.w Sensitive System Isolation; 10.d Message Integrity; 10.i Protection of System Test Data; 02.f Disciplinary Process; 02.g Termination Responsibilities; 06.d Data Protection and Privacy of Covered Information; 08.c Securing Offices, Rooms, and Facilities; 09.aa Audit Logging; 09.ab Monitoring System Use; A.12.2.1 Controls against malware; A.14.2.1 Secure development policy; A.14.2.2 System change control procedures; A.14.2.3 Technical review of applications after operating platform changes; A.14.2.6 Secure development environment; A.18.1.3 Protection of records	10.01 Security Requirements of Information Systems; 10.02 Correct Processing in Applications; 10.03 Cryptographic Controls; 10.04 Security of System Files; A.9.2 User access management; A.9.3 User responsibilities; A.12.1 Operational procedures and responsibilities; A.12.2 Protection from malware; A.12.7 Information systems audit considerations; A.14.1 Security requirements of information systems; A.14.2 Security in development and support processes; A.12.4 Logging and monitoring; A.18.1 Compliance with legal and contractual requirements

ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES; AC-16.8 MULTI-ENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION; AC-16.7 CONSISTENT ATTRIBUTE INTERPRETATION; AC-16.8 ASSOCIATION TECHNIQUES AND TECHNOLOGIES; AC-16.9 ATTRIBUTE REASSIGNMENT; AC-17.1 AUTOMATED MONITORING/CONTROL; AC-17.2 PROTECTION OF CONFIDENTIALITY/INTEGRITY USING ENCRYPTION; AC-17.3 MANAGED ACCESS CONTROL POINTS; AC-17.4 PRIVILEGED COMMANDS / ACCESS; AC-17.6 PROTECTION OF INFORMATION; AC-17.9 DISCONNECT/DISABLE ACCESS; AC-18.1 AUTHENTICATION AND ENCRYPTION; AC-18.3 DISABLE WIRELESS NETWORKING; AC-18.4 RESTRICT CONFIGURATIONS BY USERS; AC-18.5 ANTENNAS/TRANSMISSION POWER LEVELS; AC-19.4 RESTRICTIONS FOR CLASSIFIED INFORMATION; AC-19.5 FULL DEVICE / CONTAINER-BASED ENCRYPTION; AC-2.1 AUTOMATED SYSTEM ACCOUNT MANAGEMENT; AC-2.10 SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION; AC-2.11 USAGE CONDITIONS; AC-2.12 ACCOUNT MONITORING / ATYPICAL USAGE; AC-2.13 DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS; AC-2.14 PROHIBIT SPECIFIC ACCOUNT TYPES; AC-2.15 ATTRIBUTE-BASED SCHEMES; AC-2.2 REMOVAL OF TEMPORARY/EMERGENCY ACCOUNTS; AC-2.3 DISABLE INACTIVE ACCOUNTS; AC-2.4 AUTOMATED AUDIT ACTIONS; AC-2.5 INACTIVITY LOGOUT; AC-2.6 DYNAMIC PRIVILEGE MANAGEMENT; AC-2.7 ROLE-BASED SCHEMES; AC-2.8 DYNAMIC ACCOUNT CREATION; AC-2.9 RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS; AC-20.1 LIMITS ON AUTHORIZED USE; AC-20.2 PORTABLE STORAGE DEVICES; AC-20.3 NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES; AC-20.4 NETWORK ACCESSIBLE STORAGE DEVICES; AC-21.1 AUTOMATED DECISION SUPPORT; AC-21.2 INFORMATION SEARCH AND RETRIEVAL; AC-24.1 TRANSMIT ACCESS AUTHORIZATION INFORMATION; AC-24.3 NO USER OR PROCESS IDENTITY; AC-3.10 AUDITED OVERRIDE OF ACCESS

NIST 800-53 r5 Adds KEYWORDS and Privacy Attributes

EnterpriseGRC Solutions, Inc.

COMPUTER SECURITY RESOURCE CENTER

CSRC

PUBLICATIONS

SP 800-53 Rev. 5 (Draft)

Security and Privacy Control
(Final Public Draft)

Date Published: March 2020
Comments Due: May 15, 2020
Email Comments to: sec-cert@nist.gov

Planning Note (3/20/2020):

See the current publication schedule proposed by NIST; it may be subje

NIST is currently developing additional resources, including providing th
resources will be available under "Supplemental Material."

Author(s)

Joint Task Force

Announcement

There is an urgent need to strengthen the trustworthiness and resilience of the information systems, component products, and services that we depend on in every critical infrastructure sector and which support the economic and national security interests of the United States.

This (final public draft) revision of NIST Special Publication 800-53 presents a proactive and systemic approach to developing comprehensive safeguarding measures for all types of computing platforms, including general purpose computing systems,

110	AC-11 Device Lock	AC-11	...	AC 800-53-R5				S		SESSION LOCK; INACTIVITY; AUTHENTICATION PROCEDURES	NIST 800-53 r5	AC-11 (1)		AC-11 (1)	A.11.2.8; A.11.2.9	A.11.2.8 Unattended user equipment; A.11.2.9 Clear desk and clear screen policy	A.11.2	A.11.2 Equipment
111	AC-12 Session Termination	AC-12	...	AC 800-53-R5				S		SESSION TERMINATION; NETWORK CONNECTIONS; LOGICAL SESSION	NIST 800-53 r5	AC-12		AC-12				
112	AC-14 Permitted Actions without Identification or Authentication	AC-14	...	AC 800-53-R5				O		ACTIONS WITHOUT IDENTIFICATION; WITHOUT AUTHENTICATION; BYPASS; ACTIONS W/O AUTHENTICATION	NIST 800-53 r5	AC-14	AC-14	AC-14				
113	AC-16 Security and Privacy Attributes	AC-16	...	AC 800-53-R5	P	J	D	O		SECURITY ATTRIBUTES; PRIVACY ATTRIBUTES; ACTIVE ENTITIES; PASSIVE ENTITIES; SUBJECTS; OBJECTS	NIST 800-53 r5				CCPA14.1.1 1798.150(a)(1); CCPA14.1.2 1798.150(a)(2); GMPS_ADX_D2-3.2.1; GMPS_ADX_D2-3.2.2; GMPS_ADX_D2-3.2.3; GMPS_ADX_D2-3.2.4; GMPS_ADX_D2-3.2.5; GMPS_ADX_D2-3.2.6; GMPS_ADX_D2-3.2.7; GMPS_ADX_D2-3.2.8; GMPS_ADX_D2-3.2.9; A.10.1.1; A.10.1.2; A.18.2.1; A.18.2.2; A.18.2.3; AC-17.1; AC-17.2; AC-17.3; AC-17.4; AC-17.6; AC-17.9; AC-18.1; AC-18.3; AC-18.4; AC-18.5; AC-19.4; AC-19.5; AC-4.1; AC-4.2; AC-4.3; AC-4.4; AC-4.5; AC-4.7; AC-4.8; AC-4.9; AC-4.10; AC-4.11; AC-4.12; AC-4.13; AC-4.14; AC-4.15; AC-4.17; AC-4.19; AC-4.20; AC-4.21; AC-4.22; CM-3.1; CM-3.2; CM-3.3; CM-3.4; CM-3.5; CM-3.6; CP-8.2; CP-8.3; CP-8.5; CP-8.6; CP-9.7; CP-9.8; MP-5.3; SC-12.1; SC-12.2; SC-12.3; SI-20.1; SI-20.2; SI-20.3; SI-20.4; SI-20.5; SI-20.6; SI-20.7; SI-20.8; SI-4.1; SI-4.2; SI-4.3; SI-4.4; SI-4.5; SI-4.7; SI-4.9; SI-4.10; SI-4.11; SI-4.12; SI-4.13; SI-4.14; SI-4.15; SI-4.16; SI-4.17; SI-4.18; SI-4.19; SI-4.20; SI-4.21; SI-4.22; SI-4.23; SI-4.24; SI-4.25; 11.30; HT_6d; HT_6.c; HT_9.e	14.01.01 1798.150 (a)(1): Any consumer whose nonencrypted or nonredacted personal information; 14.01.02 1798.150 (a)(2): In assessing the amount of statutory damages, the court shall consider: GMPS_3.2.1 Introduction; GMPS_3.2.2 Overview; GMPS_3.2.3 Functions; GMPS_3.2.4 Data; GMPS_3.2.5 Interfaces; GMPS_3.2.6 Non-functional Attributes; GMPS_3.2.7 Environment; GMPS_3.2.8 Glossary; GMPS_3.2.9 Appendices; A.10.1.1 Policy on the use of cryptographic controls; A.10.1.2 Key management; A.18.2.1 Independent review of information security; A.18.2.2 Compliance with security policies and standards; A.18.2.3 Technical compliance review; AC-17.1 AUTOMATED MONITORING/CONTROL; AC-17.2 PROTECTION OF CONFIDENTIALITY/INTEGRITY USING ENCRYPTION; AC-17.3 MANAGED ACCESS CONTROL POINTS; AC-17.4 PRIVILEGED COMMANDS / ACCESS; AC-17.6 PROTECTION OF INFORMATION; AC-17.9 DISCONNECT/DISABLE ACCESS; AC-18.1 AUTHENTICATION AND ENCRYPTION; AC-18.3 DISABLE WIRELESS NETWORKING; AC-18.4 RESTRICT CONFIGURATIONS BY USERS; AC-18.5 ANTENNAS/TRANSMISSION POWER LEVELS; AC-19.4 RESTRICTIONS FOR CLASSIFIED INFORMATION; AC-19.5 FULL DEVICE / CONTAINER-BASED ENCRYPTION; AC-4.1 OBJECT SECURITY ATTRIBUTES; AC-4.2 PROCESSING DOMAINS; AC-4.3 DYNAMIC INFORMATION FLOW CONTROL; AC-4.4 CONTENT CHECK ENCRYPTED INFORMATION; AC-4.5 EMBEDDED DATA TYPES; AC-4.6 METADATA; AC-4.7 ONE-WAY FLOW MECHANISMS; AC-4.8 SECURITY POLICY FILTERS; AC-4.9 HUMAN REVIEWS; AC-4.10 ENABLE / DISABLE SECURITY POLICY FILTERS; AC-4.11 CONFIGURATION OF SECURITY POLICY FILTERS; AC-4.12 DATA TYPE IDENTIFIERS; AC-4.13 DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS; AC-4.14 SECURITY POLICY FILTER CONSTRAINTS; AC-4.15 DETECTION OF UNSANCTIONED INFORMATION; AC-4.17 DOMAIN AUTHENTICATION; AC-4.19 VALIDATION OF METADATA; AC-4.20 APPROVED SOLUTIONS; AC-4.21 PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS; AC-4.22 ACCESS ONLY; CM-3.1 AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES; CM-3.2 TEST / VALIDATE / DOCUMENT CHANGES; CM-3.3 AUTOMATED CHANGE IMPLEMENTATION; CM-3.4 SECURITY REPRESENTATIVE; CM-3.5 AUTOMATED SECURITY RESPONSE; CM-3.6 CRYPTOGRAPHY MANAGEMENT; CP-8.2 TEST RESTORATION USING SAMPLING; CP-8.3 SEPARATE STORAGE FOR CRITICAL INFORMATION; CP-9.5 TRANSFER TO ALTERNATE STORAGE SITE; CP-9.6 REDUNDANT SECONDARY SYSTEM; CP-9.7 DUAL AUTHORIZATION; CP-9.8 CRYPTOGRAPHIC PROTECTION; MP-5.3 CUSTODIANS; SC-12.1 AVAILABILITY; SC-12.2 SYMMETRIC KEYS; SC-12.3 ASYMMETRIC KEYS; SI-20.1 COLLECTION; SI-20.2 ARCHIVING; SI-20.3 RELEASE; SI-20.4 REMOVAL, MASKING, ENCRYPTION, HASHING, OR REPLACEMENT OF DIRECT IDENTIFIERS; SI-20.5 STATISTICAL DISCLOSURE CONTROL; SI-20.6 DIFFERENTIAL PRIVACY; SI-20.7 VALIDATED SOFTWARE; SI-20.8 MOTIVATED INTRUDER; SI-4.1 SYSTEM-WIDE INTRUSION DETECTION SYSTEM; SI-4.2 AUTOMATED TOOLS FOR REAL-TIME ANALYSIS; SI-4.3 AUTOMATED TOOL INTEGRATION; SI-4.4 INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC; SI-4.5 SYSTEM-GENERATED ALERTS; SI-4.7 AUTOMATED RESPONSE TO SUSPICIOUS EVENTS; SI-4.9 TESTING OF MONITORING TOOLS; SI-4.10 VISIBILITY OF ENCRYPTED COMMUNICATIONS; SI-4.11 ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES; SI-4.12 AUTOMATED ALERTS; SI-4.13 ANALYZE TRAFFIC/EVENT PATTERNS; SI-4.14 WIRELESS INTRUSION DETECTION; SI-4.15 WIRELESS TO WIRELINE COMMUNICATIONS; SI-4.16 CORRELATE MONITORING INFORMATION; SI-4.17 INTEGRATED SITUATIONAL AWARENESS; SI-4.18 ANALYZE TRAFFIC / COVERT EXFILTRATION; SI-4.19 INDIVIDUALS POSING GREATER RISK; SI-4.20 PRIVILEGED USERS; SI-4.21 PROBABILISTIC DISTRIBUTIONS; SI-4.22 UNAUTHORIZED NETWORK SERVICES; SI-4.23 HOST-BASED DEVICES; SI-4.24 INDICATORS OF COMPROMISE; SI-4.25 PERSONALLY IDENTIFIABLE INFORMATION MONITORING; 21 CFR Part 11.30 encryption and digital signature standards; 06.d Data Protection and Privacy of Covered Information; 06.c Protection of Organizational Records; 09.x Security of Network Services	A.18.1	A.18.1 Compliance with legal and contractual requirements
114	AC-17 Remote Access	AC-17	...	AC 800-53-R5				O		ACCESS AUTHORIZATION; REMOTE ACCESS; EXTERNAL NETWORKS; DIAL UP; BROADBAND; WIRELESS; VIRTUAL PRIVATE NETWORK; VPN	NIST 800-53 r5	AC-17 (1) (2) (3)	AC-17	AC-17 (1) (2) (3)	A.6.2.1; A.6.2.2; A.13.1.1; A.13.2.1; A.14.1.2	A.6.2.1 Mobile device policy; A.6.2.2 Teleworking; A.13.1.1 Network controls; A.13.2.1 Information transfer policies and procedures; A.14.1.2 Securing application services on public networks	A.6.2; A.13.1; A.13.2; A.14.1	A.6.2 Mobile devices and teleworking; A.13.1 Network security management; A.13.2 Information transfer; A.14.1 Security requirements of information systems
115	AC-18 Wireless Access	AC-18	...	AC 800-53-R5				O		WIRELESS ACCESS; USAGE RESTRICTION; CONFIGURATION REQUIREMENTS; CONNECTION REQUIREMENTS	NIST 800-53 r5	AC-18 (1) (3) (4)	AC-18	AC-18 (1) (3)	A.6.2.1; A.13.1.1; A.13.2.1	A.6.2.1 Mobile device policy; A.13.1.1 Network controls; A.13.2.1 Information transfer policies and procedures	A.6.2; A.13.1; A.13.2	A.6.2 Mobile devices and teleworking; A.13.1 Network security management; A.13.2 Information transfer

03/16/20: SP 800-53 Rev. 5 (Draft)

TOPICS

Security and Privacy

access control; audit and accountability; awareness training & education; contingency planning; incident response; identification & authentication; privacy

https://github.com/usnistgov/OSCAL/tree/master/content/nist.gov/SP800-53/rev5

Additional Resources that Tie Out IOT – CSA – Requires use of CSTAR Registry – Referencing Requires Explicit Permission

EnterpriseGRC Solutions, Inc.

CSA cloud security alliance® iot CONTROLS FRAMEWORK			details about the framework, download the "Guide to the CSA IoT Controls Framework" at: tps://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework	IoT System Risk Impact Levels			Supplemental Control Guidance		Implementation Guid	
Control Domain	**Control ID**	**CCM ID**	**Control Specification**	**Confidentiality**	**Integrity**	**Availability**	**Additional Direction**	**References / Rationale**	***Types of Security Controls***	***Control Implementation***
Secure Networks *SDP*	**SNT-09**	IAM-08 IVS-06	Configure a Software-Defined Perimeter (SDP) that authenticates IoT devices prior to connection to a network, and restricts activities based on pre-approved roles and privileges.	Moderate	Moderate	Moderate	The SDP approach hides the network from all devices/users. The network and applications are hidden behind gateways that reject all connection requests except from authorized devices/users. Devices/users must authenticate first with a controller that contains the necessary information to determine that the device/user is "pre-approved" then the controller informs the servers or gateways to accept connections from the particular user/device. Besides access to the network which applications the device/user can interact with are also	https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf https://downloads.cloudsecurityalliance.org/assets/research/sdp/SDP-glossary.pdf Architecture document 1.0 is in process and should be finished in 2018 Specification 2.0 will be started late Dec 2018 early January 2019 An Anti-DDOS paper is also in progress and will be finished Q1 2019 https://www.nist.gov/sites/default/files/documents/2016/09/16/waverly_rfi_response.pdf	Preventive	Automatic
Secure Networks *Visualization Tools*	**SNT-10**		Use a network visualization tool to monitor the operating state and health status of IoT devices, gateways and services. Use simple heartbeat monitoring to monitor device connectivity or SNMPv3 traps for monitoring CPU utilization, memory, and other abnormal behaviors.	Moderate	Moderate	Moderate	These tools help identify network communciation and traffic issues and can also help identify a DoS attack.		Detective	Automatic
Secure Networks *Wireless Network Boundaries*	**SNT-11**		Define physical boundaries for WSNs and limit the power rating of ZigBee and ZWave devices to minimize signal leakage.	High	High	High			Preventive	Automatic
Secure Networks *Segmentation*	**SNT-12**	IVS-09	Set up Wireless Sensor Networks (WSN), such as ZigBee, ZWave and Bluetooth, to be disconnected from the Internet with only authorized gateways exposing internet connectivity.	Moderate	Moderate	Moderate		CTA. Recommended Best Practices for Securing Home Systems Securing your Internet of Things from the Ground Up. Microsoft Azure White Paper.	Preventive	Manual
Secure Networks *Environment Scanning*	**SNT-13**	IVS TVM	At least quarterly, scan the physical environment to look for anomalies, such as radiofrequency (RF) attacks and rogue device insertion.	High	High	High			Detective	Automatic
Secure Networks *Device Communication*	**SNT-14**	IVS TVM MOS	Require all communications with an IoT device to be initiated by the device. Log and alert about unauthorized connection requests	Moderate	Moderate	Moderate			Preventive	Automatic
Secure Networks *ZigBee Default Keys*	**SNT-15**		Disable the default ZigBee Trust Center (TC) key and generate/use a non-default key for protecting the confidentiality of keys in transport.	Moderate	Moderate	Moderate		https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf	Preventive	Semi-Automatic
Secure Networks *ZigBee Master Keys*	**SNT-16**		Distribute ZigBee Master Keys out of band. Never pass master keys over the network. Master keys are used to establish additional key material.	Moderate	Moderate	Moderate			Preventive	Automatic
Secure Networks *ZigBee Networks Keys*	**SNT-17**		Rotate ZigBee Network Keys at least annually, and disable prior keys upon distribution/establishment of the new network key.	Moderate	Moderate	Moderate			Preventive	Automatic
Secure Networks *Zwave*	**SNT-18**	IVS-06 IVS-12 IVS-13 IPY-04	Supplement Z-Wave networks with AES 128 cryptographic keys for authentication. Use these keys in addition to the standard 4-byte Home ID to access a Z-Wave network.	Moderate	Moderate	Moderate		CTA. Recommended Best Practices for Securing Home Systems	Preventive	Automatic

SANS IOT Internet of Things Reading Room

EnterpriseGRC Solutions, Inc.

Reading Room

Internet of Things

Featuring 14 Papers as of July 3, 2019

DICE and MUD Protocols for Securing IoT Devices
STI Graduate Student Research
by Muhammed Ayar - June 5, 2019
+ Overview
Download

Practical Industrial Control System (ICS) Cybersecurity: IT and OT Have Converged - Discover and Defend Your Assets
Analyst Paper (requires membership in SANS.org community)
by Doug Wylie and Dean Parsons - September 26, 2018
+ Overview
Download

- **Associated Webcasts:** Practical Industrial Control System (ICS) Cybersecurity: IT and OT Have Converged--Discover and Defend Your Assets
- **Sponsored By:** Tenable

PiOT – a small form factor defense for indefensible devices
by James Leyte-Vidal - August 2, 2018
+ Overview
Download

The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns
Analyst Paper (requires membership in SANS.org community)
by Barbara Filkins - July 18, 2018
+ Overview
Download

- **Associated Webcasts:** The State of Industrial IoT
- **Sponsored By:** Forescout Technologies BV, Accenture, Indegy

Building the New Network Security Architecture for the Future
Analyst Paper (requires membership in SANS.org community)
by Sonny Sarai - January 22, 2018
+ Overview
Download

SANS

SANS Institute
Information Security Reading Room

DICE and MUD Protocols for Securing IoT Devices

Muhammed Ayar

A Matter of Perspective: Threats and Risks

Overall, the majority of respondents (59%), regardless of organization size, are only somewhat confident in their organization's ability to secure their IIoT devices. See Figure 8.

Interestingly, members of the OT department—the individuals who are likely the most knowledgeable about IIoT implementation—appear to be the least confident in their organization's ability to secure these devices, while company leadership and management, including department managers, appear to be the most assured, as illustrated in Figure 9.

"Members of the OT department, the individuals who are likely the most knowledgeable about IIoT implementation, appear to be the least confident in their organization's ability to secure these devices, while company leadership and management, including department managers, appear to be the most assured."

The discrepancy in the views of management and leadership from OT in the company's capability to secure IIoT is problematic. Such pronounced disparity surely leads to challenges for the OT group's ability to secure budget for such investments as ongoing security skills-building, technologies and services to help safeguard operations, and resources to respond and recover to incidents.

The same data may also suggest an overall leadership and mar
perspective that current company security investments in IIoT a
somehow adequate—or at least deemed adequate enough to c
current risks to the overall business.

Given the current state of your security program (people, policies, processes, controls and technology) how would you rate your organization's ability to secure your IIoT devices?

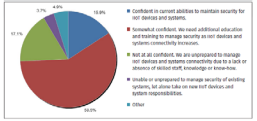
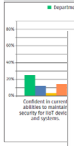


Figure 8. Current State of Security program regarding IIoT

Given the current state of your security program (people, policies, processes, controls and technology) how would you rate your organization's ability to secure your IIoT devices?



SANS Analyst Program | The 2018 SANS Industrial IoT Secur

Threats and Vulnerabilities

Confidence in being able to secure an organizations IIoT infrastructure depends on understanding the threats and risks to be faced, especially in light of the complexity that stems from allowing external connectivity for OT systems and adding a growing number of devices that expand effort to manage asset inventory, device and system configuration, and change management. The results are presented in Table 6.

In line with Figure 2 (on page 4), patching and product upgrades are trouble spots and are expected to remain so for the next two years. The recognition by so many that IIoT devices will be vulnerable and remain vulnerable due to lack of patching exposes how investments in infrastructure hardening may continue to be viewed as a sufficient security strategy to adequately protect IIoT systems.

Risk

Respondents (48%) acknowledge that

Table 6. IIoT Concerns over the Next Two Years

Greatest Challenges in the Next Two Years		Response
1	Difficulty or lack of patching IIoT devices and systems, leaving them vulnerable	55.95%
2	Accidental exposures resulting from user error and system complexity	41.67%
3	Difficulty controlling, locating, tracking, preventing and managing IoT connectivity to critical infrastructure and other mission-critical systems	39.29%
4	Failure to incorporate good security practices into the IIoT design, build, operate and maintenance lifecycle models for systems	30.29%
5	IIoT "Things" used as infection vectors to spread in the enterprise	34.52%
6	Multivendor environment without device and technology standardization	29.76%
7	Denial of service attacks on IIoT devices and systems that cause damage or loss of life	25.00%
8	Shortage of vendor investments to incorporate security into the design of IIoT devices, systems and supporting products	19.05%
9	Sabotage and destruction of connected IIoT devices and systems	13.10%

BEST PRACTICES

Threats are constantly evolving, and for IT and non-IIoT devices, there are instances where product patching could have at least raised the difficulty for an attacker to meet an objective. For this reason, implementing disciplined change management, careful endpoint selection, reducing endpoint and network complexity, and closely monitoring IIoT connections and communications are remain highly suitable recommendations, in addition to the best practice of developing and executing ongoing IIoT patching procedures.

Table 7. Greatest Concerns for IIoT Security Over Next Two Years

Risk		Response
1	Lack of security considerations in product and system installation, configuration, service, support and maintenance	47.6%
2	Shortage or absence of adequate security considerations in IIoT product design and manufacturing	39.3%
3	Pace or lack of updates for vulnerabilities to OS, firmware or other software for IIoT devices	38.1%
4	Creating new attack surfaces that expose or enable additional vulnerabilities such as related to the command and control (C2) channel to a IIoT device and system	34.5%
5	User-introduced vulnerabilities for IIoT devices through oversight, misconfiguration and user-error	32.1%
6	Potential loss of sensitive data enabling more sophisticated attacks	29.8%
7	Shortage or absence of adequate security considerations in system design and manufacturing	23.8%
8	Negative impact on system safety posture or ability to maintain safe operation or shutdown	22.6%
9	Impacts from conflicting operational priorities in solutions that span safety, security, reliability, resilience and privacy	19.1%
10	Lack of relevant, sensible and enforceable industry standards on IIoT devices and systems	17.9%
11	Other	5.2%

8 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns 16

SANS

A SANS Survey

The 2018 SANS Industrial IoT Security Survey:
Shaping IIoT Security Concerns

Written by **Barbara Filkins**
Advisor: **Doug Wylie**

July 2018

Sponsored by:
ForeScout Technologies, Inc.

https://www.sans.org/reading-room/whitepapers/internet/dice-mud-protocols-securing-iot-devices-38980

https://www.sans.org/reading-room/whitepapers/internet

What creates the threads that we can assert?

EnterpriseGRC Solutions, Inc.

Ten normative references

Benchmark contains both descriptive information and structural information

Group item that can hold other items

Item three types of items: <xccdf:Group>, <xccdf:Rule> and <xccdf:Value>

Model suggested scoring model for an <xccdf:Benchmark>

Profile element is a named tailoring for an <xccdf:Benchmark>

Rule the description for a single item of guidance or constraint. <xccdf:Rule> elements form the basis for testing a target platform for benchmark

compliance

Status acceptance status of an element with an optional date attribute, which signifies the date of the status change

Tailoring element holds one or more <xccdf:Profile> elements-records additional benchmark tailoring

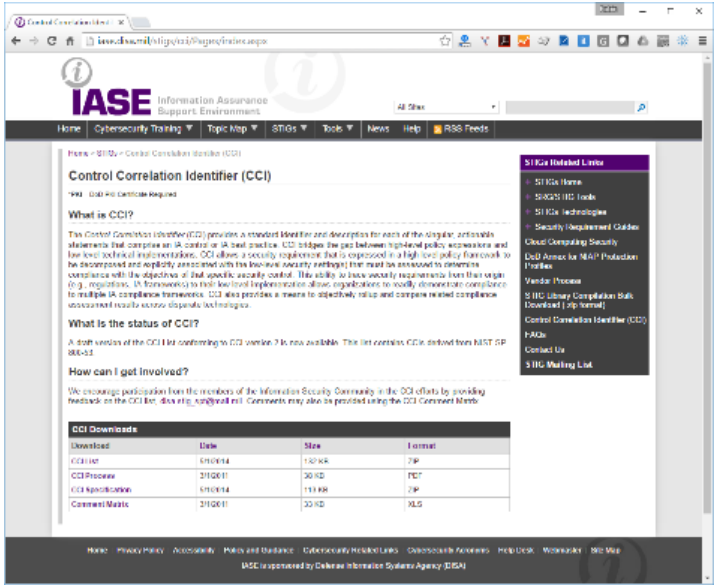
TestResult element encapsulates the results of a single application of an <xccdf:Benchmark> to a single target platform

Value a named parameter that can be substituted into properties of other elements within the <xccdf:Benchmark>

Control Correlation Identifiers CCI

EnterpriseGRC Solutions, Inc.

- http://iase.disa.mil/stigs/cci/Pages/index.aspx



- The *Control Correlation Identifier* (CCI) provides a standard identifier and description for each of the singular, actionable statements that comprise an IA control or IA best practice.
- CCI bridges the gap between high-level policy expressions and low-level technical implementations. CCI allows a security requirement that is expressed in a high-level policy framework to be decomposed and explicitly associated with the low-level security setting(s) that must be assessed to determine compliance with the objectives of that specific security control.
- This ability to trace security requirements from their origin (e.g., regulations, IA frameworks) to their low-level implementation allows organizations to readily demonstrate compliance to multiple IA compliance frameworks.
- CCI also provides a means to objectively rollup and compare related compliance assessment results across disparate technologies.

Open Vulnerability and Assessment Language (OVAL)

EnterpriseGRC Solutions, Inc.

OVAL in the Enterprise	
• Vulnerability Assessment • Configuration Management • Patch Management • Policy Compliance	• Community Repositories of OVAL Content • Vulnerability Databases and Advisories • Benchmark Writing • Security Content Automation

- **OVAL®** is an information security community effort to standardize how to assess and report machine state of computer systems.
- Tools and services that use OVAL for the three steps of system assessment — representing system information, expressing specific machine states, and reporting the results of an assessment — provide enterprises with accurate, consistent, and actionable information so they may improve their security.

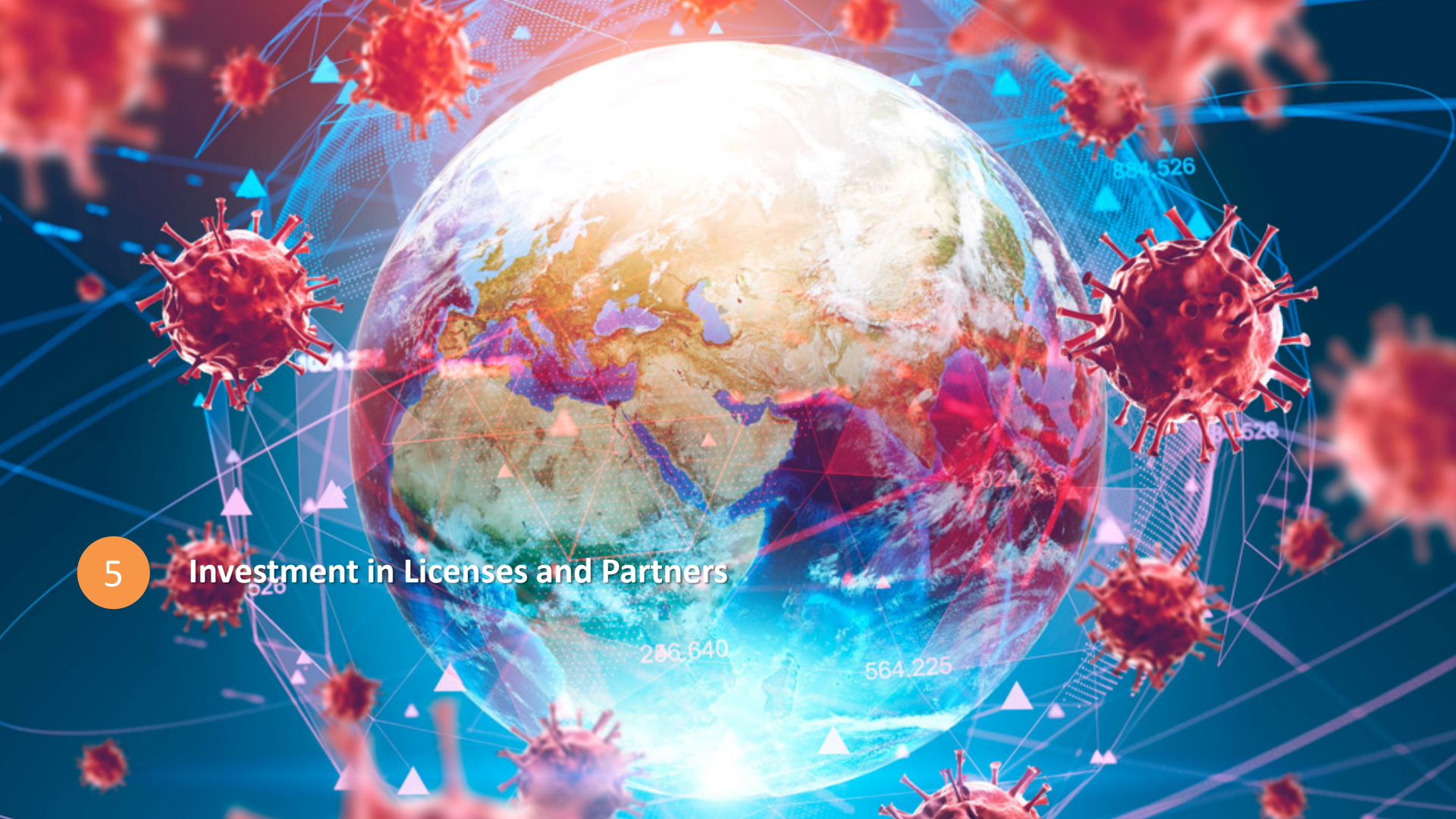
Possible Future Integration is working with MITRE ATT&CK

EnterpriseGRC Solutions, Inc.

Interfaces for Working with ATT&CK: There are two different ways for you to access the ATT&CK content:

- ATT&CK expressed in STIX 2.0 GitHub repository: There are a few different ways to interact with the ATT&CK content (repo). Python, the best way is to utilize cti-python-stix2. The USAGE doc in the repo to helps. Since STIX 2.0 is JSON that library is the programming language of choice to interact with the raw content, such as the full set of Enterprise ATT&CK content found here.
- TAXII Server: The TAXII server stays up to date with the content found in our GitHub repository, so consumers access the ATT&CK content there. As the TAXII Server release blog post states, consumers use the cti-python-stix2 and cti-taxii-client to get the ATT&CK content from the TAXII server.

MITRE | ATT&CK®

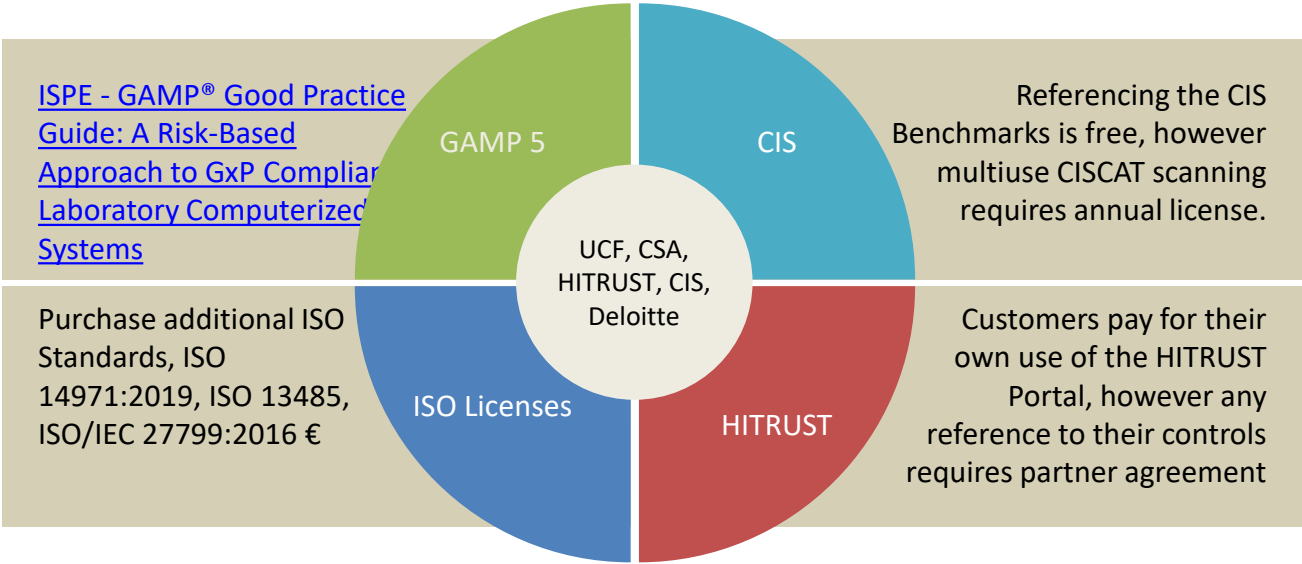


5 Investment in Licenses and Partners

Licenses Necessary to Mapping into the LSHC World

EnterpriseGRC Solutions, Inc.

- Strategic Partners might include Unified Compliance Network, HITRUST, Big Four such as Deloitte, Center for Internet Security, CIS*



Experience Creating CIS Partner Relationship

EnterpriseGRC Solutions, Inc.

Sponsors

ALIEN VAULT
Unified Security for Threat Detection, Incident Response, and Compliance

cavirin
CyberPosture Intelligence for the Hybrid Cloud

HALOCK
Prioritizing your CIS Controls and meeting Duty of Care

IBM Security

NNT
Delivering Controls with CIS-Certified "Security through System Integrity"

Qualys. Continuous Security

CIS SecureSuite Membership

SANS Security Leadership POSTER

CIS Controls™

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.

CIS Controls V7 separates the controls into three distinct categories:

Basic:
Key controls which should be implemented in every organization for essential cyber defense readiness.

Foundational:
Technical best practices provide clear security benefits and are a smart move for any organization to implement.

Organizational:
These controls are more focused on people and processes involved in cybersecurity.

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

> "Start by taking care of the basics: build a solid cybersecurity foundation by implementing the [CIS Controls], especially application white-listing, standard secure configurations, reduction of administrative privileges and a quick patching process."
>
> Zurich Insurance Group
> *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*
> Switzerland

CIS Benchmarks™

A single operating system can have over 200 configuration settings and studies of cyber attacks and security incidents invariably reach the same conclusion: poor configuration choices and management are major contributors to the success of attackers. Moreover, every reasonable security framework requires secure configurations as part of ensuring suitable endpoint posture.

CIS Benchmarks are best practices for the secure configuration of a target system.

Available for more than 100 technologies, CIS Benchmarks are developed through a unique consensus-based process comprised of cybersecurity professionals and subject matter experts around the world. CIS Benchmarks are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry and academia. CIS Benchmarks are free to download in PDF format, with additional file formats (XCCDF, Word, etc.) available to CIS SecureSuite Members.

To further help you with your adoption of the CIS Controls within your organization, each benchmark recommendation is also annotated with the relevant CIS Control.

→ **https://www.cisecurity.org/cis-benchmarks/**

CIS SecureSuite® Membership

Used worldwide, CIS SecureSuite Membership provides integrated cybersecurity resources to help businesses, nonprofits, governmental entities and IT experts start secure and stay improve overall cybersecurity posture. CIS SecureSuite delivers integration of the CIS Benchmarks (the only consensus-based, best practice security configuration guides

Cybersecurity + Community

When designing the latest version of the CIS Controls, our community relied on key principles to guide the development to simplify, focus, and align them to address the current cybersecurity threat environment. Version 7 of the CIS Controls was developed to align with the latest cyber threat data, security technology, as well as increasing business demands for information technology. We recognize that the cybersecurity world is constantly shifting and reacting to new threats and vulnerabilities, which often results in chaos and confusion about which steps to take in order to harden systems and data.

In order to cut through the confusion, we collaborated on CIS Controls V7 with a global community of cybersecurity experts – leaders in academia, industry and government – to secure input from volunteers at every level that included feedback from a community of over 300 individuals dedicated to improving cybersecurity for all.

Thanks to people like you, the CIS Controls continue to grow in influence and impact across a world-wide community of adopters, vendors and supporters. The idea that started with a small group of friends has become an international movement of volunteers across the entire cyber ecosystem developing, sharing and supporting best practices that can help every enterprise defend itself. CIS is here to help support, evolve and bring together expertise and energy like yours to create, support and sustain best practices in defense.

CIS appreciates the many security experts who volunteer their time and talent to support the CIS Controls and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

As a non-profit driven by volunteers, CIS is always looking for new topics and assistance in creating cybersecurity guidance. If you're interested in volunteering and/or have questions, comments or have identified ways to improve this guide, please write us at **controlsinfo@cisecurity.org** and join a CIS Control Community.


Thank You..