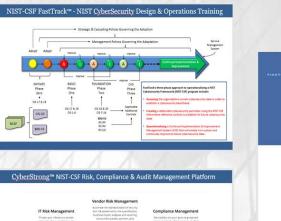
NIST-CSF FastTrack[™] Accredited Training Programs Rebalancing the Relationship Between Cybersecurity Risk, Compliance & Audit









Pricing Options: Per Academy of Subscription Options Hosting Options: Cyter-Staff or Client Hosted		Management Options: Client Branded Portal web Student Monitoring & Reporting Training Options: Individual, Workforce, Internitipa		
Underse Lipskilling - Workforce Lipskilling - Retired Millary - College Grads - Under Employed - Under Employed - Disadvantaged	Candidate Assessment Individual or Organizational		Video Learning & Quizzes	Digital Courseware
	Knowledge Academy Cybersecurity Certification Training		N .	
	Skills Academy Cybersecurity Skills Training		Multi-touch learning	
	Ablities Academy Cybersecurity Virtual Internship Team Trainings		6	2 Par
	Online Staffing Marketplace Connecting Candidates to Hiring Companies		Checkpoints & Sample Papers	Online Expert Mentoring
Global Reach	Customization and New Program Development Options			

NICE CyberStaff[™] NIST-CSF Workforce Upskilling & Intern Training Program

itSM Solutions™

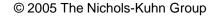
IT Experience. Practical Solutions.



Agenda and Objectives

- Committee of Sponsoring Organizations (COSO) of the Treadway Commission
- NIST Cybersecurity Frameworks
- NIST Cybersecurity Professional (NCSP) Certification Training Programs
 - NIST-CSF FastTrack[™] Design & Operations Certification Training
 - NIST-CSF FastTrack[™] Specialist Training
 - NIST-CSF FastTrack[™] CyberStrong Platform Training
 - NICE-CWF CyberStaff[™] Workforce Upskilling and Intern Training Program
- CyberStrong Platform[™] Risk, Compliance & Audit Management Platform



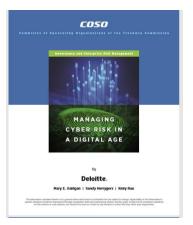


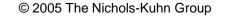


Committee of Sponsoring Organizations (COSO)

- The Committee of Sponsoring Organizations of the Treadway Commission contributing members include the American Accounting Association (AAA), American Institute of CPAs (AICPA), Financial Executives International (FEI), The Institute of Management Accountants (IMA) and The Institute of Internal Auditors (IIA)
- The purpose of its guidance is to provide an overview for business executives and board members on cyber risk management through principles defined in the COSO Enterprise Risk Management Framework.
- This guidance provides context related to the fundamental concepts of cyber risk management techniques used to build strategic risk management policies for an enterprise. The intended audience and use of this article is listed below

Audience	Intended Use
Board of Directors	 Understanding of the following topics to aid in oversight of management cyber processes: The need for board and executive involvement for an effective cyber risk management program How to leverage the COSO Enterprise Risk Management (ERM) Framework to govern the cyber
Audit Committee Members	security strategy, execution and monitoring programKey concepts and examples of cyber risk management strategies
Executives (CEO, CIO, CRO, etc.)	 Understanding of the following topics to aid executive direction of cyber risk management: How to leverage the COSO Enterprise Risk Management (ERM) Framework to manage cyber risk Overview of cyber risk considerations and mitigation techniques (e.g., risk appetite, risk prioritization) Illustrative examples of notable technical cyber security frameworks
Cyber Practitioners	Understanding of how cyber risk fits into an ERM approach







NIST Cybersecurity Frameworks

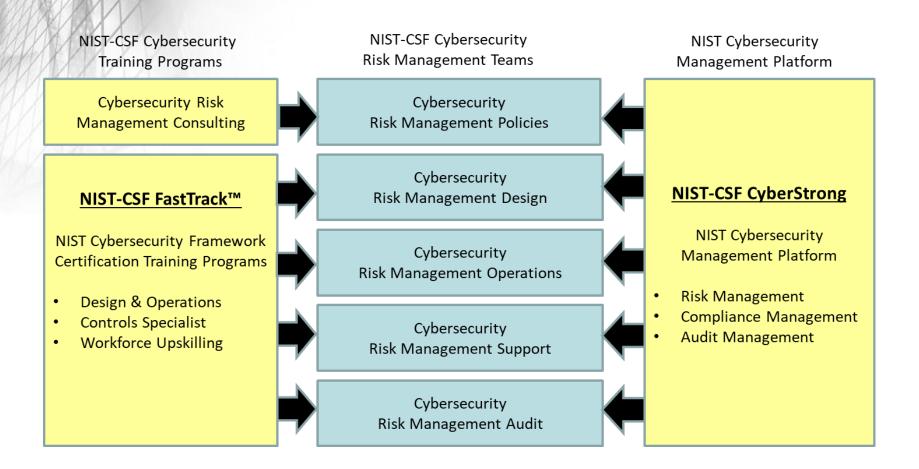
- The NIST Cybersecurity Framework was created to provide a uniform standard that **government**, **businesses and auditors** can use to align their cybersecurity risk management programs with business outcomes
- The NICE Cybersecurity Workforce Framework was created to identify the human capital required for a successful NIST Cybersecurity deployment.
- The combined NIST/NICE Frameworks have now been approved as the governing framework for **Cybersecurity Risk Management** for the US government along with a growing number of critical infrastructure sectors and international governments.
- itSM's NIST-CSF FastTrack[™] training programs provide organizations with the capability to **Design, Operationalize, Manage and Continually Improve** COSO aligned enterprise cybersecurity risk management policies using the NIST Cybersecurity Framework informative reference controls and management systems.







NIST-CSF FastTrack[™] Enterprise Training Program





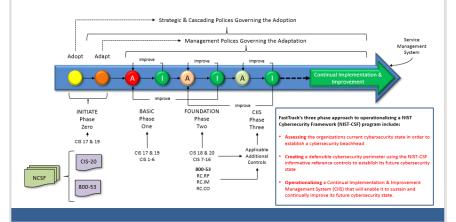


NIST-CSF FastTrack[™] Design & Operations Training

NIST-CSF FastTrack[™] certification training is designed to help organizations design & operationalize a cybersecurity program built around <u>COSO's Guidance for Managing Cyber Risk in a</u> <u>Digital Age</u> and the NIST Cybersecurity Framework. The program teaches candidates how to:

- Assess an enterprise current cybersecurity state in order to establish a cybersecurity beachhead
- **Design** a defensible cybersecurity perimeter using NIST-CSF informative reference controls to establish an enterprise future cybersecurity state
- **Operationalize** a Continual Implementation & Improvement Management System (CIIS) that will enable it to sustain and continually improve the enterprise future cybersecurity state.

NIST-CSF FastTrack™ - NIST CyberSecurity Design & Operations Training







NIST-CSF FastTrack[™] Design & Operations Training

For Cybersecurity & Risk Professionals

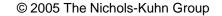
NIST-CSF FastTrack teaches Cybersecurity & Risk professionals <u>how</u> to design, implement, operationalize and continually improve the controls, management systems and workforce skills required to comply with an organization cybersecurity policies and regulatory requirements.

For Internal & External Auditors
 NIST-CSF FastTrack teaches
 cybersecurity auditors <u>what</u> NIST
 Cybersecurity core & mission critical
 capabilities (controls, management
 systems, workforce skills etc.) need to be
 in place in order to comply with an
 organization cybersecurity policies and
 regulatory requirement.

Experience. Practical Solutions

Strategic & Cascading Polices Governing the Adoption Management Polices Governing the Adaptation Service Management Adopt Adapt INITIATE BASIC FOUNDATION CIIS Phase Phase FastTrack's three phase approach to operationalizing a NIST Phase Phase Cybersecurity Framework (NIST-CSF) program include: Zero One Two Three sing the organizations current cybersecurity state in order t CIS 17 & 19 establish a cybersecurity beachhead Applicable CIS 17 & 19 CIS 18 & 20 Additional ating a defensible cybersecurity perimeter using the NIST-CSI CIS 1-6 CIS 7-16 CIS-20 Controls informative reference controls to establish its future cybersecuri 800-53 RC.RP BC IM ting a Continual Implementation & Improvemen 800-53 RC CO nagement System (CIIS) that will enable it to sustain and continually improve its future cybersecurity state

NIST-CSF FastTrack[™] - NIST CyberSecurity Design & Operations Training



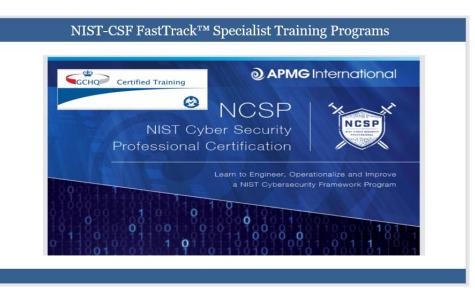


NIST-CSF FastTrack Specialist Training

The NIST-CSF FastTrack™ Specialist

Programs provide candidates access to a series of training programs that enable them to specialize in any of the informative reference areas associated with the NIST Cybersecurity Framework. Programs include:

- NIST Publication Training (800-53 etc.)
- RESILIA[™] Cyber Resilience Training
- Digital Transformation Readiness Training
- ITIL[™] V4 Training
- IQ4 Cybersecurity Virtual Internship Training
- CYBRScore Cybersecurity Skills Training







NIST-CSF FastTrack Specialist Training

- For Cybersecurity & Risk Professionals NIST-CSF FastTrack Specialist programs enable Cybersecurity & Risk professionals to become specialist in one or more of the informative references outlined in the NIST Cybersecurity Framework.
- For Internal & External Auditors
 NIST-CSF FastTrack Specialist programs
 enable cybersecurity auditors to learn the
 details behind the NIST-CSF informative
 reference controls to ensure they align with
 an organization cybersecurity policies and
 regulatory requirement.







NICE-CWF CyberStaff[™] Training

The NICE-CWF CyberStaff[™] Program is designed to rapidly upskill existing staff or new interns with the knowledge, skills and abilities to become NIST cybersecurity professionals. CyberStaff[™] training academies include:

- Knowledge Academy Online Certification training's where candidate learns the Knowledge of cybersecurity and the NIST cybersecurity framework via accredited certification training programs
- Skills Academy Online Practice Lab's where candidate learns the hands-on skills associated with NIST & NICE Frameworks
- Abilities Academy Online Virtual Internship training's where candidates learn to solve real world cybersecurity problems in collaboration other candidates and industry mentors.

NICE CyberStaff[™] NIST-CSF Workforce Upskilling & Intern Training Program







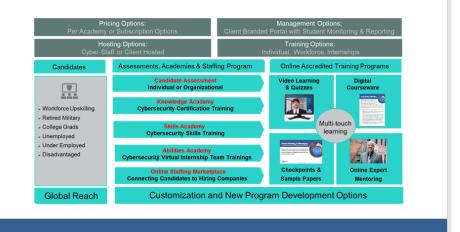
NICE-CWF CyberStaff[™] Training

• For IT, Cybersecurity & Risk Professionals The NICE-CWF CyberStaff[™] program enables organizations to rapidly upskill its current staff to support its NIST Cybersecurity program.

For New Interns

The NICE-CWF CyberStaff program provides interns with a pathway to the NIST & NICE skills required to become a contract or fulltime employee in the field of cybersecurity risk management.

NICE CyberStaff[™] NIST-CSF Workforce Upskilling & Intern Training Program







NIST-CSF FastTrack[™] CyberStrong Platform[™] Training

- The <u>CyberStrong Platform</u>[™] enables continuous improvement and real-time measurement, allowing your organization to manage cybersecurity as you would any other business function, irrespective of your company's size.
- CyberStrong's AI-powered optimizations automate risk mitigation action planning for compliance, risk and audit initiatives that enables an "always on" approach to previously state GRC activities.
- The result is a more efficient process, as well as more informed decision making. Executive reports are updated in real-time and shared with a single click, assuring non-security executives of your successes.







NIST-CSF FastTrack[™] CyberStrong Platform[™] Training

- For Cybersecurity & Risk Professionals CyberStrong provides an online tool kit and management system to perform NIST Cybersecurity assessments, policy development, project plans, work assignments, audits, status reports and realtime continuous risk monitoring and improvement.
- For Internal & External Auditors CyberStrong enable auditors to perform continuous assessments of the operating environment to ensure that the organization continues to meet or exceed its policy and regulatory requirements
- For Executive Management CyberStrong online governance dashboards provides executive management with real time visibility into its cybersecurity compliance and investments

Experience. Practical Solutions.







The CyberStrong Story

Automated, Intelligent Cybersecurity Compliance, Risk & Audit Management

George Wrenn, CyberSaint CEO and Founder, channeled his experience as the CSO of Schneider Electric, as a Consultant for the Fortune 100, and his involvement in NIST Cybersecurity Framework development to launch CyberSaint Security.

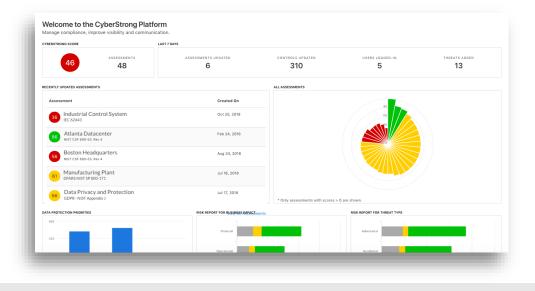
We envision a world where a all business functions and leaders align to build cybersecurity resilience and boost business productivity - protecting and empowering their most critical assets, employees, customers and partners. We empower our customers to leverage powerful technology that enables measurement, enhances communication and improves cybersecurity resiliency through the CyberStrong Integrated Risk Management platform.





Market Validation for CyberStrong

CyberStrong helps organizations foster a risk-aware culture that improves decision making and performance through an integrated view of how well that organization manages its unique set of risks.



"CyberSaint is an example of a technology provider that demonstrates a vision for addressing emerging risks associated with cybersecurity."

Gartner Competitive Landscape for Integrated Risk Management, Dec 2019

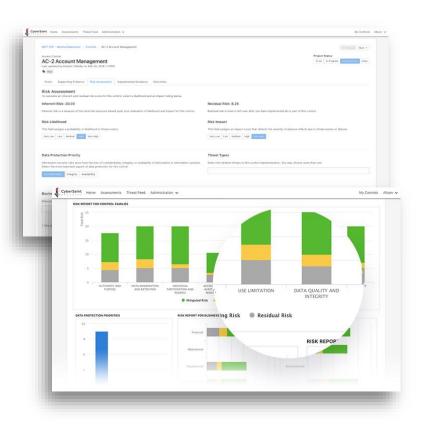




CyberStrong for Internal Audit

CyberStrong provides Internal Auditors with:

- Accountability, signoff, and activity tracking
- Intuitive repository for risk and compliance data
- Credible measurement and clear metrics
- Regulatory and legal compliance against standards
- Risk scoring against trusted methodologies
- Continuous improvement and real-time reporting
- Streamlined communication from audit, to executives, to boards
- Remediation action plans from executives to teams
- Return on Security Investment (ROSI) reporting



Communicate Program Posture to Executives. Empower Teams to Close Gaps.





Feature Highlights

Continuous Remediation Plans

Real-Time Reports for Auditors and Executives

Dashboard Controls Optimizations Reports	Threats Snapshots			
Score Simulator ^{lista}	a ta madal tanzata far una ananciadia	a and the lowest cost bishest insert one to get these	We arrived three energy law medium and black four shore	without these locals at some successful
Our optimization uses machine learning on historical dat compliance and provide a set of rank-ordered control su increasing marginal cost of improvement.	ggestions to attain each target. The ca	In and the roless cost, regress impact way to get them. acculations take into account your current score, the cor	we provide three scores, two, measure and rege. Our argo strols you have scored already, the cost and importance of	f each control in general, and the
LOW	MEDIUM		нон	
72		77		82
5 Controls View Controls		12 Centrols View Centrols		Controls
PE-2: Physical and Environmental Protection Physical	Arrass Authorizations		× Mar 15, 2018	Viewing 12 Cont
AC-18-5: Access Control Wireless Access Antennas			×	To Do.
CM-2-1: Configuration Management Baseline Configu			×	To Do
CP-2: Contingency Planning Contingency Plan				Norda Tanan
MP-2: Media Protection Media Access				Needs Service
AC-2: Access Control Account Management				
CM-2: Configuration Management Baseline Configura	ition .			To Do
Owner: Padraic O'Reilly				# Create Sna
Cambridge Datacenter 3	3			@ <u>Create Sni</u>
				Ø <u>Create Sor</u>
Cambridge Datacenter 3 Industrial - Bespoke Framework 1.0	50% project	t completed		🖉 Create Sou
Cambridge Datacenter 3 Industrial - Bespoke Framework 1.0 ashboard Controls Optimizations Report	50% project	t completed		🖉 Create Sou
Cambridge Datacenter 3 Industrial - Bespoke Framework 1.0 ashboard Controls Optimizations Report cers	50% project s Threats Snapshots			Ø Cente So
Cambridge Datacenter 3 Industrial - Englock Framework 1.0 unboard Controls Optimizations Report onts an of Action and Mitigation (POAM)	50% project 5 Threats Snapshots Spreadsheet	1. Download		Ø Cente Sor
ambridge Datacenter 3 Industrial - Burguiste Framework 1.0 anthourd Controls Optimizations Report overs an of Action and Mitigation (POMI) attems Security Flam (SSP)	50% project Threats Snapshots Spreadsheet Word Document	 Download Download 		Ø Coste Sor
anthonidge Datacenter 3 Industrial - Burguiste Framework 1.0 anthonard Controls Optimizations Report area and Action and Mitigation (POM) attems Security Flam (SSP) ak Assessment (RA)	50% project Threats Snapshots Spreadsheet Spreadsheet	Download Download Download		€ Crasts Sor
Ambridge Datacenter 3 Industrial - Respect 73 anthonard Controls Optimizations Report overs and Action and Mitigation (POMI) actem Security Plan (SSP) assessment (RA) assessment RM	> 50% project s Threads Enapshots Spreadsheet Spreadsheet PDF	Download Download Download Download Download		€ Crasts. Sor
anthonidge Datacenter 3 Industrial - Respects Pranework 1.0 anthonard controls Optimizations Report area and Action and Mitigation (POMI) acted Security Plan (SSP) assement Summary Report assement List Report	Sprachheet Sprachheet Sprachheet Sprachheet Por Por	Download Download Download Download Download Download		€ Crasta Sor
Anthonidge Datacenter 3 Industrial - Respect 7 January 10 anthonard Controls Optimizations Report overs and Action and Mitigation (POMI) assessment (RA) assessment (RA) assessment (RA) assessment (RA) assessment (RA) assessment (RA)	> 50% project s Threads Enapshots Spreadsheet Spreadsheet PDF	Download Download Download Download Download Download Download Download		€ Crasta Sor
Anthonidge Datacenter 3 Industrial - Respect 7 answork 1.0 anthonard controls Optimizations Report overs and Action and Mitigation (POMR) at Assessment (RA) assessment (RA)	Sprachheet Sprachheet Sprachheet Sprachheet po po po po	Download Download Download Download Download Download Download Download Download		€ Craste Sor
Anthonidge Datacenter 3 Industrial - Respect 7 answork 1.0 anthonal controls Optimizations Report overs and Action and Mitigation (POMR) at Assessment (RA) assessment (RA) as	S0% project Threads Supplieds Spreadtheet Word Decument Spreadtheet POF POF POF POF POF	Download		€ Contra line
Anthonidge Datacenter 3 Industrial - Respect 7/answork 1.0 anthona Controls Optimizations Report over an of Action and Mitigation (POMM) at Assessment (RA) assessment (RA) as	905 project Threats Shapshots Spreadsheet Spreadsheet POF POF POF POF POF	Download		e conte lior
Anthonidge Datacenter 3 Industrial - Respect 7/answork 1.0 anthona Controls Optimizations Report on Action and Mitigation (POMM) assessment (RA) assessment (R	Pors project Treats Snaphots Sprashheet Word Document Sprashheet Por Por Por Por Por Por	Download Download		e conteilor
Anthonidge Datacenter 3 Industrial - Respect 7/answork 1.0 anthona Controls Optimizations Report over an of Action and Mitigation (POMM) at Assessment (RA) assessment (RA) as	905 project Threats Shapshots Spreadsheet Spreadsheet POF POF POF POF POF	Download	redum Report 1 Download Low Report	e coste los

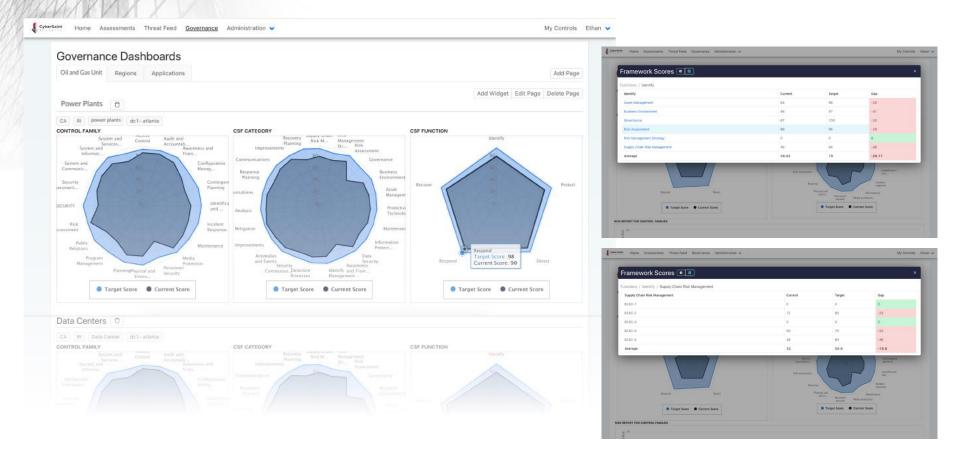


NIST CSF - Atlanta Datacenter



Create Snapshot

Dynamic Governance Dashboards







Questions <u>www.itsmsolutions.com</u> support@itsmsolutions.com





