

Defend Your Organization From Cyber Threats

with a Skills-Based Framework Approach & Fully-Mapped Paths by Job Roles

View Cyber Security Learning Paths

[Learn more](#)

A Real-World Practitioner with Real insights: Meet Aaron Kraus

[Learn more](#)

Featuring Accredited Certification Training from Cyber Security Industry Experts:

CompTIA

(ISC)²

PREFERRED OFFICIAL TRAINING PROVIDER

ISACA
Accredited Elite Partner

IT Control
Member Training Center

CERTNEXUS
Certified Security Analyst

 **LEARNING TREE**
INTERNATIONAL

Cyber Security Threats Are On The Rise

What's the best way to protect against attacks — and avoid becoming headline news?

\$11.4 million

The cost of global cybercrime per minute

- RiskIQ

58%

58% of CISOs said their IT systems were definitely or probably under attack without them knowing it

- Core Security

4 Million

The number of trained cyber professionals needed to close the skills gap

- (ISC)² Cybersecurity Workforce Study

Optimize Your Cyber Security Workforce by Leveraging Industry Frameworks

Learning Tree's holistic skill-based training is mapped to two key industry frameworks to address gaps and create better alignment between people, processes, policy, and technology.

The National Initiative for Cybersecurity Education (NICE) Framework

The NICE Framework has seven categories, each comprised of several specialty areas. Each specialty area is comprised of tasks, as well as the Knowledge, Skills, and Abilities (KSAs) required to complete the tasks.

National Institute of Standards & Technology (NIST) Framework

With the NIST Cybersecurity Framework, an organization can overlay the Framework across current processes to determine gaps in its current cyber security risk approach and develop a roadmap to improvement.



People

Having a clear, up-to-date understanding of job roles and the competent people to fulfill those roles is essential for any organization to function effectively in a cyber security environment.



Process/Policy

Cyber attacks are evolving and striking organizations constantly. To continuously defend your organization from these threats, your workforce needs to establish structured processes and implement best practices.



Technology







While new technology can be easy to acquire, your organization will still be at risk of an attack until your people have the right security skills. By providing your workforce with the right cyber security training, your technology will be implemented at full potential.

Learning Aligned to the International Standards Organization

ISO/IEC 27001 is an information security standard and part of the ISO/IEC 27000 family of standards. It is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its goal is to provide a standard to align security practices and methodologies. Adhering to this standard can help keep your organization safe. ISO 27002 is the list of detailed controls that can be referenced to meet the standard. ISO 27001 has a rigorous certification process and passing this is a coveted achievement.

Course Alignment

Courses in our NICE Framework learning paths also align to the following ISO 27001 areas.

NICE/NIST Category	ISO 27001	Learning Tree Learning Path Section
 <p>Oversee & Govern</p>	<p>Security policies A5 (what & how to)</p> <p>Organization of information security A6 (including mobile and homeworking)</p> <p>Human resources security A7 (joiners, movers & leavers)</p> <p>Supplier relationships A15 (agreements, SLAs, reviews, risk)</p>	<p>Executive Cyber Leadership</p> <p>Cyber Security Management</p> <p>Strategic Planning & Policy</p> <p>Project/Program Management and Acquisition</p>
 <p>Operate & Maintain</p>	<p>Asset management A8 (acceptable use, classification & media)</p> <p>Information security aspects of business continuity management A17 (business continuity, disaster avoidance, IT redundancy)</p> <p>Compliance A18 (laws, regulations, privacy, information security reviews)</p>	<p>System Administration</p> <p>Data Administration</p> <p>Customer Service & Tech Support</p> <p>Network Services</p> <p>Systems Analysis</p>
 <p>Investigate</p>	<p>Information security incident management A16 (reporting events, responsibilities, response, evidence collection)</p>	<p>Forensics - FOR</p>
 <p>Analyze</p>	<p>Operational Security A12 (change management, capacity, malware, disaster recovery, logging, monitoring, vulnerability management)</p> <p>Communications security A13 (network segregation, information transfer, messaging)</p>	<p>All Source Analysis</p> <p>Exploitation Analysis</p> <p>Language Analysis</p> <p>Target Analysis</p> <p>Threat Analysis</p>
 <p>Securely Provision</p>	<p>System acquisition, development and maintenance A14 (security requirements, development and support processes)</p>	<p>Software Development</p> <p>Risk Development</p> <p>Systems Requirement Planning</p> <p>Systems Development</p> <p>Technology R&D</p> <p>Test & Evaluate</p>
 <p>Protect & Defend</p>	<p>Access control A9 (user and systems access)</p> <p>Cryptography A10 (key and encryption management)</p> <p>Physical environmental security A11 (entry/exit, disposal, clear desk, etc.)</p> <p>Information security incident management A16 (reporting events, responsibilities, response, evidence collection)</p>	<p>Cyber Defense Infrastructure Support</p> <p>Vulnerability Assessment & Management</p>

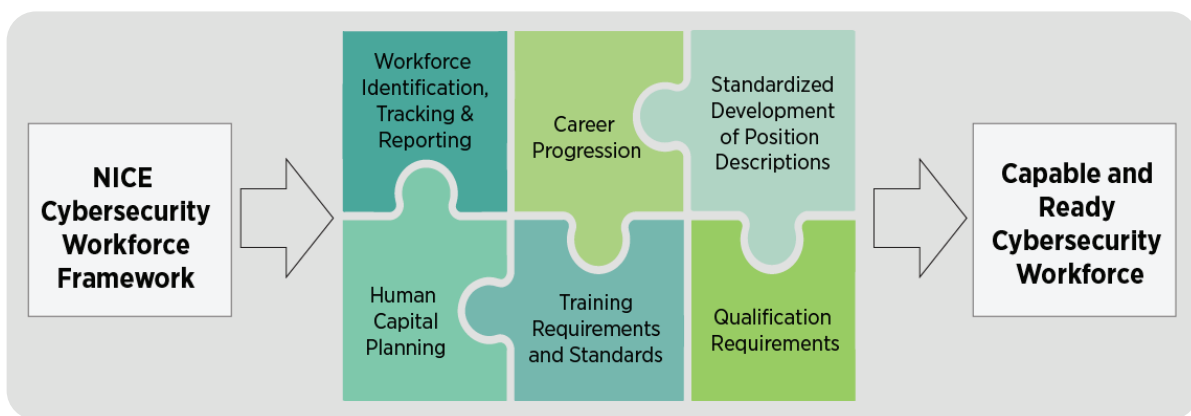
Learning Paths Aligned to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

NIST SPECIAL PUBLICATION 800-181

The NICE Framework

The National Initiative for Cybersecurity Education (NICE) Framework improves communication about how to identify, recruit, develop, and retain cyber security talent. It is a resource from which organizations can develop additional publications, tools, or training plans that meet their needs to define or provide guidance on various aspects of cyber security and IT workforce development, planning, training, and education.

The NICE Framework prescribes specialty areas of focus within high-level groupings of common cyber security functions that have an impact on an organization's ability to protect its data, systems, and operations. The framework provides a national standard for organizing the way employers, cyber security workers, and training and certification providers define and discuss cyber security work.



Learning Tree offers cyber security training in the following NICE Framework Cybersecurity Work Categories:



Analyze



Operate and Maintain



Oversee and Govern



Securely Provision

NIST

Risk Management



Investigate



Collect and Operate



Protect And Defend

Learning Tree Cyber Security Learning Paths Aligned to the NICE Framework



Analyze

Performs highly-specialized review and evaluation of incoming cyber security information to determine its usefulness for intelligence.

Course #	All-Source Analyst (Role: AN-ASA-001)	Level
4521	Starter Guide to Cyber Security	Foundation
E008	Security Essentials Labs	Foundation
446	CompTIA Security+ Certification	Intermediate
2047	Cyber Security Analyst Certification (CySA+)	Advanced
1904	All-Source Analyst	Foundation
1360	All-Source Analyst	Foundation
Course #	Exploitation Analyst (Role: AN-EXP-001)	Level
4521	Starter Guide to Cyber Security	Foundation
468	System and Network Security Fundamentals	Foundation
E008	Security Essentials Labs	Foundation
446	CompTIA Security+ Certification	Intermediate
537	Penetration Testing: Tools and Techniques	Intermediate
2049	CompTIA PenTest+ Certification	Intermediate
E006	Penetration Testing & Network Exploitation Labs	Intermediate
2047	Cyber Security Analyst Certification (CySA+)	Advanced
Course #	Multi-Disciplined Language Analyst (Role: AN-LNG-001)	Level
4521	Starter Guide to Cyber Security	Foundation
E008	Security Essentials Labs	Foundation
2012	Social Engineering	Intermediate
446	CompTIA Security+ Certification	Intermediate
2047	Cyber Security Analyst Certification (CySA+)	Advanced
Course #	Target Network Analyst (Role: AN-TGT-002)	Level
450	Networking Fundamentals	Foundation
468	System and Network Security Fundamentals	Foundation
2032	Certified Network Defender (CND)	Intermediate
2708	CompTIA Network+ Certification	Intermediate
2047	Cyber Security Analyst Certification (CySA+)	Advanced



Operate and Maintain Provides the support, administration, and maintenance necessary to ensure effective and efficient Information Technology (IT) system performance and security.

Course #	System Administrator - Microsoft Systems (Role: OM-ADM-001)	Level
4521	Starter Guide to Cyber Security	Foundation
E008	Security Essentials Labs	Foundation
2056	Identity Management	Intermediate
1551	System Administrator - Microsoft Systems	Intermediate
8593	System Administrator - Microsoft Systems	Intermediate
Course #	System Administrator - Linux/UNIX (Role: OM-ADM-L01)	Level
143	Linux Fundamentals	Foundation
– OR –		
428	UNIX Fundamentals	Foundation
2045	CompTIA Linux+ Certification	Intermediate
2056	Identity Management	Intermediate
144	Linux Administration and Support	Intermediate
1901	Linux Optimization & Troubleshooting	Advanced
396	UNIX and Linux Tools	Advanced
Course #	Systems Security Analyst (Role: OM-ANA-001)	Level
2060	System Security Certified Practitioner (SCCP)	Foundation
4521	Starter Guide to Cyber Security	Foundation
E008	Security Essentials Labs	Foundation
2010	Cyber Security Perimeter Defense	Intermediate
2046	Certified Advanced Security Practitioner (CASP)	Advanced
8591	Systems Security Analyst	Intermediate
Course #	Database Administrator - SQL Server (Role: OM-DTA-001)	Level
2107	Microsoft SQL Server® Introduction	Foundation
925	SQL Programming Fundamentals	Foundation
382	Relational Database Design	Intermediate
141	SQL Server High Availability	Advanced
8428	Performance Tuning and Optimizing SQL Databases	Advanced
Course #	Data Analyst (Role: OM-DTA-002)	Level
4521	Starter Guide to Cyber Security	Foundation
925	SQL Programming Fundamentals	Foundation
E008	Security Essentials Labs	Foundation
2065	Certified Information Privacy Professional (CIPP)	Intermediate
382	Relational Database Design	Intermediate
2066	Certified Information Privacy Technologist (CIPT)	Advanced

Certification Prep Training Course



Operate and Maintain – Continued

Course #	Database Administrator - Oracle (Role: OM-DTA-001)	Level
2226	Oracle Database 12c Introduction	Foundation
4521	Starter Guide to Cyber Security	Foundation
925	SQL Programming Fundamentals	Foundation
382	Relational Database Design	Intermediate
446	🔗 CompTIA Security+ Certification	Intermediate
2228	Oracle Database 12c Backup, Recovery, and Server Tuning	Advanced
Course #	Network Operations Specialist (Role: OM-NET-001)	Level
2060	🔗 System Security Certified Practitioner (SCCP)	Foundation
450	Networking Fundamentals	Foundation
468	System and Network Security Fundamentals	Foundation
E005	Network Essentials Lab	Foundation
2708	🔗 CompTIA Network+ Certification	Intermediate
451	Network Configuration & Troubleshooting	Intermediate
2046	🔗 Certified Advanced Security Practitioner (CASP)	Advanced
Course #	Technical Support Specialist (Role: OM-STS-001)	Level
468	System and Network Security Fundamentals	Foundation
2012	Social Engineering	Intermediate
445	🔗 CompTIA A+ Comprehensive	Intermediate
2046	🔗 Certified Advanced Security Practitioner (CASP)	Advanced
8590	Technical Support Specialist	Foundation
8592	Identity and Access Administrator Training	Intermediate



Collect and Operate Provides specialized denial and deception operations and collection of cyber security information that may be used to develop intelligence.

Course #	All Source-Collection Manager (Role: CO-CLO-001)	Level
4500	Big Data Technologies, Trends & Insights	Foundation
4521	Starter Guide to Cyber Security	Foundation
1250	🔗 Big Data Foundations - Certified Data Science Professional (DSA-CDSP)	Intermediate
2065	🔗 Certified Information Privacy Professional (CIPP)	Advanced
284	Critical Thinking for Problem Solving	Advanced
1231	Azure Training: Designing/Implementing Data Integration Solutions	Intermediate
1279	Azure Synapse Analytics Training	Intermediate
1266	Apache Kafka: Hands-On Training	Foundation



Securely Provision Conceptualizes, designs, procures, and/or builds secure Information Technology (IT) systems, with responsibility for aspects of system and/or network development.

Course #	Software Developer (Role: SP-DEV-001)	Level
4521	Starter Guide to Cyber Security	Foundation
E008	Security Essentials Labs	Foundation
2028	🔑 EC-Council Certified Application Security Engineer (CASE) .NET	Intermediate
1825	Secure Coding	Intermediate
940	Securing Web Applications, Services & Servers	Intermediate
2059	🔑 Certified Secure Software Lifecycle Professional (CSSLP)	Advanced
Course #	Secure Software Assessor (Role: SP-DEV-002)	Level
1830	Software Testing Fundamentals	Foundation
4521	Starter Guide to Cyber Security	Foundation
2028	🔑 EC-Council Certified Application Security Engineer (CASE) .NET	Intermediate
537	Penetration Testing: Tools and Techniques	Intermediate
2049	🔑 CompTIA PenTest+ Certification	Intermediate
940	Securing Web Applications, Services & Servers	Intermediate
2059	🔑 Certified Secure Software Lifecycle Professional (CSSLP)	Advanced
3161	🔑 Advanced Software Testing Analysis (ISTQB Certification)	Advanced
Course #	Authorizing Official/Designating Representative (Role: SP-RSK-001)	Level
4521	Starter Guide to Cyber Security	Foundation
2013	Cyber Security Risk Management	Intermediate
2037	🔑 Certified Risk and Information Systems Controls (CRISC)	Intermediate
Course #	Security Control Assessor (Role: SP-RSK-002)	Level
4521	Starter Guide to Cyber Security	Foundation
2013	Cyber Security Risk Management	Intermediate
2037	🔑 Certified Risk and Information Systems Controls (CRISC)	Intermediate
2051	Cyber Security Risk Assessment (U.S. Gov't)	Intermediate
Course #	Systems Requirements Planner (Role: SP-SRP-001)	Level
4521	Starter Guide to Cyber Security	Foundation
468	System and Network Security Fundamentals	Foundation
2013	Cyber Security Risk Management	Intermediate
2051	Cyber Security Risk Assessment (U.S. Gov't)	Intermediate
2058	🔑 Certified Information Systems Security Professional (CISSP)	Intermediate
289	Disaster Recovery Planning	Intermediate
2046	🔑 Certified Advanced Security Practitioner (CASP)	Advanced
Course #	Information Systems Security Developer (Role: SP-SYS-001)	Level
468	System and Network Security Fundamentals	Foundation
E008	Security Essentials Labs	Foundation
2058	🔑 Certified Information Systems Security Professional (CISSP)	Intermediate
E003	Systems Security Professional Essentials Labs	Intermediate
589	Vulnerability Assessment	Advanced
E007	Vulnerability Assessment Management Labs	Advanced



Securely Provision – Continued

Course #	Systems Developer (Role: SP-SYS-002)	Level
4521	Starter Guide to Cyber Security	Foundation
E008	Security Essentials Labs	Foundation
446	🔑 CompTIA Security+ Certification	Intermediate
940	Securing Web Applications, Services & Servers	Intermediate
2046	🔑 Certified Advanced Security Practitioner (CASP)	Advanced
Course #	System Testing and Evaluation Specialist (Role: SP-TST-001)	Level
1830	Software Testing Fundamentals	Foundation
4521	Starter Guide to Cyber Security	Foundation
537	Penetration Testing: Tools and Techniques	Intermediate
2049	🔑 CompTIA PenTest+ Certification	Intermediate
E006	Penetration Testing & Network Exploitation Labs	Intermediate
3161	🔑 Advanced Software Testing Analysis (ISTQB Certification)	Advanced



Risk Management Management level risk analysis, planning, and governance.

Course #	Risk Management Professional (Role: RM-RMF-001)	Level
2050	Cyber Security for Management and the Boardroom	Foundation
286	Risk Management for Projects, Programs and Operations	Foundation
2013	Cyber Security Risk Management	Intermediate
4528	NIST Framework Compliance	Intermediate
2051	Cyber Security Risk Assessment (US Gov't)	Advanced



Investigate Investigates cyber security events or crimes related to Information Technology (IT) systems, networks, and digital evidence.

Course #	Cyber Defense Forensics Analyst (Role: IN-FOR-002)	Level
4521	Starter Guide to Cyber Security	Foundation
E008	Security Essentials Labs	Foundation
2031	🔑 Certified Ethical Hacker (CEH)	Intermediate
537	Penetration Testing: Tools and Techniques	Intermediate
2049	🔑 CompTIA PenTest+ Certification	Intermediate
E002	Ethical Hacking Essentials Lab	Intermediate
E006	Penetration Testing & Network Exploitation Labs	Intermediate
2023	🔑 Computer Hacking Forensic Investigator (CHFI)	Advanced



Oversee and Govern

Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cyber security work.

Course #	Executive Cyber Leader (Role: OV-EXL-001)	Level
2050	Cyber Security for Management and the Boardroom	Foundation
2013 – OR –	Cyber Security Risk Management	Intermediate
2051	Cyber Security Risk Assessment (U.S. Gov't)	Intermediate
4528	NIST Framework Compliance	Intermediate
2026 – OR –	Certified CISO (CCISO)	Advanced
2038	Certified Governance of Enterprise IT (CGEIT)	Advanced
Course #	Privacy Officer/Privacy Compliance Manager (Role: OV-LGA-002)	Level
2065	Certified Information Privacy Professional	Foundation
2066	Certified Information Privacy Technologist	Intermediate
2067	Certified Information Privacy Manager	Advanced
Course #	Information Systems Security Manager (Role: OV-MGT-001)	Level
2050	Cyber Security for Management and the Boardroom	Foundation
2013	Cyber Security Risk Management	Intermediate
2051	Cyber Security Risk Assessment (U.S. Gov't)	Intermediate
3310	Strategic Thinking for Operational Management	Intermediate
4528	NIST Framework Compliance	Intermediate
2036	Certified Information Security Manager (CISM)	Advanced
Course #	Program Manager (Role: OV-PMA-001)	Level
3310	Strategic Thinking for Operational Management	Foundation
4521	Starter Guide to Cyber Security	Foundation
2013	Cyber Security Risk Management	Intermediate
2051	Cyber Security Risk Assessment (U.S. Gov't)	Intermediate
3611	Skills for Program Success	Intermediate
2036	Certified Information Security Manager (CISM)	Advanced
Course #	IT Project Manager (Role: OV-PMA-002)	Level
2050	Cyber Security for Management and the Boardroom	Foundation
2036	Certified Information Security Manager (CISM)	Advanced
296	Project Management Introduction	Intermediate
3310	Strategic Thinking for Operational Management	Intermediate
276	Project Management Professional (PMP)	Advanced
Course #	IT Program Auditor (Role: OV-PMA-005)	Level
4521	Starter Guide to Cyber Security	Foundation
E008	Security Essentials Labs	Foundation
446	CompTIA Security+ Certification	Intermediate
2040	Certified Information Systems Auditor (CISA)	Advanced



Oversee and Govern – Continued

Course #	IT Project Manager (Role: OV-PMA-A02)	Level
2050	Cyber Security for Management and the Boardroom	Foundation
918	🔗 Agile Fundamentals (ICP-FA Certification)	Foundation
2036	🔗 Certified Information Security Manager (CISM)	Intermediate
3310	Strategic Thinking for Operational Management	Intermediate
3641	🔗 DevOps Software Certification (ICP-FDO Certification)	Intermediate
1213	🔗 (ISC)2 CCSP Certified Cloud Security Professional	Advanced

Course #	Cyber Policy and Strategy Planner (Role: OV-SPP-002)	Level
4521	Starter Guide to Cyber Security	Foundation
E008	Security Essentials Labs	Foundation
2012	Social Engineering	Intermediate
2013	Cyber Security Risk Management	Intermediate
2037	🔗 Certified Risk and Information Systems Controls (CRISC)	Intermediate
2046	🔗 Certified Advanced Security Practitioner (CASP)	Advanced
284	Critical Thinking for Problem Solving	Advanced

🔗 **Certification Prep Training Course**

Meet Our Cyber Security Curriculum Dean: Aaron Kraus



About Aaron Kraus

Aaron Kraus is a Learning Tree Instructor and InfoSec/Cybersecurity executive with 15 years of experience across diverse industries. He blends a diverse background of education, leadership, and global perspective on risk-based decision making into actionable, data-driven information security management.

Insights from Aaron:

- On-Demand Webinar | [Cyber Security for Your Newly-Remove Workforce >](#)
- Blog Series | [Inside the NICE Framework >](#)

Learn More at: LearningTree.com/SecureIT
or Call 1-800-843-8733





Protect and Defend

Identifies, analyzes, and mitigates threats to internal Information Technology (IT) systems and/or networks.

Course #	Cyber Defense Analyst (Role: PR-CDA-001)	Level
4521	Starter Guide to Cyber Security	Foundation
2010	Cyber Security Perimeter Defense	Intermediate
2032	Certified Network Defender (CND)	Intermediate
446	CompTIA Security+ Certification	Intermediate
E005	Network Essentials Lab	Intermediate
2047	Cyber Security Analyst Certification (CySA+)	Advanced
2031	Certified Ethical Hacker (CEH)	Advanced
E002	Ethical Hacking Essentials Lab	Advanced

Course #	Cyber Defense Incident Responder (Role: PR-CIR-001)	Level
4521	Starter Guide to Cyber Security	Foundation
E008	Security Essentials Labs	Foundation
2025	EC-Council Certified Incident Handler (ECIH)	Intermediate
- OR -		
446	CompTIA Security+ Certification	Intermediate
2031	Certified Ethical Hacker (CEH)	Intermediate
E002	Ethical Hacking Essentials Lab	Intermediate
2070	Cyber Security First Responder (CFR)	Advanced
537	Penetration Testing: Tools and Techniques	Advanced
2049	CompTIA PenTest+ Certification	Intermediate
E006	Penetration Testing & Network Exploitation Labs	Advanced

Course #	Cyber Defense Infrastructure Support Specialist (Role: PR-INF-001)	Level
2060	System Security Certified Practitioner (SCCP)	Foundation
468	System and Network Security Fundamentals	Foundation
2010	Cyber Security Perimeter Defense	Intermediate
2031	Certified Ethical Hacker (CEH)	Intermediate
2032	Certified Network Defender (CND)	Intermediate
E005	Network Essentials Lab	Advanced

Course #	Vulnerability Assessment Analyst (Role: PR-VAM-001)	Level
589	Vulnerability Assessment	Foundation
940	Securing Web Applications, Services & Servers	Foundation
E007	Vulnerability Assessment Management Labs	Foundation
537	Penetration Testing: Tools and Techniques	Intermediate
2049	CompTIA PenTest+ Certification	Intermediate
E006	Penetration Testing & Network Exploitation Labs	Intermediate
2046	Certified Advanced Security Practitioner (CASP)	Advanced

High-Performance Training & Implementation Solutions From Learning Tree

Technology Brands

Adobe	IBM	Oracle	SAP
AWS	Lean Six Sigma	Red Hat	VMware
Cisco	Microsoft	Salesforce	

IT & Management Training Topics

Agile & Scrum	Cyber Security	Linux & UNIX	Python, Perl & C++
Apple Programming	DevOps	Microsoft Dynamics 365	SharePoint
Azure	FAC P/PM	Microsoft Office	Software Development
Big Data & Data Science	ITIL®	Mobile App Development	SQL Server
Business Analysis	ITSM Certification Training	.NET / Visual Studio	Web Development
Business Intelligence	Java Programming	Networking & Virtualization	Windows Training
Cloud Computing	Leadership & Professional Development	Power BI	
Communication Skills		Project Management	

500+ Expert Instructors – Real-World Practitioners

Serving our global footprint and averaging 15+ years of real-world consulting experience to deliver real-world results

Honored In Serving 60,000+ Organisations

For 45 years, Learning Tree has been a trusted partner for the world's largest corporations in Financial Services, Healthcare, all levels of Government, Professional Services, Manufacturing, Education and Non-Profits.

Demonstrated Past Performance

Offering end-to-end capabilities resulting in improved organisational performance – Workforce Development



LearningTree.com/SecureIT | 1-800-THE-TREE (843-8733)