DSM.promo

CYBERSECURITY TRAINING · CAPABILITY STATEMENT

Training the team your auditors will test.

Role-scoped cybersecurity and compliance training that maps to the standards your organization is examined against — assessed in, measured out, and delivered as board-ready evidence each cycle.

Core competencies

Security awareness
Behavioral training that measurably reduces click-through on simulated phishing and social engineering.

Compliance training
Mapped to the controls your auditors test. Completion records that survive an examination.

Hands-on labs
Live environments where teams practice detection and response — not slideware.

Incident drills
Tabletop and full simulation exercises with after-action reporting for leadership.

Role-based tracks
Distinct curricula for executives, developers, and general staff — scoped to the role.

Measurement & reporting
Risk-reduction metrics delivered as board-ready evidence each cycle.

Frameworks covered

Training maps to the standards your organization is examined against — the same frameworks DSM maintains at 100%.

NIST 800-171 · NIST CSF · CMMC 2.0 · SOC 2 · ISO 27001 · HIPAA · PCI DSS · FedRAMP · GDPR · CIS v8 · FISMA · DFARS 252.204-7012 + the full 18-framework compliance library

Baseline Knowledge Check — what it covers

Every cohort member completes a short baseline assessment before live training, so the day's focus is tuned to where the room actually needs it. Core competency areas:

C-01 **Cybersecurity acquisition awareness**
When cyber risk enters the acquisition lifecycle and the boundary of the contracting professional's role.

C-02 **DFARS & CUI understanding**
The purpose of DFARS 252.204-7012, what CUI is, and subcontractor flow-down obligations.

C-03 **NIST 800-171 & CMMC**
System Security Plans as primary evidence, POA&M for gaps, and how CMMC uses NIST controls.

C-04 **Vendor response review**
Spotting vague compliance claims, requesting real evidence, recognizing a complete answer.

C-05 **Cloud & data-handling risk**
The right questions about where CUI is stored, processed, or transmitted.

Who it's for

BY ROLE

— Executive & board — risk literacy, accountability
— Engineering & DevOps — secure SDLC, threat modeling
— General staff — awareness, reporting reflexes
— IT & security teams — detection, response drills

BY INDUSTRY

— Regulated SMBs under examination
— MSP-managed client portfolios
— Healthcare & financial services
— Government & defense supply chain

How it runs

01
Assess
Baseline risk, role mapping, and the controls in scope.

02
Plan
Curriculum scoped to findings and framework requirements.

03
Train
Delivery across chosen formats with completion gating.

04
Measure
Risk-reduction reporting packaged as audit evidence.

Train the team your auditors will test.

Book a scoping consultation — we baseline risk, map roles, and return a curriculum aligned to the frameworks you're examined against.

WEB
dsm.promo/training

CONSULTATION
dsm.promo/contact