

My top three categories of interest from the NICE framework

Abdias Noel

May 24, 2026

The NICE(National Initiative for Cybersecurity Education) is a framework that maps out the different cybersecurity aspects to corresponding IT roles, with the proper skill requirements, following multiple pathways. It comprises 5 five categories: Oversight & Governance, Design & Development, Implementation & Operation, Protection & Defense, and Investigation.

Oversight & Governance (OG) is where leadership, management and compliance reside. Professionals that operate within that sphere create policies, manage risks, ensure compliance, coordinate security programs, handle legal and governance concerns, oversee security operations at a high level. Some notable roles for that category are Cybersecurity Manager, Security Compliance Officer and IT Auditor

Design & Development (DD) for system architects and builders whose skills and focus lean towards secure software development and deployment, secure network infrastructure planning and build authentication systems. These professionals are found in roles like: Security Architect, Secure Software Developer, & DevSecOps Engineer, Cloud Security Engineer, and Systems Engineer.

Implementation & Operation (IO) is for professionals that deploy, configure, and maintain infrastructure. These the day-to-day workers that enforce the policies designed by the first category to the service of systems built by the second category. They include the likes of Network Administrators, Systems Administrators, VoIP Specialists and Security Operations Technician.

Protection & Defense (PD) are the active security guards of digital assets. Some of their roles include SOC analysts, threat hunters, incident responders, blue teams' operators. Their main work includes monitoring SIEM alerts, investigating suspicious traffic, log analysis.

Investigation (IN), This is the cyber detective division. They may be Digital Forensics Analysts, Cybercrime Investigator, Malware Analyst or Forensic Examiner and they investigate cybercrimes, system breaches, and digital evidence to recover deleted files, analyze compromised systems, trace attacker activity, and preserve evidence.

If I were to sort them in order of preference (strongest to lowest) it would go as follows: Design & Development, Implementation & Operation , Protection & Defense , Investigation and lastly Oversight & Governance.

Although I am analytical, I enjoy hands-on tasks where I plan, implement, and deploy solutions. This puts design and development as my top category. The next natural option to get hands-on is in operation, which is why it is my second choice. Protection and Defense is my third choice, because I notice I have been told that I have an uncommon level of attention to detail that would make me excel in such roles. Oversight and Governance would be my last choice, because it the furthest from hands-on and development in the entire group.

References

Cybersecurity and Infrastructure Security Agency. (n.d.). *NICE framework*.
<https://niccs.cisa.gov/tools/nice-framework>