Overview of The NIST Cybersecurity Framework 2.0 Initial Public Draft

Provided by LRS Education Services

Major Changes:

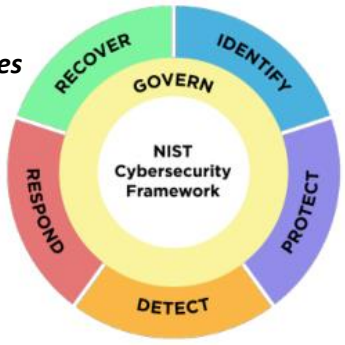
- Name: ***Cybersecurity Framework***
- Scope: ***All organizations worldwide***
- ***References*** are customizable per organizational needs. Integration with 7 NIST publications and many optional industry standards
- ***Implementation Examples*** to guide practical application of subcategories
- ***Profiles*** significantly expanded
- ***Governance*** and ***Supply Chain Risk Management*** emphases
- Increased guidance on ***cybersecurity measurement*** and ***assessment***

Goals:

- ***Understand and Assess:*** Describe current/target cybersecurity posture, determine gaps, align policy/business/technological cybersecurity risk management
- ***Prioritize***: opportunities for cybersecurity risk management, risk reduction aligned with mission, inform decisions about cybersecurity workforce needs and capabilities
- ***Communicate***: common language, concise distillation of fundamental cybersecurity concepts for executives to establish high-level risk management based on standards, guidelines, and practices

Framework Core Changes:

- 6 ***Functions***, 22 ***Categories***, 106 ***Subcategories***
- Addition of the ***Govern*** Function
- ***Implementation Examples*** added to each Subcategory
- Web-based frequently updated ***Informative References*** and ***Implementation Examples*** (full release early 2024)



Ways to Use the Framework:

- Create ***Profiles*** to support ***Understand and Assess***
- Characterize risk management outcomes with Framework ***Tiers***
- ***Communicate*** with internal and external stakeholders to support cybersecurity goals and to verify compliance
- Proactively update your ***cybersecurity*** and ***risk management*** practices to better counter the current threat landscape

LRS EDUCATION SERVICES