NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Component 3

How to Plan for your Cybersecurity Workforce

September 18, 2013

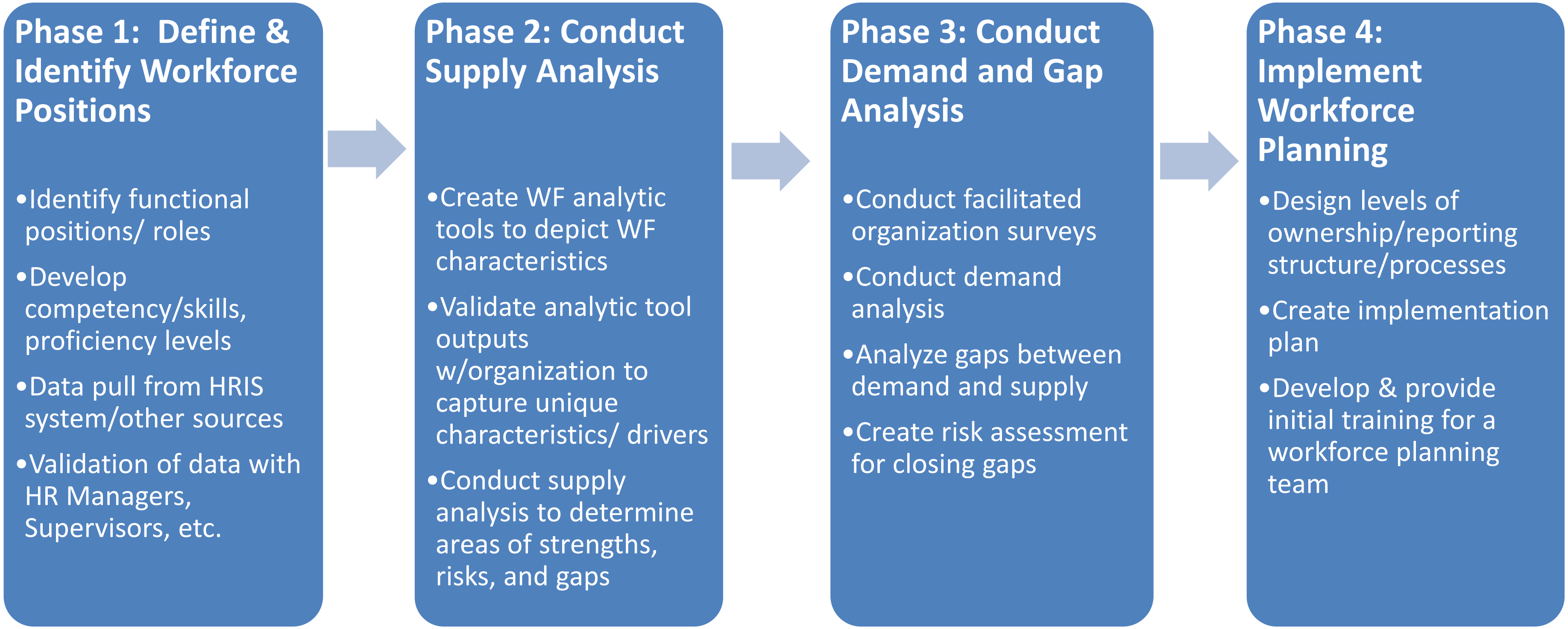
Cybersecurity Workforce Planning

As the demands of global business, computing, and society continue to revolve around information technology, cybersecurity workload is increasing faster than cybersecurity professionals can meet the demand. Workforce planning is used to address demand issues and close the workforce gap in a systematic way.

- To investigate this approach, Component 3 of the National Initiative for Cybersecurity Education (NICE) has researched the leading practices in workforce planning and identified unique considerations for application to cybersecurity.
- The intent of the current research is to encourage discussion around the best methods for cybersecurity workforce planning.

Why Workforce Planning?

***Workforce planning** is a systematic way for organizations to identify current human capital capabilities (supply), determine future human capital requirements (demand), and design and implement strategies to transition the current workforce to the desired future state.*



Phase 1: Define & Identify Workforce Positions

- Identify functional positions/ roles
- Develop competency/skills, proficiency levels
- Data pull from HRIS system/other sources
- Validation of data with HR Managers, Supervisors, etc.

Phase 2: Conduct Supply Analysis

- Create WF analytic tools to depict WF characteristics
- Validate analytic tool outputs w/organization to capture unique characteristics/ drivers
- Conduct supply analysis to determine areas of strengths, risks, and gaps

Phase 3: Conduct Demand and Gap Analysis

- Conduct facilitated organization surveys
- Conduct demand analysis
- Analyze gaps between demand and supply
- Create risk assessment for closing gaps

Phase 4: Implement Workforce Planning

- Design levels of ownership/reporting structure/processes
- Create implementation plan
- Develop & provide initial training for a workforce planning team

UNDERSTANDING CYBERSECURITY WORKFORCE PLANNING

Organizations will benefit from the following resources when it comes to improving their Cybersecurity Workforce.

1. A ***best-practice driven cybersecurity workforce planning approach*** should be developed, integrating the specific practices identified within the taxonomy of the National Cybersecurity Workforce Framework (the Framework).
2. A ***Capability Maturity Model (CMM)*** should be developed to allow organizations to self-identify their stage in workforce planning and make necessary adjustments to improve planning efforts for the cybersecurity workforce and workload.
3. The ***Cybersecurity Workforce Planning Diagnostic*** should be used by organizations to ascertain certain types of data they should consider when performing various types of analysis to determine the amount, type, and kind of cybersecurity workforce they would need to meet mission requirements.

Best Practices for Cybersecurity Workforce Planning

The *Best Practices for Cybesecurity Workforce Planning** whitepaper **highlights workforce planning methodology** and establishes an integrated and consistent means of diagnosing workforce needs and risks.

- Recommends best practice components of workforce planning, governance structures, risk assessments, alignment to the Framework, and how close monitoring of changes in skill sets and agility can aid in making quick course corrections within organizations.
- Examines workforce planning through three components— **process, strategy, and infrastructure**

PROCESS
Establishes an integrated and consistent means of diagnosing workforce needs and risks

STRATEGY
Provides a direct line of sight between business and workforce requirements

INFRASTRUCTURE
Supports execution of an effective and repeatable workforce planning process

- Together, these components allow an organization to better understand the state of its workforce and address needs to properly plan for workload

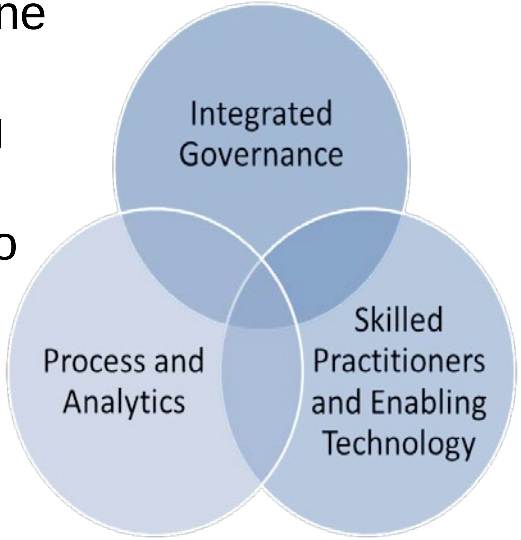
NICE
NATIONAL INITIATIVE FOR **CYBER**SECURITY EDUCATION

**** Best Practices for Planning A Cybersecurity Workforce***
white paper available on the NICCS Portal

NICE Capability Maturity Model (CMM)

A capability maturity model (CMM) **provides a structure for organizations to baseline current capabilities in cybersecurity workforce planning**, setting a foundation and consistent method of evaluation.

- Allows organizations to compare their capabilities to one another, across **process and analytics**, **integrated governance**, and **skilled practitioners and enabling technology.**
- Enables leaders to make better decisions about how to support progression and cybersecurity human capital investments.



Capability Maturity Model (CMM) focus areas

The NICE CMM* categorizes organizations through the use of three maturity levels:

- **Limited**: basic levels of workforce planning.
- **Progressing**: developing levels of workforce planning activity.
- **Optimizing**: key activity areas or segments of workforce planning capability which are fully developed.

***** ***NICE Capability Maturity Model (CMM)***
white paper available on the NICCS Portal

Cybersecurity Workforce Planning Diagnostic

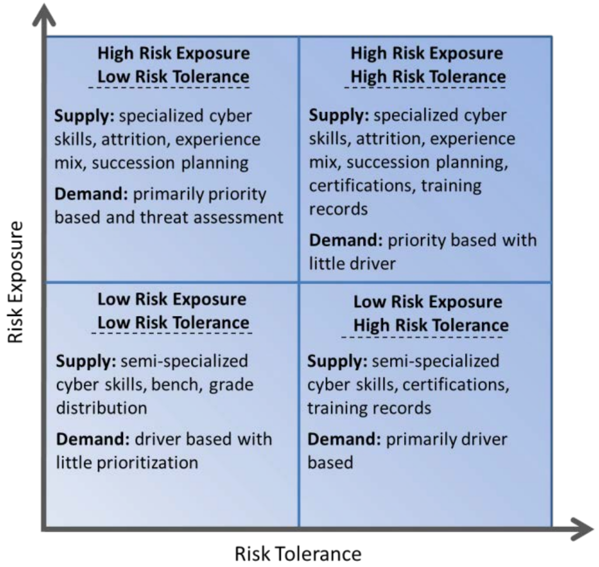
The Cybersecurity Workforce Planning Diagnostic assists organizations in thinking about **various data needs that support their cybersecurity workforce planning**

- Provides organizations with a way of thinking about certain types of data in terms of cybersecurity risk equation:

  (1) **risk exposure**: the likelihood that a threat will occur; and,

  (2) **risk tolerance**: the likelihood that the threat will succeed.

- Guides organizations through a series of questions which develops a unique diagnostic profile for that organization.



High Risk Exposure Low Risk Tolerance **Supply:** specialized cyber skills, attrition, experience mix, succession planning **Demand:** primarily priority based and threat assessment	High Risk Exposure High Risk Tolerance **Supply:** specialized cyber skills, attrition, experience mix, succession planning, certifications, training records **Demand:** priority based with little driver
Low Risk Exposure Low Risk Tolerance **Supply:** semi-specialized cyber skills, bench, grade distribution **Demand:** driver based with little prioritization	Low Risk Exposure High Risk Tolerance **Supply:** semi-specialized cyber skills, certifications, training records **Demand:** primarily driver based

- Depending on their profile, the diagnostic provides **specific data organizations need to collect** in order to perform effective cybersecurity workforce planning processes (e.g. analyze gaps and identify future workforce needs) based on risk exposure/risk tolerance type.

Cybersecurity Workforce Planning Diagnostic
Coming soon to the NICCS Portal

BENEFITS OF USING THE CYBERSECURITY WORKFORCE PLANNING METHODOLOGY, CMM, AND DIAGNOSTIC

No matter the maturity level, an organization will realize several benefits by practicing good cybersecurity workforce planning. These benefits include, but are not limited to:

- ***Increased consistency*** in execution of organization-wide Cybersecurity workforce planning activities;
- Enhanced ***data-driven decision making*** and analysis around shaping, building, growing, and supporting a cybersecurity workforce;
- Enhanced ***confidence and credibility*** from the field in headquarter decisions and guidance on cybersecurity workforce planning;
- ***Decreased response times to analysis requests and external reporting requirements***, enabling timely and proactive decisions to modify or change cybersecurity workforce policy as needed; and,
- ***Increased organizational alignment and pragmatic solution development*** between workforce, human capital, budget, and strategic planning organization sections or departments.

FURTHER INFORMATION

NICE will continue to share these materials with cybersecurity professionals across the nation in the public, private, and academic sectors.

For more information please visit: **http://niccs.us-cert.gov/**

Contact Information:

Robin “Montana” Williams

Director,

National Cybersecurity Education & Workforce Development Office

Tel (703) 235-5169

Robin.Williams@HQ.DHS.GOV