Changing Your Work Role Without Starting Over

Getting Into Something New - On Ramps, Back Doors, and Other Segues

This is an introduction to a series of future blogs addressing two specific questions from recent focus groups:

- How can I move into something new without having to start over?
- How can I move into management if I'm receiving no training?

This is work we love and believe in, but before exhorting you to make overtures or attempt contributions, we recommend doing some evaluation

- Understand your work culture - is it "stay in your lane" or open to curiosity and collaboration?
- As you prepare, what strengths or experience appear most relevant?
- Beyond the introduction here or in other blogs, what can you research or learn about?
- Who might be approachable to see where you can help?

What is on your side?
Every project has a timetable, budget, and some sort of methodology that calls for certain work, artifacts, and pace. If you can be a credible source and save the project a step or two it will be hard to pass up your offer of assistance.

Keeping all that in mind, let's look at where recent projects show openings. Our experience is that these two topics are samples that can be generalized. In other words, no matter how new or emergent the undertaking, there will be standard white collar work activities in the mix. If you are willing to learn and stretch a bit, then there is even more of an opportunity to begin a shift.

Later blogs will work on further details but here are some highlights from recent projects.

Cybersecurity

No one in business can ignore cybersecurity imperatives today. These projects consistently begin with inventory and assessment activities whether run in-house or using outside expertise. Here are elements of work that do not depend entirely on cybersecurity experience or expertise:

- **Procurement / Vendor Selection**: early conversations often focus on whether you need an indicative assessment or a full audit-type project; the former helps figure out how to get going, the latter would jump right to implementation, staffing, etc. Along the way, the usual request for proposal, vendor response tracking, and related support is needed
- **Project Management**: Scheduling session, scribing, tracking materials requested vs received; later prioritizing and implementing remediation
- **Content Management**: A sophisticated vendor CISO offered the idea of a Cybersecurity Governance Library but short of a taxonomy, gathering any existing policy, asset, and related data can help
- **Inventories**; Need roster of digital assets but often gets coupled with continuity and resiliency which leads to system, portal, and other resource identification
- **Cyber insurance**: demands reporting on network topology, service providers, PII / Personally Identifiable Information (literally record counts), and on and on

Volunteering for some of these "chores" can create your path to involvement.

Changing Your Work Role Without Starting Over

Getting Into Something New - On Ramps, Back Doors, and Other Segues

Cloud

The scalability, on demand provisioning, and cybersecurity strengths offered by today's major vendors create a compelling story. However, for many business computer systems, the move to the cloud often involves partial to full rewrite such as existing database to cloud vendor database, interaction with client infrastructure, etc.

As well as some of the activities mentioned in the cybersecurity section above, there is a big opportunity in these projects for testing – of system logic and behavior, outputs, new mechanisms for infrastructure related functionality such as providing reports, logs, print jobs, email automation, etc. This one begins with a careful look at your current environment and thinking about how to verify the new one has the advantages of the cloud but still does what you need it to do

- **Test case design**: think about both frequent transactions but also second tier frequency, periodic reporting, peripheral users, etc.
- **Testing**: doing the meticulous and sometimes repetitive steps of running or entering test scripts (It will not always work the first time)

If you want to dig a little deeper, focus on additional background materials. For example, a cybersecurity assessment vendor is likely to refer to one or more standards used in their work (see NIST or CIS). Or you may research exactly what your state or local regulations consider to be protected PII. (Personally Identifiable Information). This will let you further help with assessment and inventory activities.

For a cloud project, the particular vendor (AWS, Microsoft, or Google) will have background materials, certifications, etc. For example, AWS Certified Cloud Practitioner is a challenging but worthwhile designation. Even starting down the path will help you participate; the book is under $30 on Amazon.

Also, let's think about what happens when you get some experience to help focus on what you are looking to gain as you prepare
- context: you know the landscape (expectations)
- fluency: you know the terminology and activities
- work: some sense of the steps, efforts, analysis, etc.
- tools: what technologies are used

The approach is to start an orientation that moves you up on the experience curve. We begin with a very high level understanding of activities, deliverables, etc. as described here or especially in the more detailed blogs. Follow that up with some research and discussion and you have a story. All of which is meant to position you to provide something useful.

Almost every initiative these days involves technology so if you have some tech background that will help. But, the pace of change also means that we all must take some responsibility for learning so an appetite for that learning curve (hill?) may be the most important characteristic of all.

Finally, as you watch work unfold at your organization – company, agency, nonprofit, consultancy, whatever the format – where would a volunteer ease a bottleneck or backlog? Prep, and go!