1. If I use Amazon or other Cloud based system, am I then compliant simply by using these FedRamp approved cloud based systems?

   Yes, as long as the *implementation* of the service meets FedRAMP Moderate security baseline. Here's exactly what the DFARS says:

   > If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

   And here's the list of approved FedRAMP providers:
   https://marketplace.fedramp.gov/#/products?status=Compliant&sort=productName

   The bottom line is that any cloud service you choose needs to provide compelling evidence that they meet the FedRAMP Moderate security baseline. If they can't or won't, you shouldn't use them.

   The word *implementation* is italicized above because FedRAMP approval is just the first step in security certification; as a customer of a cloud service you must also ensure your particular instance is secure as well. To use an analogy:
   FedRAMP is the equivalent of the National Highway Traffic Safety Administration (NHTSA). The NHTSA provides a general certification that a manufacturer's vehicle is safe to travel America's roads; however, each state has its own safety inspection process that is more detailed than the NHTSA. Similarly, while FedRAMP certifies the vendor's product, the contractor must ensure their specific implementation of that product is secure as well. Thus, the cloud service provider must be able to provide you assurance that your particular instance is secured to the Moderate baseline.

2. How involved/robust does the incident response plan need to be?

   Here are the exact objectives from the 800-171A (DRAFT):

   - an operational incident-handling capability is established.
   - the operational incident-handling capability includes preparation.

- the operational incident-handling capability includes detection.
- the operational incident-handling capability includes analysis.
- the operational incident-handling capability includes containment.
- the operational incident-handling capability includes recovery.
- the operational incident-handling capability includes user response activities.
- incidents are tracked.
- incidents are documented.
- authorities to whom incidents are to be reported are identified.
- organizational officials to whom incidents are to be reported are identified.
- identified authorities are notified of incidents.
- identified organizational officials are notified of incidents.
- the incident response capability is tested.

Your IR plan must touch upon all of these elements to be compliant. The Centers for Medicare and Medicaid Systems (CMS) has a nice handbook on incident response, which includes a template for an Incident Response Plan in one of the Appendices: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf. This would be a great place to start developing your IRP.

3. For Access Control you mentioned "separating duties" – in a small business with limited "back office" personnel, what do you recommend to meet this control?

Here are the exact objectives from the 800-171A (DRAFT):

- the duties of individuals requiring separation to reduce the risk of malevolent activity are defined.
- organization-defined duties of individuals requiring separation are separated

I recommend generating a granular list of all duties performed at your organization with respect to the covered information and systems. Let's say you are an engineering company; you'd have duties such as "create usernames and passwords", "approve access to IT systems", "create engineering drawings", "send engineering drawings to customer", "create and send invoices", etc. Then create a matrix that shows what personnel execute each duty, and use that to help define which duties need to be separated. Notice the "organization-defined" in the objective—***you*** define the duties and the separation. You'll probably notice from the matrix that you already have a lot of separation.

BTW, you'll want to save the matrix you created as "compelling evidence" of your strategy to separate duties. The matrix is in fact part of your system security plan.

4. Do these requirements apply to small companies/small DoD contracts/grants?

   The requirements apply if the contract involves the contractor/company/organization processing “covered defense information” aka “Controlled Unclassified Information (CUI)” as listed here: https://www.archives.gov/cui/registry/category-list. The size of the business does not matter, so yes, small businesses/organizations can be subject to this requirement.

   CUI may or may not be explicitly marked as such by the government; it is up to the contractor to understand what information is and is not CUI, which may mean asking the government contract officer for direction.

5. Hi, I joined this just as you were on the tail end of discussing how to get a copy of the slideshow. I heard you mention a website, can I get a link to the slideshow?

   Rebecca emailed the slides to all participants, and the VIB Network will make them available on their website.

6. Does this pertain to Pallet Companies?

   It depends on what type of information the Pallet company processes, stores, or transmits to/for the DoD. See #4 above.