



Information Systems Contingency Planning

A Success Story

What are We Going to Talk About

- Introduction to the FBI
- Affect of Financial Systems on the FBI Mission
- Architecture of a Financial System
- Hardware Architecture
- Network Architecture
- Enterprise Redundancy
- Backup & Recovery
- Testing & Exercises
- Plan for Single Site Operation
- Have a Plan



Introduction to the FBI

- Who is the FBI?
 - We are the premier national law enforcement and domestic intelligence agency in the world.
- Why do our Information Systems need a Contingency Plan?
 - We have mission critical systems that we require to have operational in order to do our job and meet our mission.

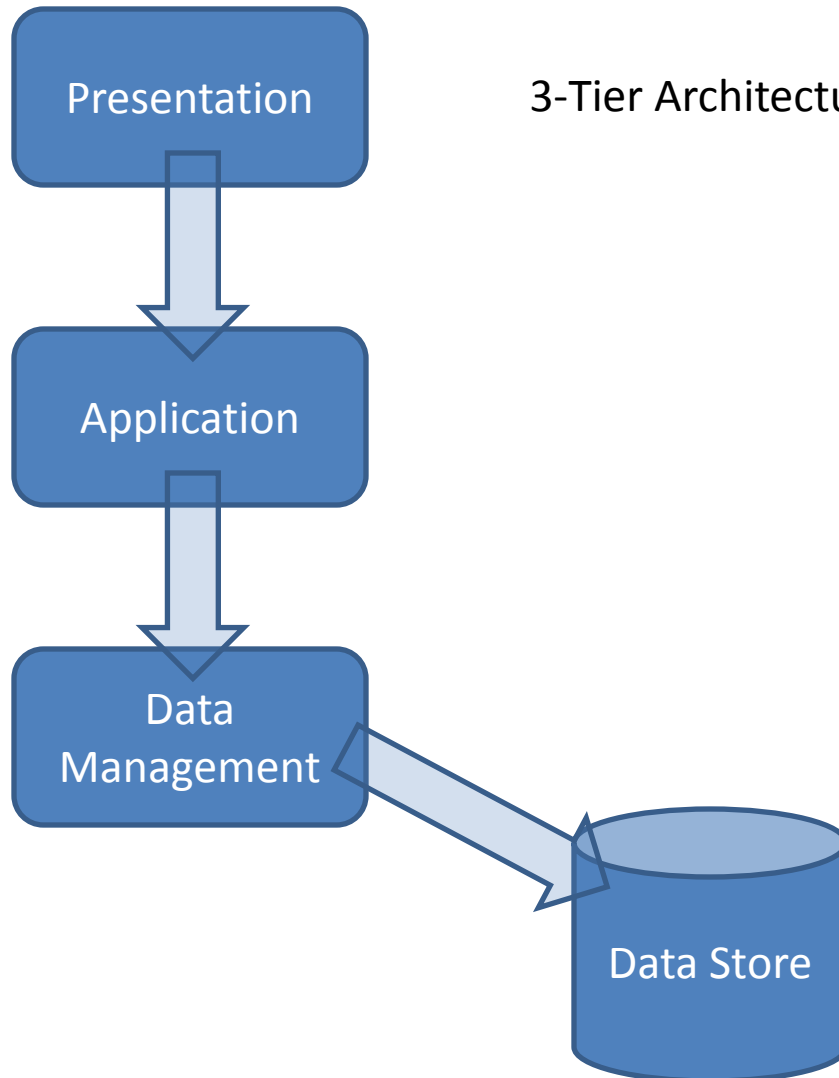


Financial Systems and the FBI Mission

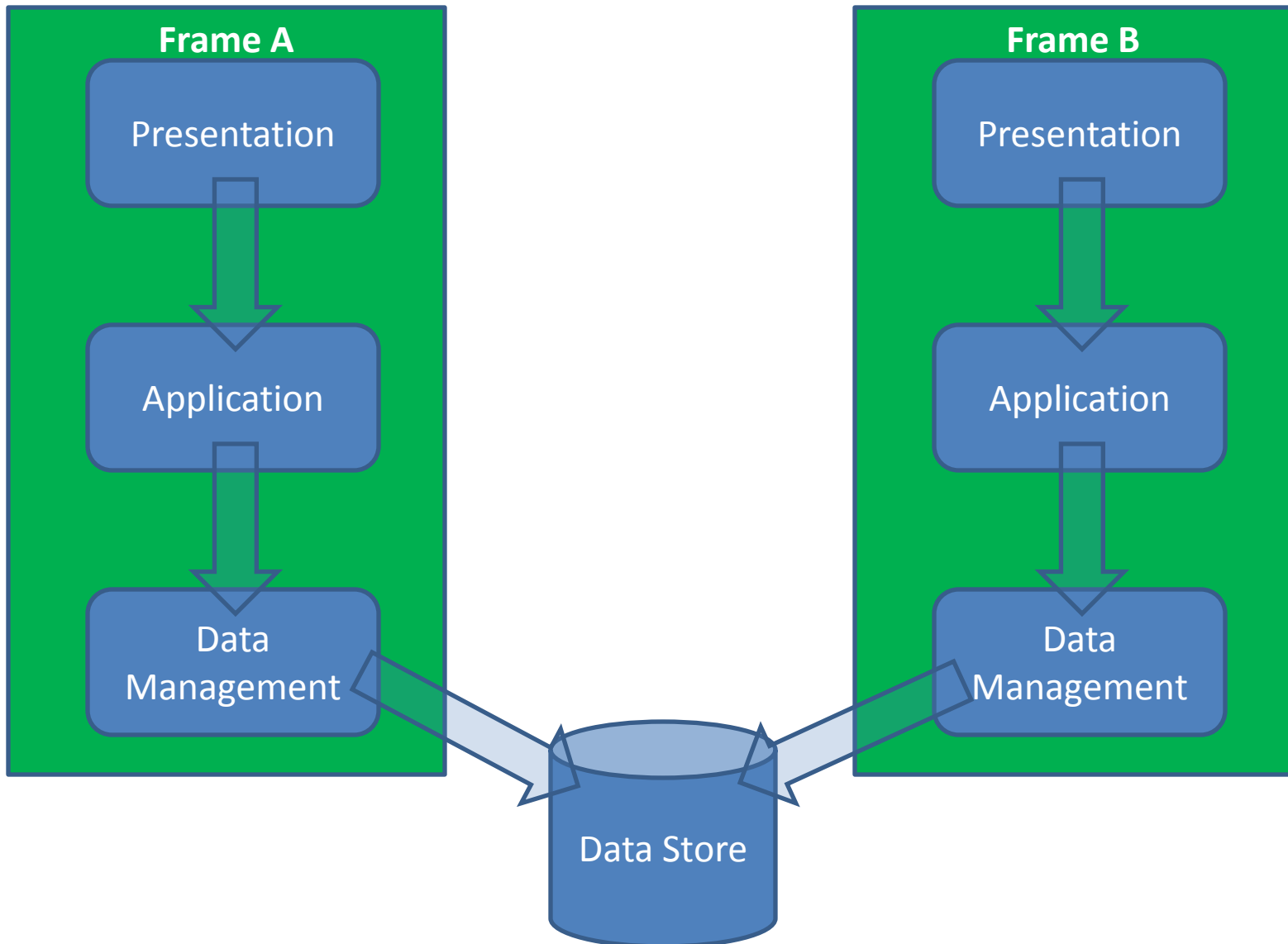
- Why can you not do without it?
 - You can! Just not as efficiently.
- Superstorm Sandy
 - Landfall: 29 Oct 2012, New Jersey, Post-Tropical Cyclone
 - \$71.4B Damages (US)
 - Fuel
 - Storage
 - Temporary Facilities



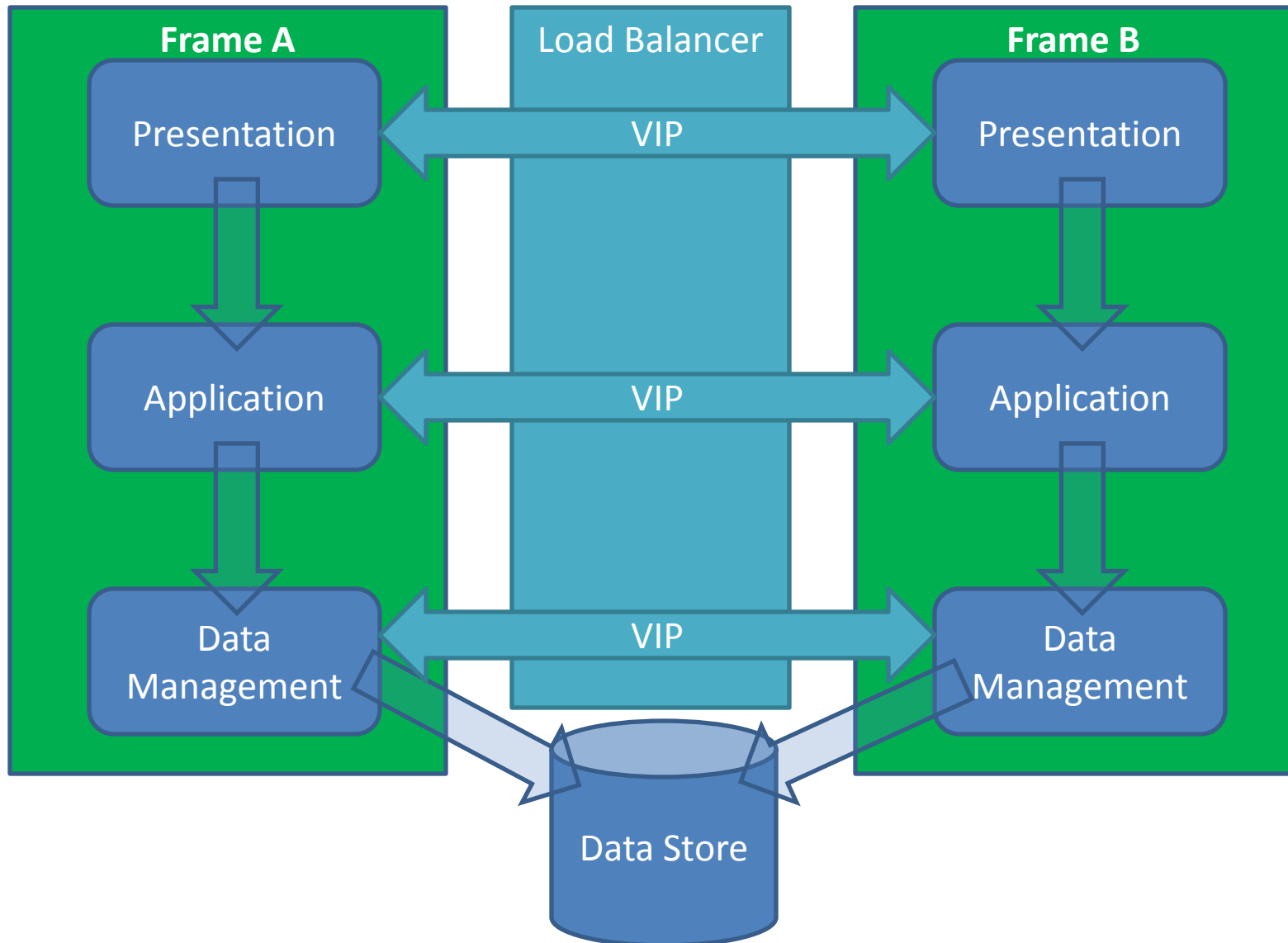
Architecture of a Financial System



Hardware Architecture

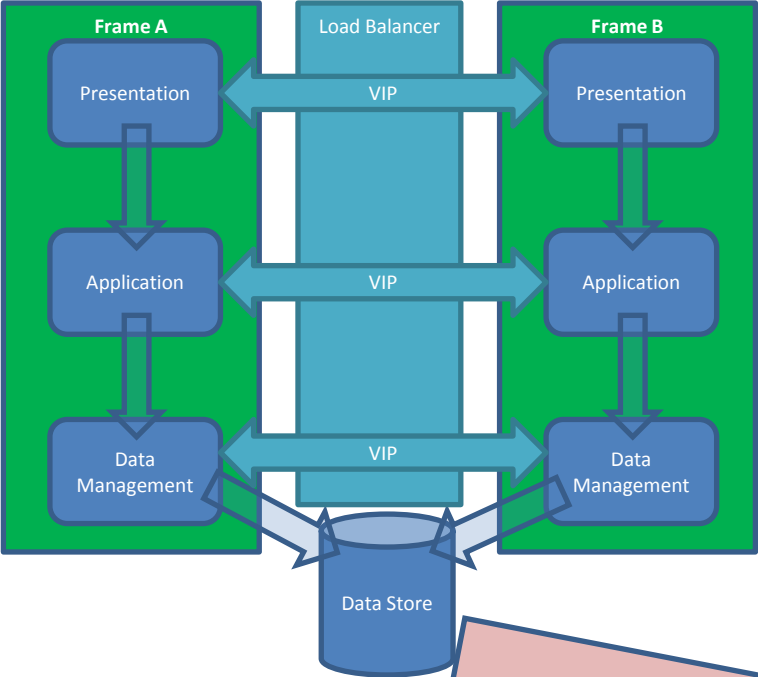


Network Architecture

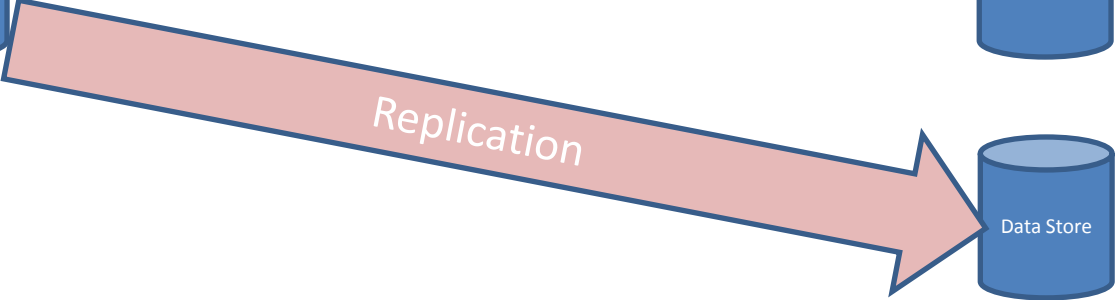
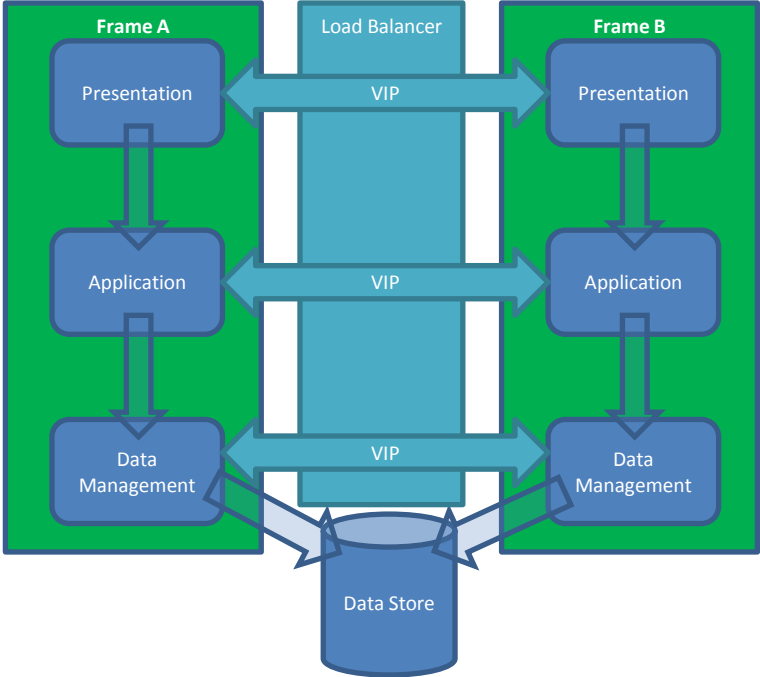


Enterprise Redundancy

Primary Site



Secondary Site



Back Up and Recovery

- Periodic Back Ups
 - Retention Period
 - Varies by content
 - Retention Locations
 - Local & Remote
- Back Up Validation
 - Weekly Recovery Tests
 - Random File Selections
 - Fully Automated Testing



Testing & Exercises

- Table Top Exercises
 - Inclusive: You don't know who will be available in a real situation
 - Realistic: Plan alternate paths through your scenario based upon the behavior of the participants
 - Learn: Refine your plan based upon your experience
- Recovery Exercise
 - Use Your Plan: Designate people to execute, designate others to observe and take note of any problems
 - Learn: Refine your plan based upon your experience



Single Site Operations

- Plan for Single Site Operations
 - Plan for sufficient infrastructure at each of your sites to support Single Site Operations
 - Sufficient, not excessive infrastructure
- What do you do with that “extra” infrastructure when all sites are functioning?
 - Planning / Staging / Executing System Upgrades
 - Development & Testing for Multiple Generations
- If your system is Mission Critical then you should plan to avoid outages during upgrades



Have a Plan

- Who will execute the ISCP? How much experience do they have? What do they need to know already? What can be automated?
 - You want to limit the amount of fore knowledge that is required.
 - You want to limit the number of people/organizations required to execute the plan.
 - You want to limit the number of dependencies before you get to that critical point.
- What things do you not worry about?
 - This varies by the type of IS. If you are an application then you don't worry about the Data Center. The Data Center must take care of itself. Now you don't have to worry about generators, cooling, fuel, ...
- Stage your plan with supporting materials (like a password list) and make sure the right people know how to get to it.
 - The right people will know about it because you engage them in table-top and hands-on recovery exercises.
 - Execute your plan. Have lots of observers. Refine your plan.
- You might not survive the situation – but your information system will!





Questions?