How Many Copies Is Enough?

A Flexible, Replicable Simulation Framework for Assessing Storage Risk

MIT Digital Document Preservation Simulation
iPRES 2015, Chapel Hill, NC

Micah Altman

Richard Landau

- MIT Libraries, Program on Information Science

- http://informatics.mit.edu

Problem to Solve

- How to protect a large, valuable, digital document collection
  - How many copies do you need to keep it safe?
  - Where to put the copies?
  - Are you sure they're still there?
  - Whether to use compression, encryption, … ?
- Not much hard data on which to base policy decisions
- We developed a flexible, replicable simulation framework
- We aim to provide some guidance, based on some common, but not universal, calibration points.

The Model We're Using

- You have a collection of digital documents
- You contract with some outside agencies to store copies of your collection
  - Specialized servers
  - Commercial cloud storage providers
    - Amazon, Google, Rackspace, BackBlaze, Dropbox, ...
- You "audit" the servers with some frequency
  - Do they still have copies of all documents?
  - Replace any copies missing or corrupted

Our Basic Data, to Extrapolate

- Not keyed to any specific problems
- Will supply many hints on how to extrapolate from our data to your situations
  - Number of docs, doc sizes, storage shelf sizes
  - Server failure rates
  - Audit strategies
- Experimental results
  – you can simulate with your own parameters

Assumptions

- Everything costs
  - Storing multiple copies
  - Higher quality services to store your docs
    - Data generally not available about "quality"
  - Bandwidth for auditing
- Our goal:
  - Provide data showing general tradeoffs
    - Use to set broad policies
  - Provide a framework to model specific characteristics
    - Use to check specific practices

Two Types of Failures

- One document at a time
  - Cosmic ray, disk block failure
- All documents in a collection
  - Local catastrophe
  - Economic downturn, change of business strategy
  - Loss of encryption key
- All failures are silent (to the client = library)
  - Until you try to retrieve a document
- Some failures are correlated
  - Local environment can affect block failures
  - Global conditions can affect multiple providers

Single Document Failure

- Common: A copy of a document dies on a particular server
- Documents are fragile
  - Compressed, encrypted: small failure makes document unreadable
- Variation: Repairable documents
    - Small failure damages only one segment
    - Model this as a set of smaller docs

Institutional Failure

- Less common: A server dies, losing all the documents it contains
  - Institutional failure due to fire, flood, war, economic downturn, etc.
- Infrequent but dangerous, particularly if correlated

Digital Simulation Programs

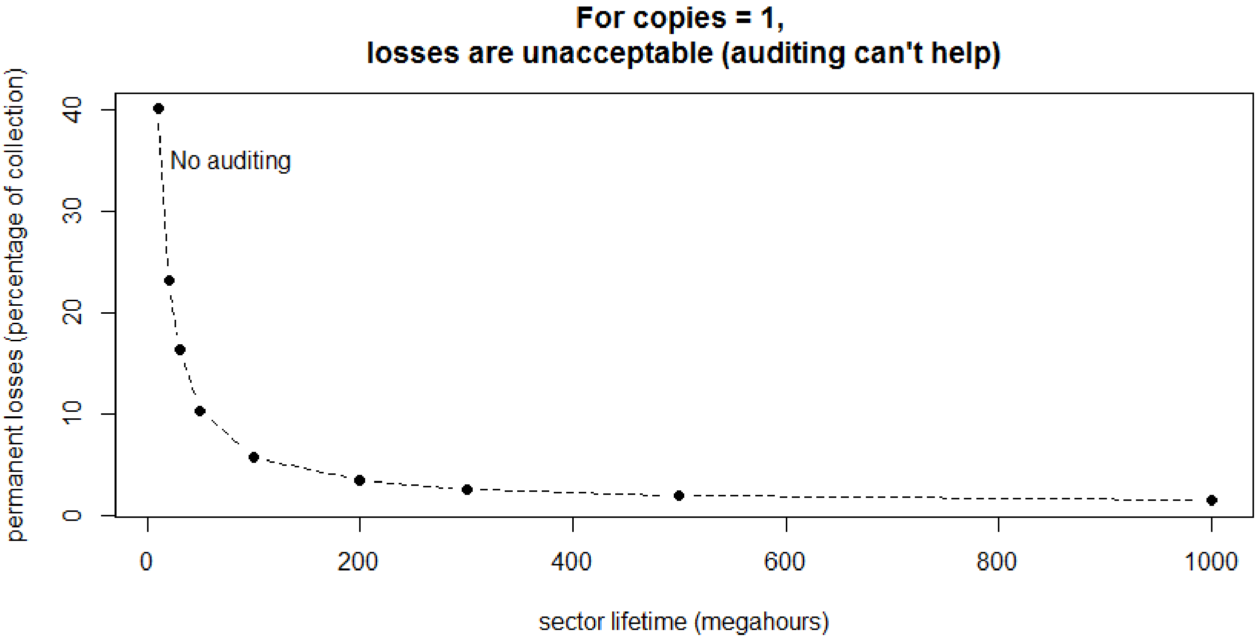
- Input
  - error rates, numbers of copies, auditing rate, etc.
- Output
  - number of documents permanently lost over the life of the test
- Discrete-event simulation
  - Failure events happen at random intervals
  - Audits are regularly scheduled
- Open source
  - Open license, available on Github

Observations

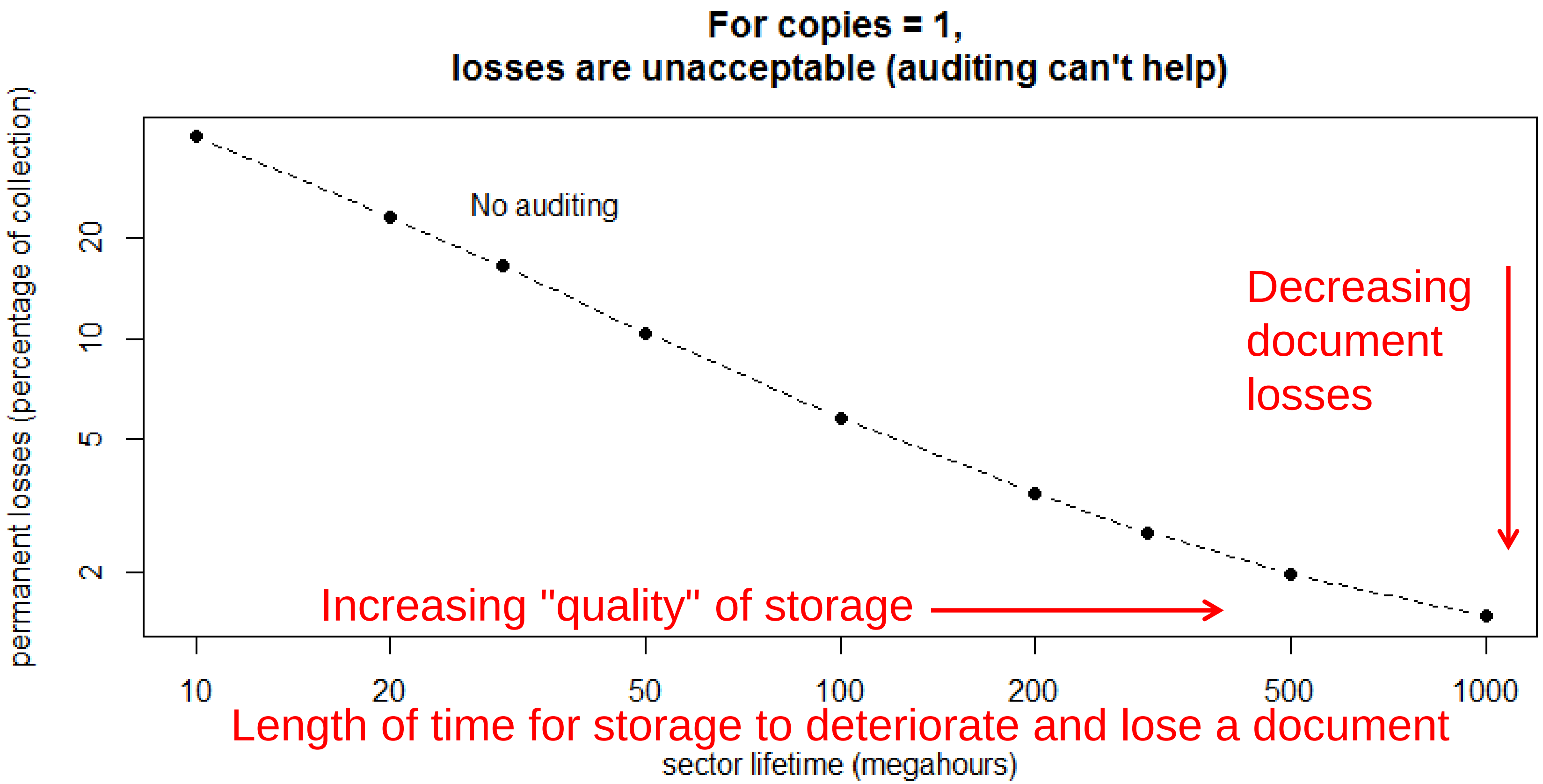
- For one copy, simple Poisson calculation yields failure rates
  - But hard to observe on simple graphs

Hard to Compare Curves

- $e^{-\text{something}}$ is a fading exponential curve
- Easier to compare if plotted as logs to straighten the lines



One Copy? All Losses Are Permanent Losses



For copies = 1,
losses are unacceptable (auditing can't help)

Decreasing document losses

Increasing "quality" of storage

Length of time for storage to deteriorate and lose a document

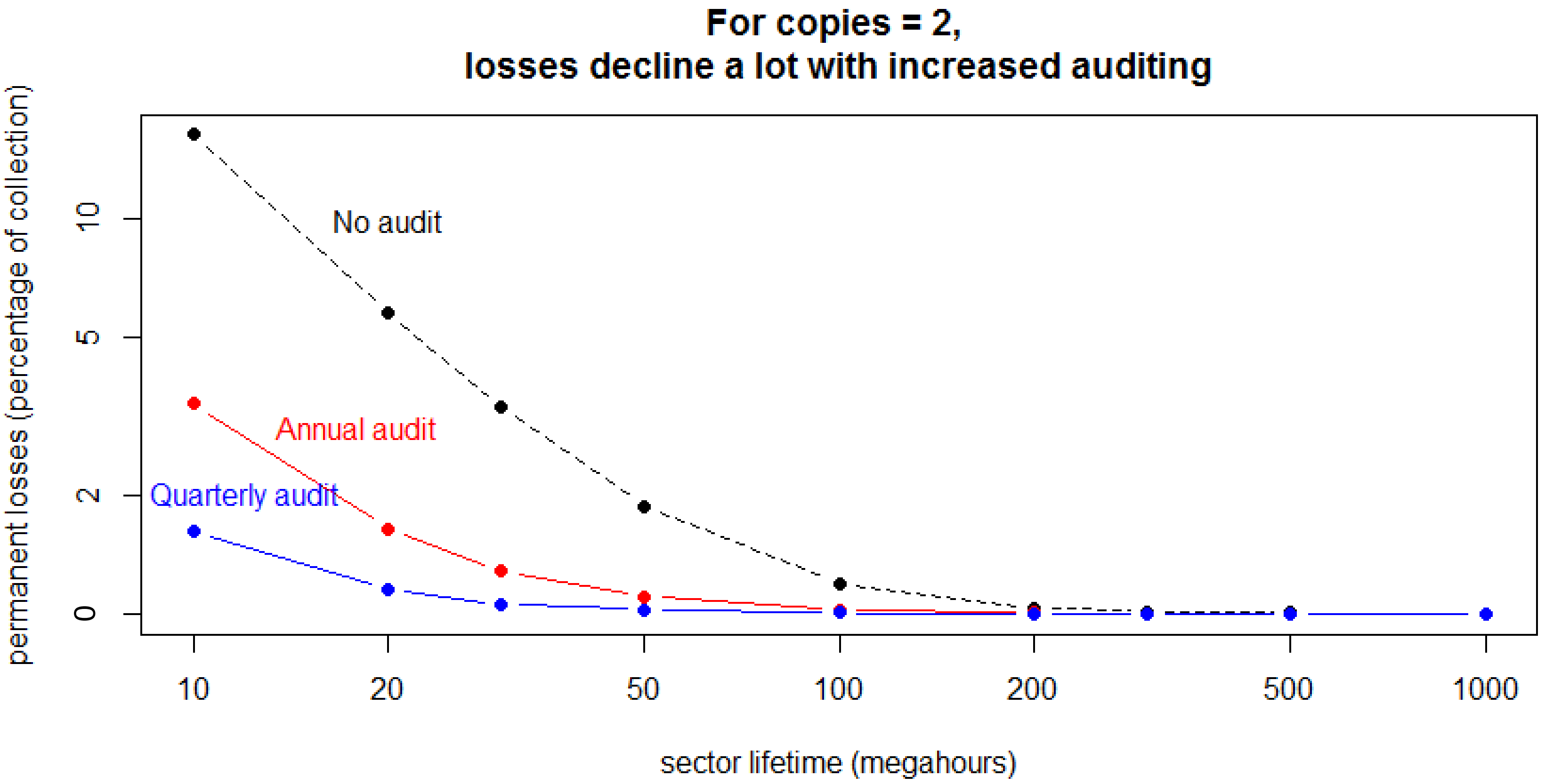
Good News & Bad News

- Bad news: if anyone really understands the "quality" of modern storage, he/she is not talking

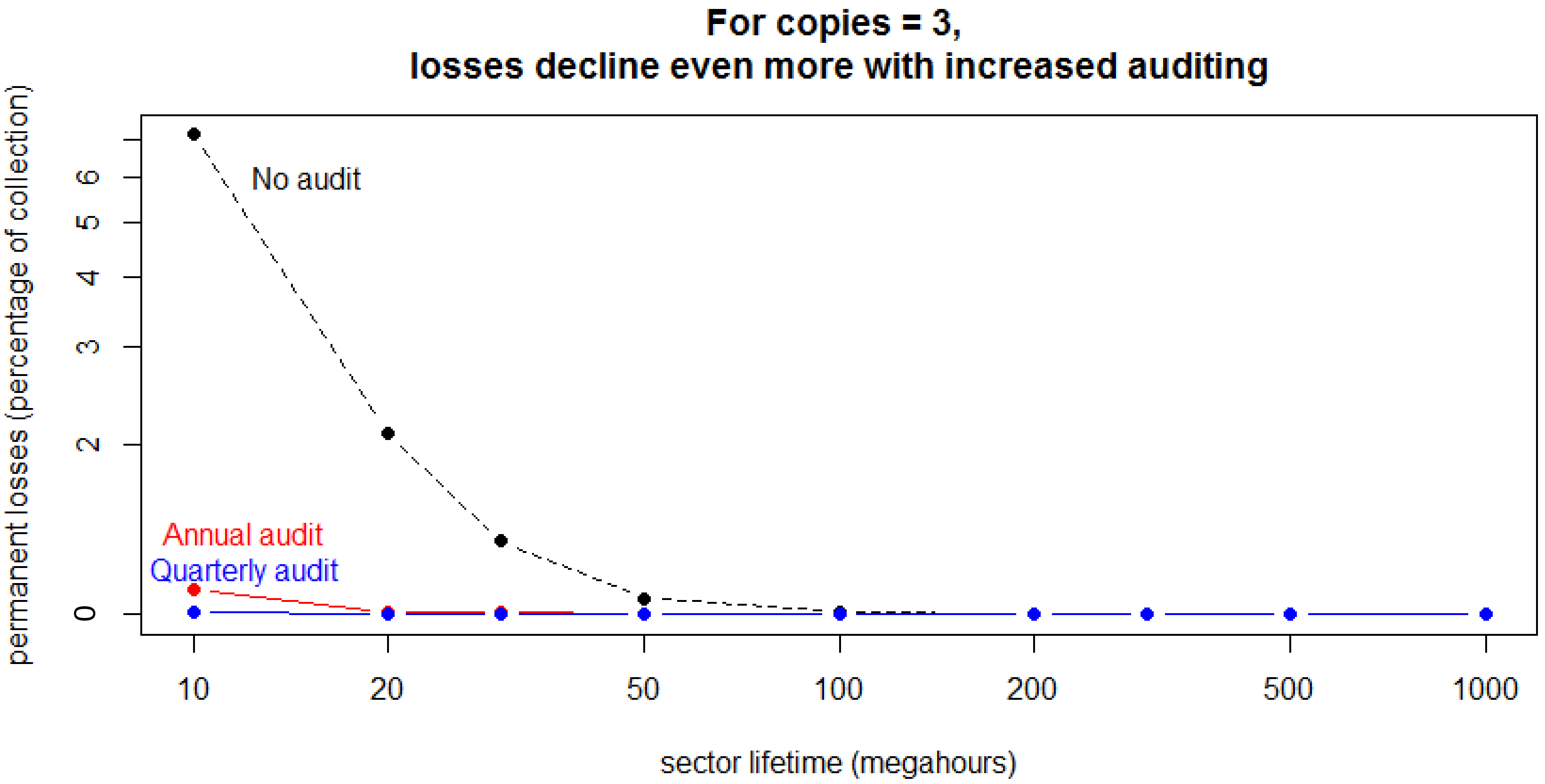
- Good news: we *think* that modern storage methods, like those used in cloud storage, are very reliable, high quality

- Strategy: Structure storage to protect your collection from *variations* in reliability

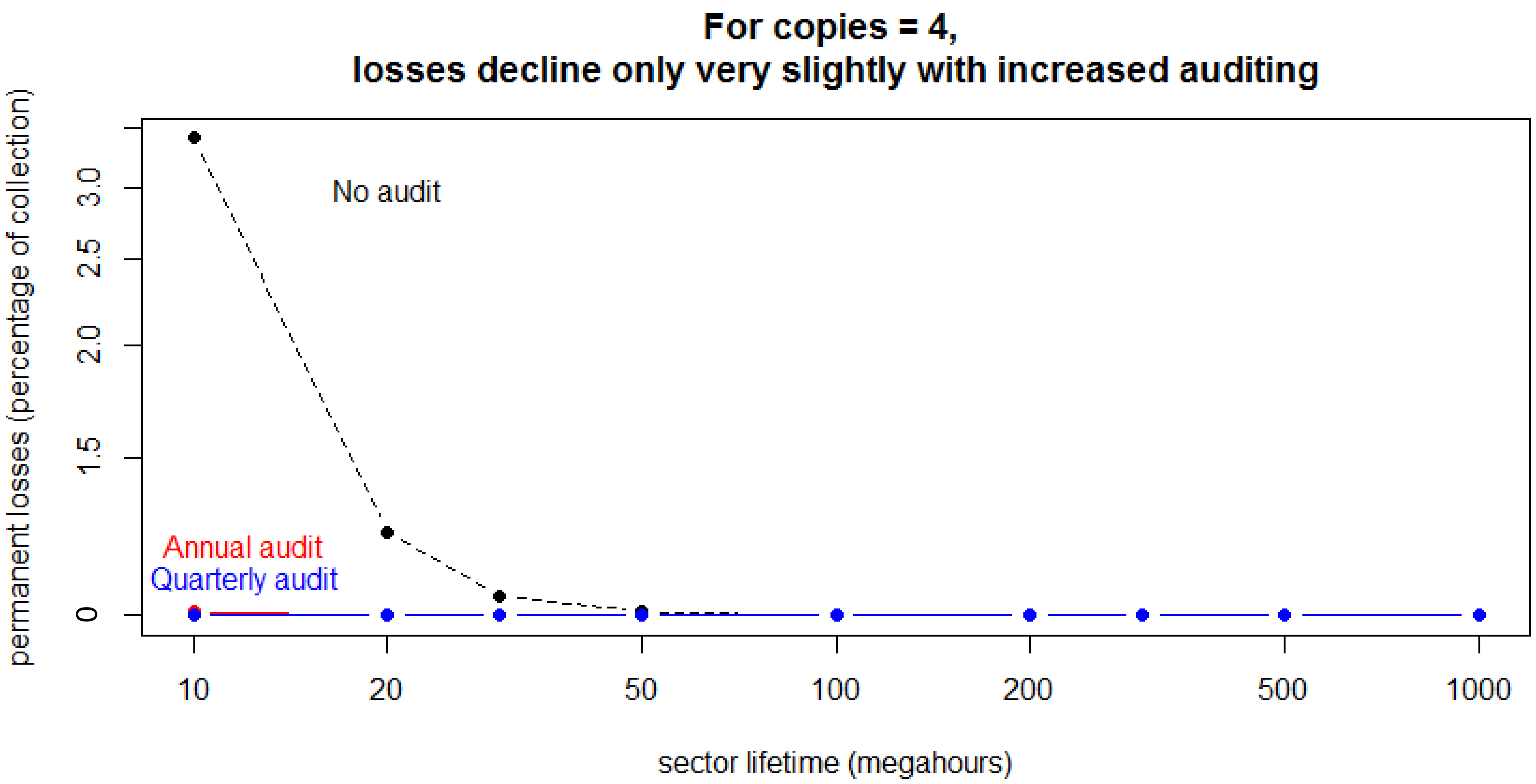
Two Copies? Definitely Not Enough



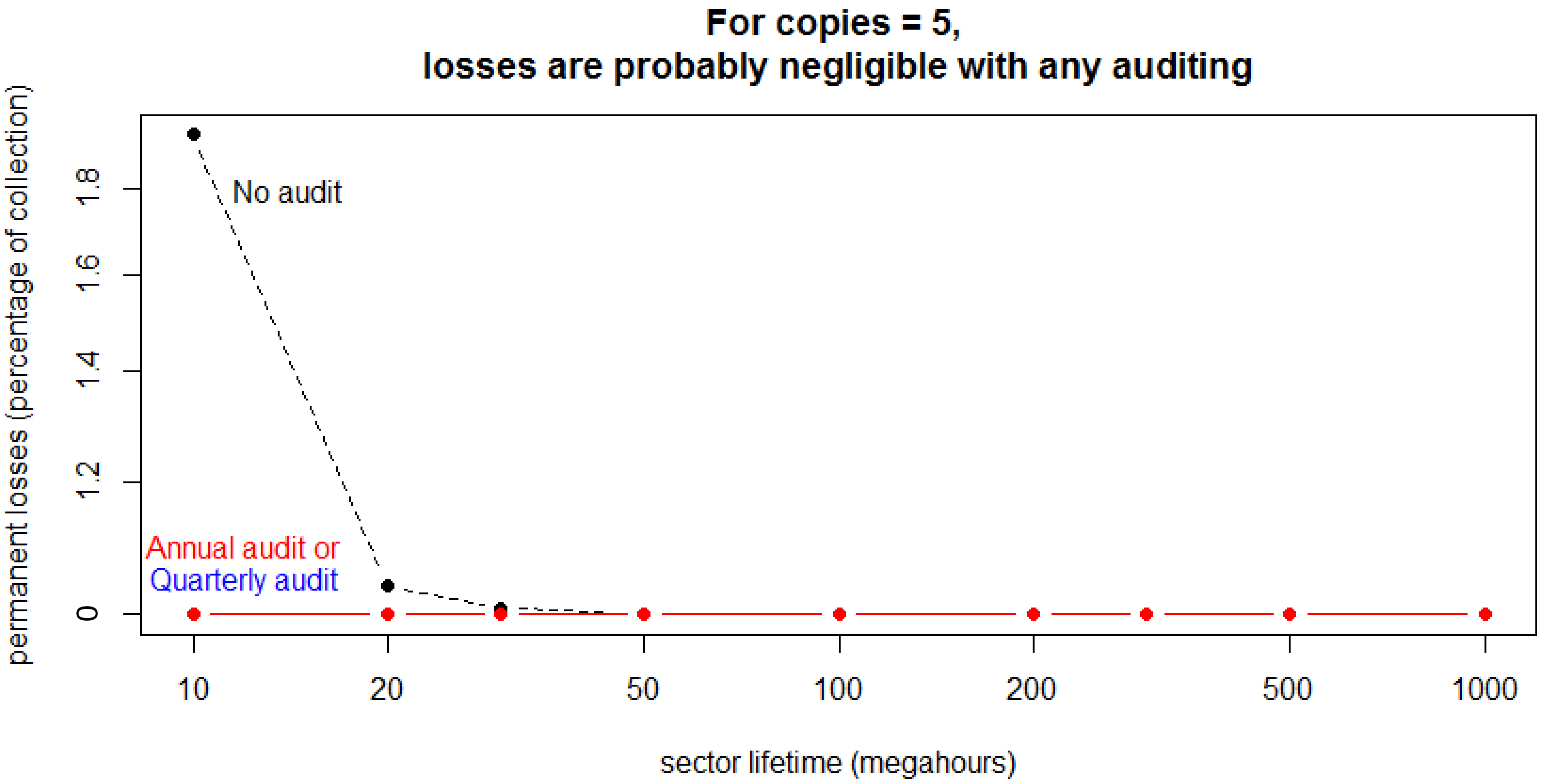
Three Copies? Marginal



Four Copies? Looks Good



Five Copies? Works

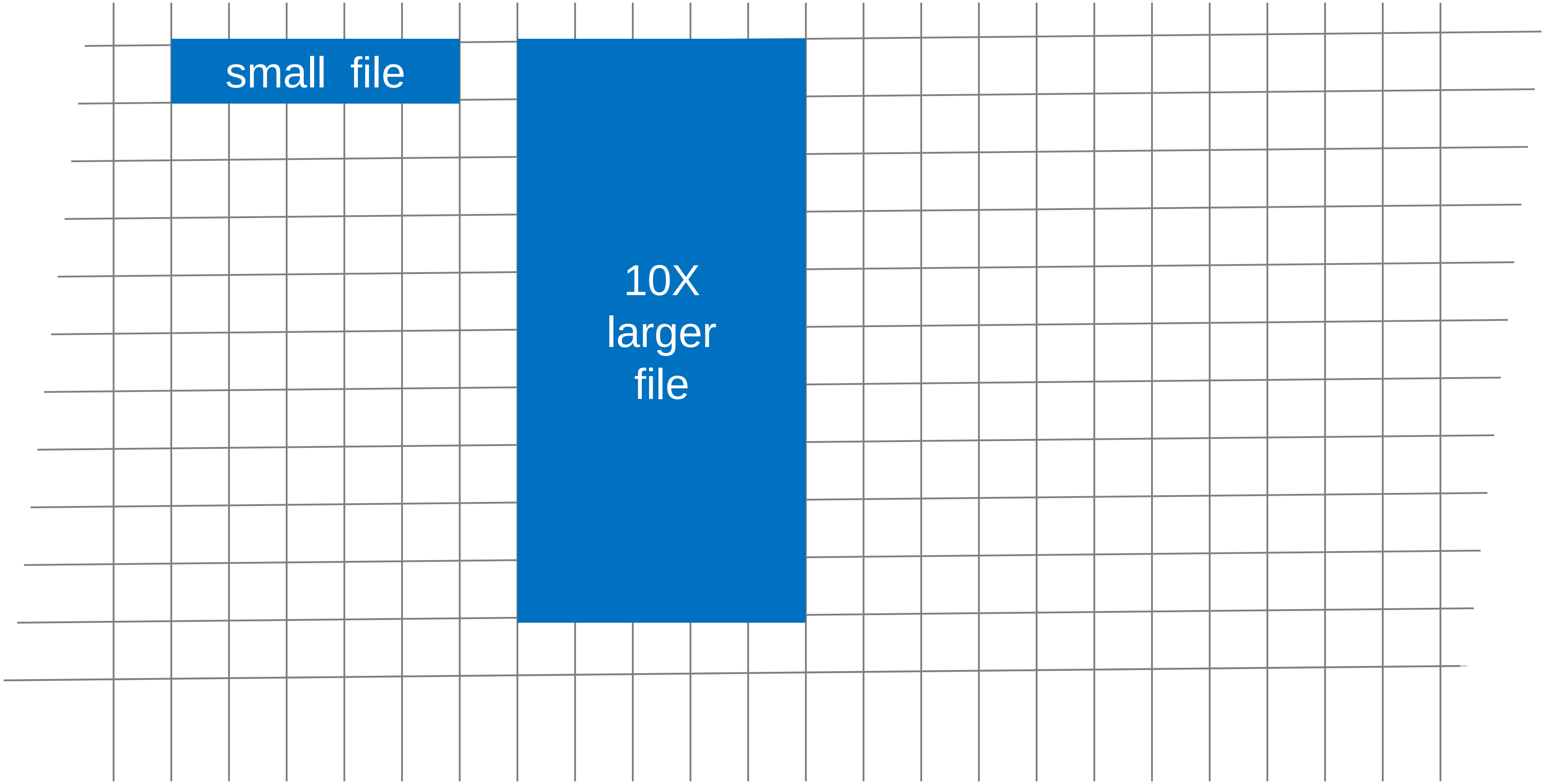


Size Doesn't Matter (for Modeling)

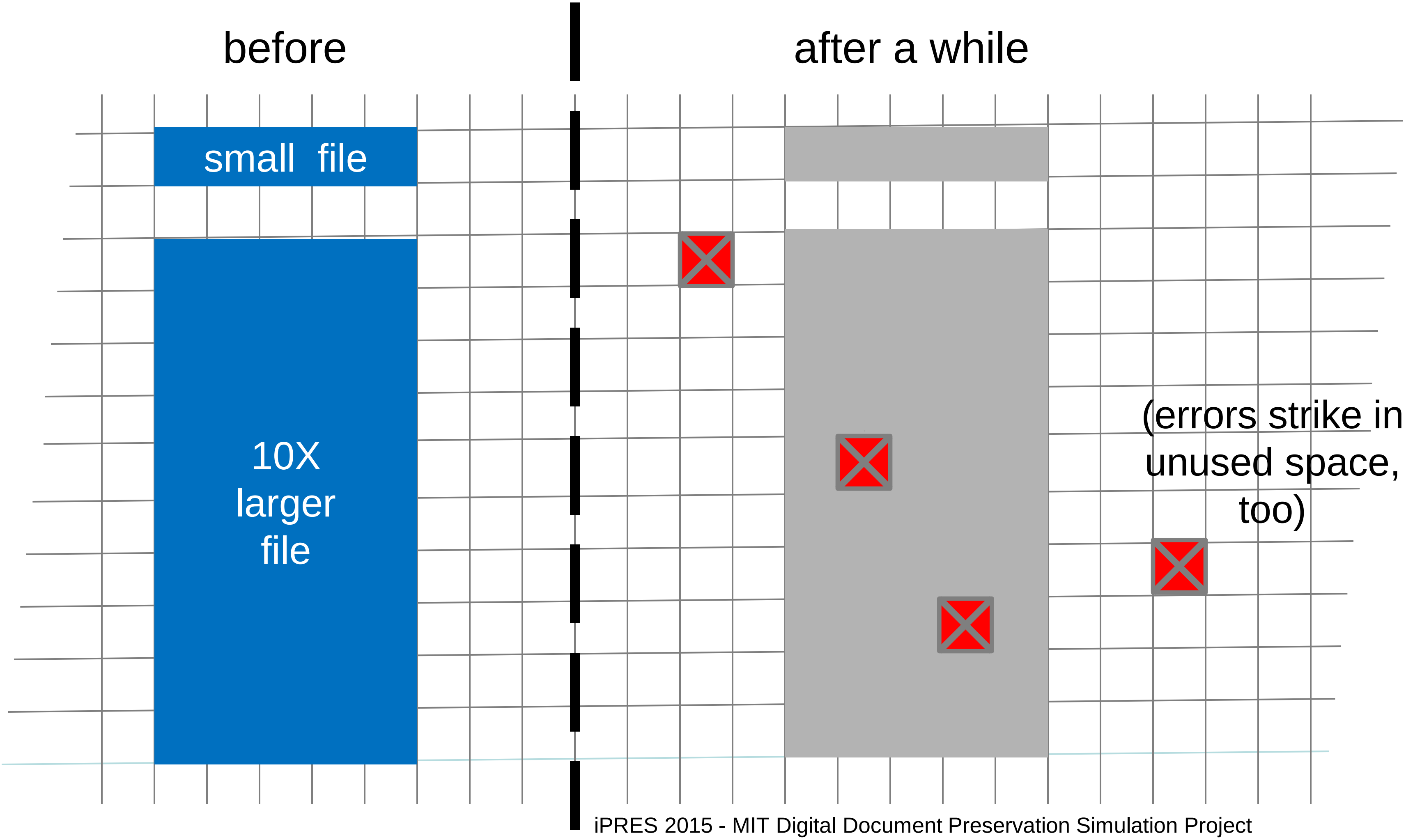
- Document sizes and error rates scale easily
  - Larger doc presents a larger target area
  - For a constant rate of block errors, larger doc will be hit more often
- Scales precisely as you would expect
  - 10x larger doc is hit 10x as often

    OR
  - 10x larger doc + 1/10 block error rate is hit 1x as often
  - (or 10x larger doc with 10x longer block lifetime)

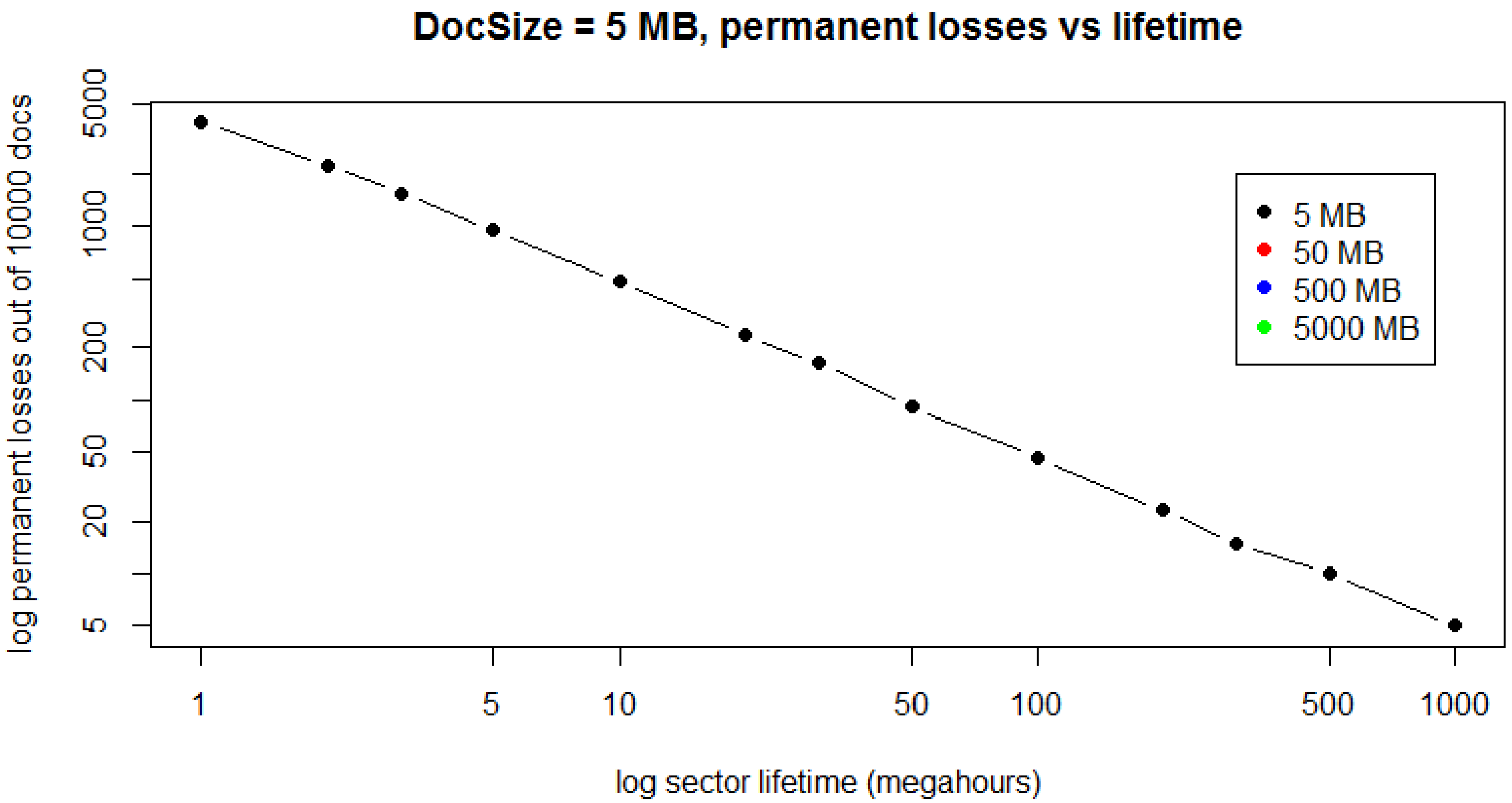
Initial State With Small and Large Files



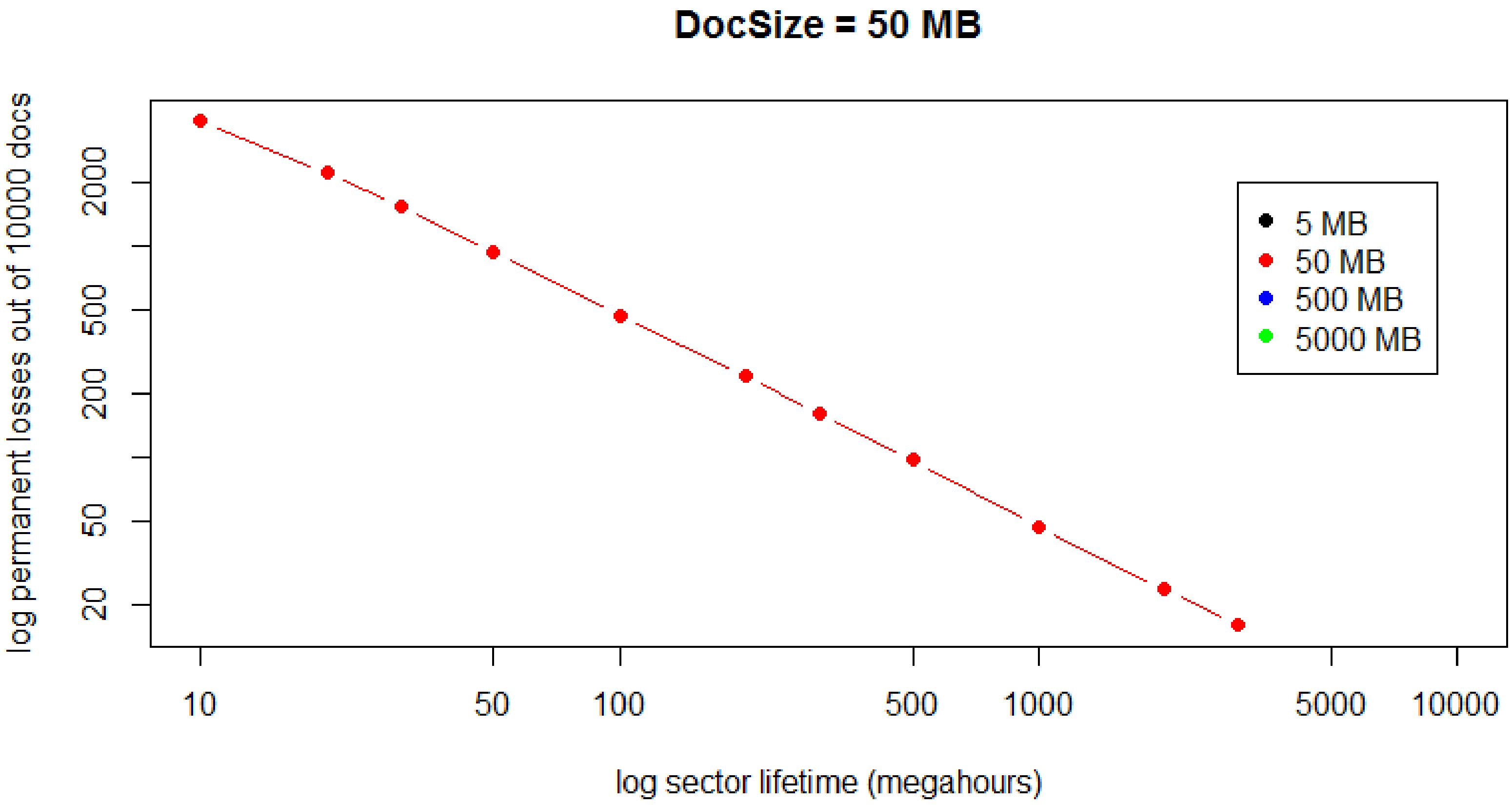
Errors Are More Likely to Strike Larger Targets, Proportionally



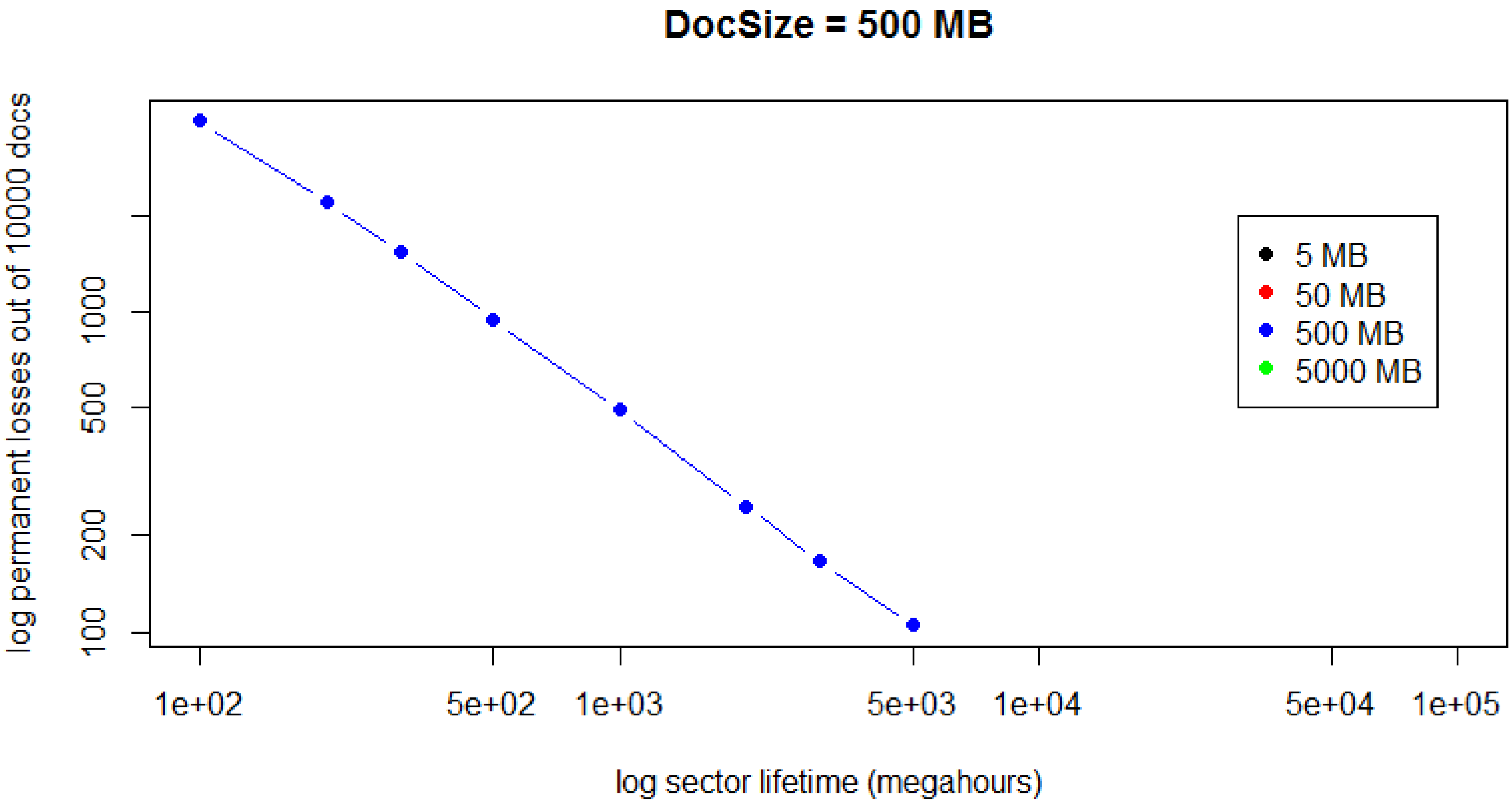
Measured Doc Losses vs Sizes and Lifetimes



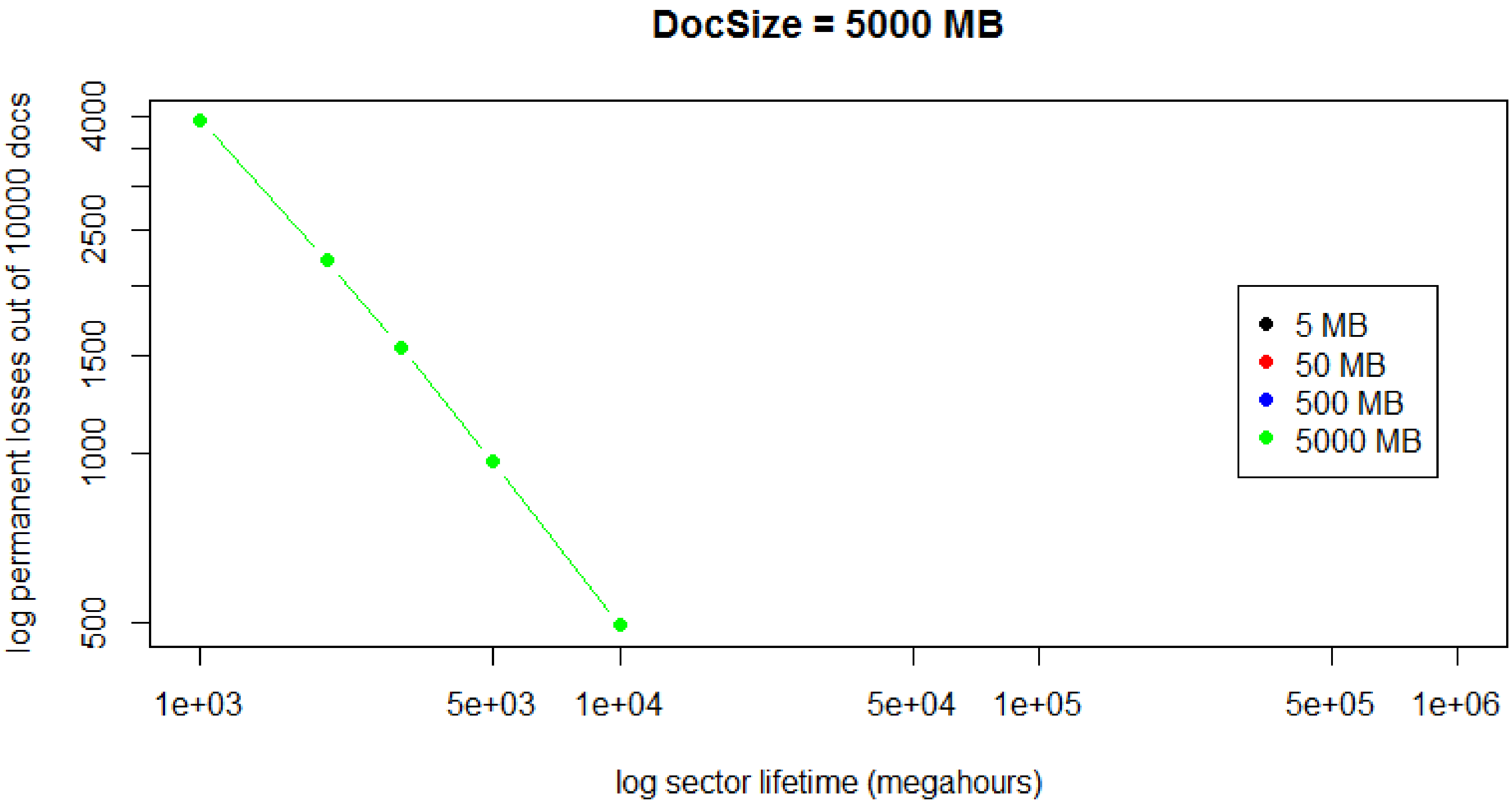
10X Larger Docs (50 MB)



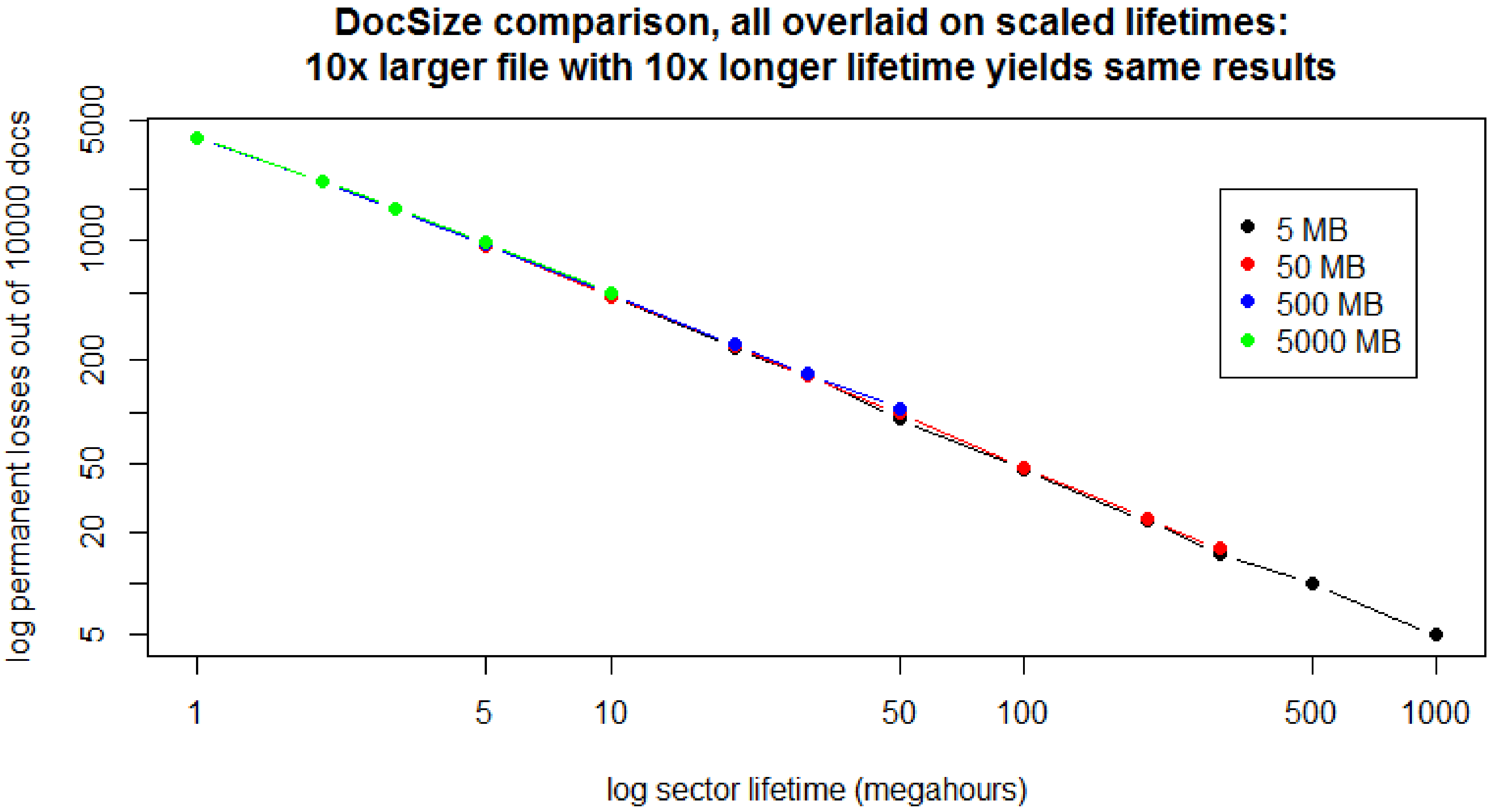
100X Larger (500 MB)



1000X Larger (5000 MB)



Re-scale Lifetimes to Match Various Sizes



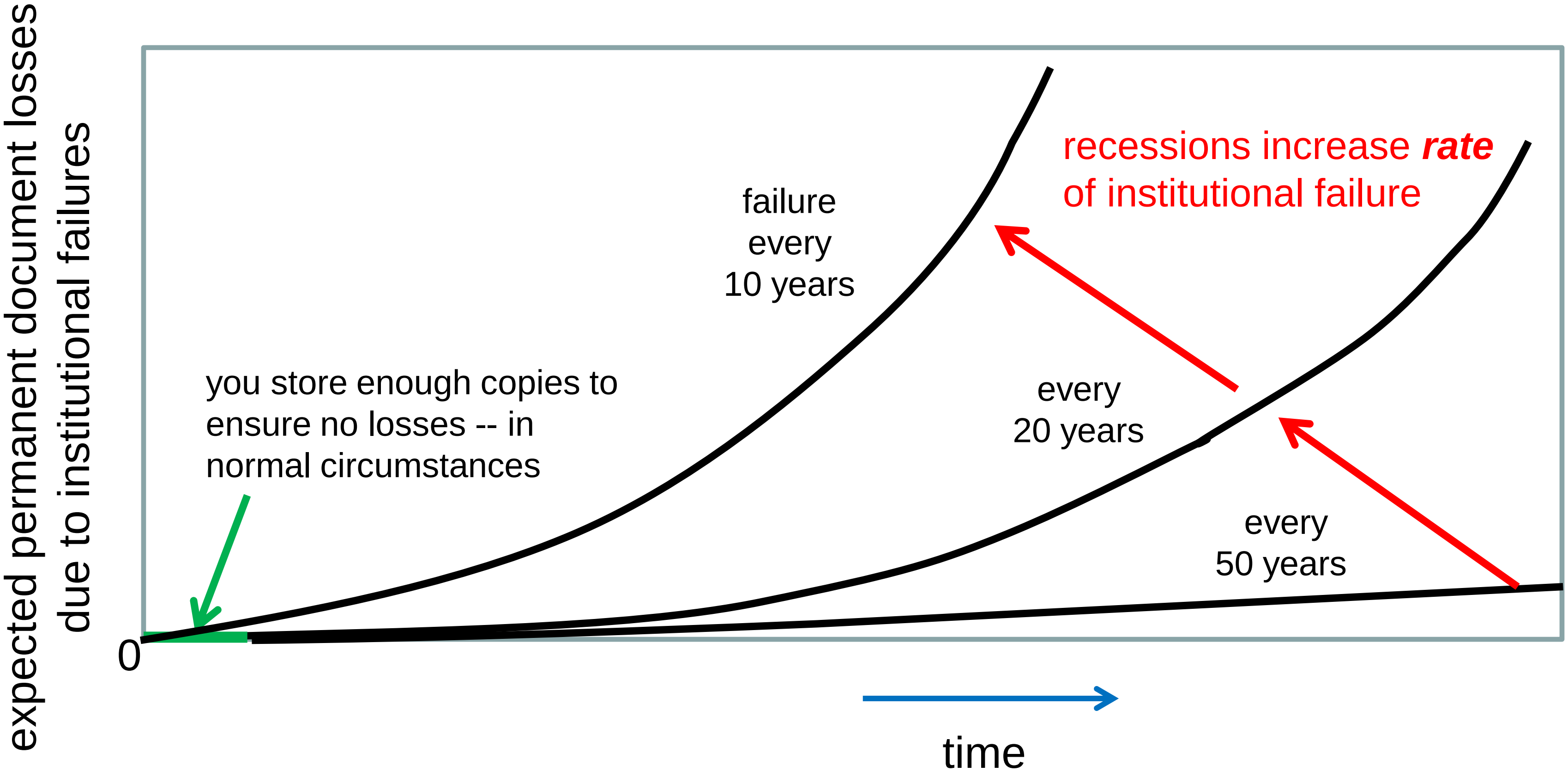
Effect of Compression

- Assume recoverablility rate R and compression rate C
- Show how this is equivalent to changing collection and document size
- Note that if C>R always a win
- Note areas where if C<R still saves sufficient space to store another copy
  - Does this make up for higher failure rate from compression?

Institutional Failures Are Dangerous

- You protect your collection with N copies
- An institution fails, removing one copy entirely
  - Until this is discovered during the next audit cycle, you actually have only N-1 copies
- If a second institution should fail near the same time, then only N-2 copies
- Correlation of institutional failures?
  - Economic downturn
  - Regional conditions
  - Copies kept too close together, e.g, in-house

Recession → Failures → Losses



you store enough copies to ensure no losses -- in normal circumstances

recessions increase ***rate*** of institutional failure

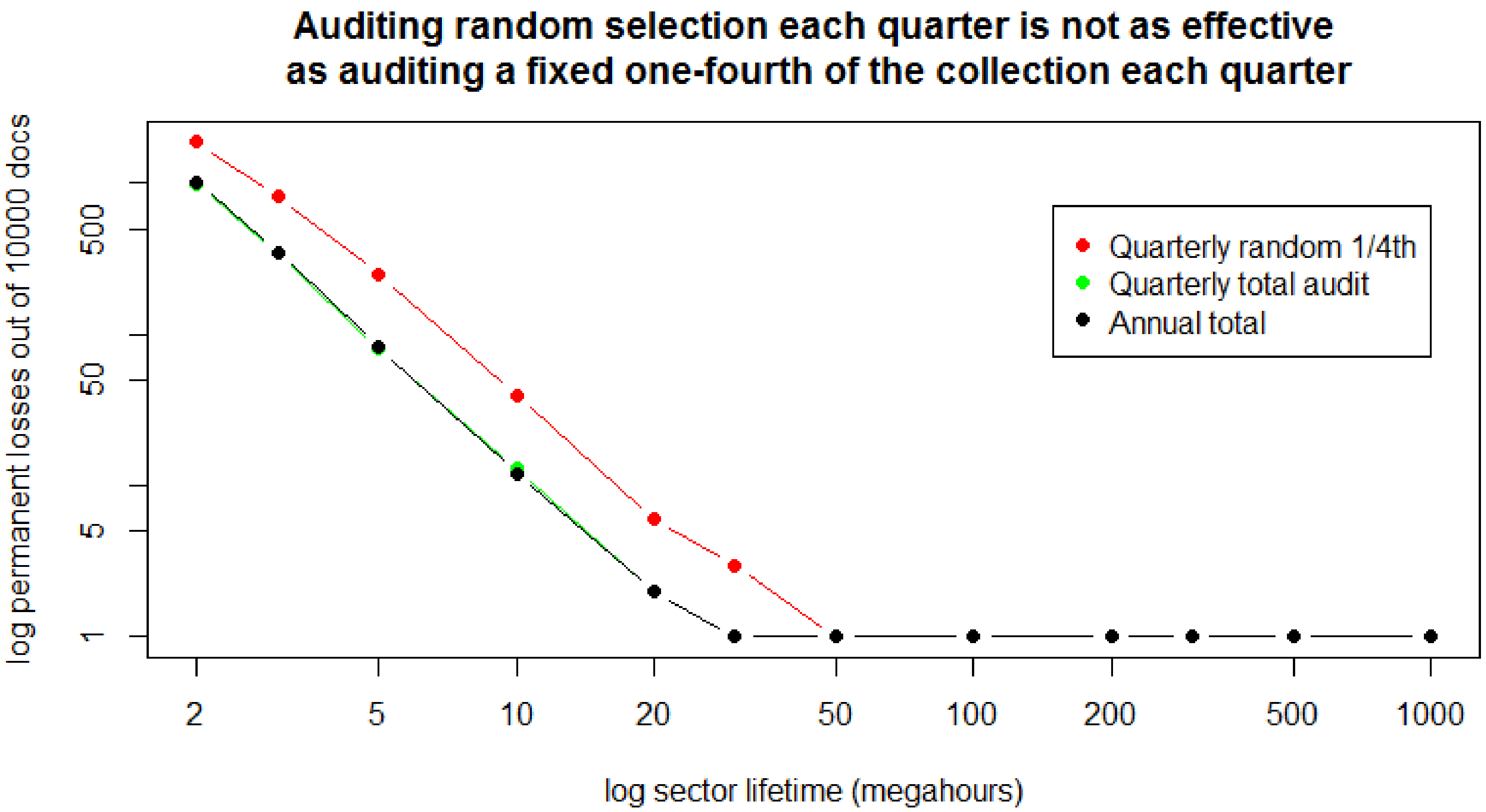
Several Auditing Strategies

- TOTAL: every audit cycle, check every copy of every document
- SEGMENTED: check part of collection at intervals during the audit cycle
    - Entire collection checked every audit cycle (sampled *without replacement)*
- RANDOM SEGMENTED: check randomly selected part of collection at intervals during the audit cycle
    - – Selected *with replacement:* some documents will be missed in the cycle
- POPULARITY: divide collection into pieces, audit some more frequently

Tricky Audits Don't Help

- Total or segmented audit is always better than random audit
  - E.g., auditing randomly selected 1/4 of the collection every quarter
    - Some documents will be missed entirely if the audit set is selected with replacement
  - (Note: segmented is very slightly better than total, because it looks at some failures earlier when failure rates are very high)

Random Selection Leaves Errors



Preliminary Conclusions - 1

- More copies are better (duh!)
- Auditing is *essential* to collection health
  - Protects collection over huge range of "quality"
  - Very frequent auditing is probably overkill
  - Tricky auditing (subsets, random) is less effective

Other: Questions- 2

- Institutional failures are pernicious -- but how often do they occur?
  - The problem: a silent institutional failure reduces the number of redundant copies you have stored
  - Risk is increased until you discover the problem (in auditing) and provision a new server
    - Thought you had four copies? Well, for a period of time, you actually have only three.
    - And another failure before the audit reduces copies to two
    - Failures may be correlated due to economic conditions, wars

Other: Questions - 3

- How many copies do you need to limit losses?
  - Limit permanent losses to some part of the collection?
  - Better: How many to keep likelihood of *any* permanent loss under some percentage?
    - 5 per cent, 1 per cent, 0.1 per cent?
  - For institutional failures, how many copies to keep likelihood of total loss under some percentage?

Audit We Must

- Auditing is expensive (in bandwidth, bytes moved, time)
  - Read back all the contents of all the documents?
  - We should work toward efficient auditing functions

What Next?

- *Q: What information do you need to manage your libraries?*

Backup

Form of the Data

- Fixed number of documents, fixed time
  - Scale to your needs
- Number of copies varies, 1 to 10
- Reliability of storage servers varies
  - Very little real data in this area
- Auditing strategies vary
- Document size varies (but doesn't matter)

Institutional Failures

- (NEED GRAPH)
- Assume baseline # of copies, quality and auditing yields 0 loss in the absence of institutional failure
- Closed form – compare expected loss vs. frequency of business failure events (inverse of business half-life?)
- Recession → pushes failure curve out