Reporting

- The purpose of all the previous work
- Transmogrifies overwhelming amounts of data into clear communication
- Must be literate & readable
- Know (and write to) your audience
- A substantial, real **document** that measures adherence to the security policy
- Afterwards - why was it written?

Know your audience

- Head of organization
- Manager of systems
- Technical thugs

Content of the Audit Report

- Approximately 15-100 pages
- Technical details increase as report goes on
- Title page
- Table of contents
- Executive summary & prioritized recommendations
- The main body
- Final conclusions & detailed recommendations
- Appendices
- Glossary

The Executive Summary

- Perhaps the most difficult part to write
- No more than 1-2 pages
- Understandable to upper management
- State reasons for doing the audit
- Include a brief overview of organization & systems audited

The Executive Summary (cont.)

- Indicates change in security from last audit
- Has measure of site compliance to the policy
- Summarizes significant strengths & weaknesses
- Covers the top recommendations

The body of the Report

- The easy part
- Be complete; educate readers
- Explain/defend all recommendations/claims
- Compare/contrast between previous audit
- Break the problem into smaller pieces
- State what was examined, and why
- Grade or evaluate each piece
- Conclusions and recommendations

Compare/contrast between previous audit

- If the previous audit found problems:
  - Were they fixed?
  - Did the policy change to reflect them?
- Were any new problems found? Why?
- Say if there was no change, or if the policy was changed to allow potential problems to exist

Break the problem into smaller pieces

- Network security
- Host level security
- Polices, procedures, and documentation
- Physical Security
- Security architecture

Break the problem into smaller pieces (cont.)

Each piece, or section, should discuss:

- The scope of the section
- What importance the section has to this site
- How important (relatively) is the section?
- What tools, methods, etc. were used?
- What was discovered?

Grade or evaluate each piece

- Grade individual components if sensical, with an overall score.
- Helps people understand the state of the system
- Use a rating that is easily understood (1-10, a letter grade, etc.)
- Subjective is fine, a **good** quantitative method is better

Final conclusions & detailed recommendations

- Unifies the executive summary & body
- Prioritize and summarize **all** recommendations
- Does the policy require a reasonable level of security?
- Grade or evaluate the total system
- What happened to the audit data?
  - Where was it stored?
  - How was kept secure?
  - How can it be recovered?

Appendices

- Tools used in audit
- Systems or networks examined
- Significant output that couldn't fit in body (cracked passwords, a list of ports to filter, etc.)
- A list of security patches needed
- Raw audit output, if appropriate
- Bibliography of suggested reading (books, papers, URL's, etc.)

What happens after the report?

- Action!
- Responsible personnel should meet to discuss
- Create a list of:
  - Action items
  - Who is responsible for resolution
  - A specific due date for action