

"Preparing a High Impact Consultant's Report"

IAPSC Successful Security Consulting

Session #8

September 23, 2013

Attendee Handout



Common Types of Security Consultant Reports

Security Assessment Report

Prepared at conclusion of security assessment, provides evaluation of existing security conditions, risk analysis, and consultant's findings and recommendations.

Design Concept Report

Explains security design concepts for facility, including concepts for physical security, security systems, and security operations. Usually done in conjunction with new construction or renovation projects.

Architectural Design Phase Report

Prepared when working on an architectural design team, these reports are typically done at the conclusion of each of the traditional architectural design phases: Programming, Schematic Design, Design Development, and Construction Documents phases.

Peer Review Report

Also called Design Review Reports, these are done when the consultant is hired to review the design work done by architects, engineers and other security consultants. Typically done near end of Design Development phase just before construction documents are released.

Forensic Report

Written when consultant is retained as an expert witness, these reports typically summarize the incident and provide the consultant's opinion on foreseeability, breach of duty, and causation.

Many other types of reports are prepared by consultants depending on their area of practice. These can include Security Staffing Review Reports, Policies & Procedures Review Reports, Value Engineering Reports, Security Systems Review Reports, Security Master Plans, Proposal Review Reports, and many others.

Security Assessment Reports

- Security assessment report is most common type of report for most consultants.
- The report is what you use to deliver your findings and recommendations to client after you have been hired to evaluate security conditions at their facility.
- There are as many different styles of reports as there are consultants – you will adopt your own style, and it will probably evolve over time.
- There is no one right or wrong way of doing it.
- Certain assessment methodologies or clients may have specific formatting requirements, but 90% of time, the format is up to the individual consultant.

Anatomy of a Basic Security Assessment Report

Outside Cover

- Client name, logo, facility location, date of report.
- Keep it simple and clean; provide more information on inside cover.
- Consider using version number (V1, V2, V3, etc.) instead of using “Draft Report”, “Final Report”, etc.

Inside Cover

- Project address.
- Consultant's name and contact info.
- Team members who worked on project.
- Certifications (CPP, CSC, etc.) of consultants.
- Cover photo (optional).

Acknowledgments

- Optional, but recommended.
- A list of all people who participated or contributed to project.
- Shows thoroughness of effort; many readers will be surprised at the large number of people you have talked to.
- Gather names from sign-in sheets and/or business cards obtained during interviews.
- Can have powerful influence on CEO's and other decision makers when depth of participation in assessment is known.

Table of Contents

- Use automatic table of contents (TOC) feature in MS Word or other word processing software.
- Provide more detailed, multi-level TOC rather than just a simple list of report chapters. This shows thoroughness of report right from the start, and also allows readers to navigate right to desired topics.

Executive Summary

- Describe the most important things you want the CEO or other decision maker to know.
- 1 or 2 pages maximum.
- Make it meaningful and impactful.
- Hardest part of report to write; suggest that it be done last.
- Don't just cut and paste content from other sections.

Introduction and Scope

- Describe who commissioned the assessment.
- Describe what facilities the assessment included.
- Describe what you did: field surveys, people interviewed, documents examined, research conducted, etc.
- Exclusions: Explain what you didn't do: facilities not included, systems and processes not examined, etc.

Description of Facilities

- Brief description of site and buildings included in assessment.
- Provides background information so that someone not familiar with site can follow the report. (Don't assume everyone reading the report know will already know this information).
- Include a site map or drawing when appropriate.

Description of Existing Security Program

- Brief description of existing security program at facility: provide overview of security management structure, staffing, security personnel, and security systems used.
- Facts about existing conditions only here – not the place to provide opinions or recommendations.
- Background information so that an outsider can follow the report.
- Most CEOs and senior management probably don't know details of existing security program and will find this very helpful.
- Shows in-depth knowledge of client's existing conditions by consultant.

Risk Analysis

- Analysis of client's security risks and threats.
- May include loss history, crime statistics reports, calls for service reports.
- May talk about industry specific and location specific crime trends.
- Summary of high-priority risks and threats.
- May include risk analysis matrix here that summarizes risks by likelihood and consequences.

Consultant's Evaluation and Opinion

- Optional, but recommended for most reports.
- Sometimes also called "conclusions".
- Provides summary of consultant's feelings about adequacy/inadequacy of security program relative to the security risks that the client faces.
- Points out major strengths and weaknesses of existing program in general way.
- Offers general (not specific) strategies for security improvements.

Findings and Recommendations

- This section is where you point out specific problems in detail and recommend solutions.
- This is most important part of report - everything done before this was laying groundwork for this section.
- Findings and recommendations can be presented in separate report sections, or presented together.
- Some consultants use the term "observations" instead of "findings".
- Suggest that each finding/recommendation be numbered.
- Suggest that separate recommendations be made for each distinct area of work. For example, don't say "fix fencing", "improve lighting" and "add surveillance cameras" all in one recommendation - list these each as separate recommendations.
- Include photos if they help to communicate findings, but don't use just as filler.
- Findings and Recommendations can be presented by category:
 - Policies & procedures
 - Physical security
 - Personnel
 - Etc.....
- Or by location or department:
 - Parking Garage
 - Administration Building
 - Warehouse
 - Etc.....

Appendices

- Place things here that the reader may need to reference, but which would interrupt the flow of the report if placed in the main content.
- Also called "Attachments".
- Examples of items in this section may include: lighting surveys, crime data, loss history, personnel data, cost estimates, glossaries, and product data sheets.

Summary of Recommendations

- Table that has one-line summary of each recommendation listed by recommendation number.
- Very helpful for client to have short-list of action items.
- Many clients combine this with executive summary to provide essence of report in just a few pages.
- Can use to prioritize recommendations.
- Can use to provide estimates of initial and ongoing costs.

Report Writing Tips

Understand Importance of the Report

- The report is often the only tangible work product delivered by the consultant.
- Report may read five, ten, or twenty years after you write it.
- The report serves as a lasting reminder of your knowledge, skills, and quality of work.
- Many clients equate full cost of consulting assignment with report = “This report cost \$35,000”.
- Report can be widely distributed and read by people you may never imagine.
- Report can become a legal document; discoverable by attorneys and scrutinized in a courtroom setting many years later.

Consider Who Will be Reading the Report

- In addition to the person who hired you, your report may be read by:
 - Top-level executives who are totally unfamiliar with facility, existing security program, or problems being encountered.
 - Boards of Directors.
 - Outside regulatory agencies.
 - Insurance companies.
 - Community groups.
 - Elected officials.
 - Lawyers, judges and jury if used in litigation.

Write Report Specifically for This Client and This Project

- Develop specific outline of what you want to say for this specific project.
- OK to use templates to prompt your thoughts, but not to dictate how report will be written.
- Minimize your use of boilerplate and filler material.
- Don't start with previous report and try to edit it to fit this project.
- Don't let your "inventory" of prewritten materials effect what you decide to write.
- If you look at three of your recent reports and 90% of the content is the same in each, you are probably doing something wrong.

Start Writing Early

- Because many consultants find report writing to be unpleasant, they until the last minute to start writing.
- Waiting until the night before the deadline to start writing the report puts you under increased pressure and causes you to make more mistakes.
- Start writing while critical details from your field surveys and interviews are still fresh in your mind.
- When you begin to write the report, you will probably uncover areas where additional facts are needed. Give yourself ample time to do additional field work or conduct research if necessary.
- Allow time for the report to be reviewed and edited before it is sent to the client.

Write Simply and Clearly

- Write as you would talk (conversational tone).
- Use short sentences.
- Don't use big words when a small word would do. The goal is to communicate – not impress with your vocabulary.
- Make every word count. Always be on the lookout for words, paragraphs or even entire sections that can be removed from the report without diluting the main message. When in doubt, leave it out.
- If what your writing about doesn't seem into the flow of your text, you are probably trying to put it in the wrong place.
- If you are having trouble writing, sometimes it is because you are not really sure what you want to say. Stop, outline your thoughts, decide what you are going to say, then write.
- Make report only as long as it needs to be – stop writing when you have finished what you have to say. Quantity doesn't equal quality. A well-written 25 page report is better than a 250 page report that is loaded with redundant information and filler.

(For some good tips on effective writing, visit: <http://webaim.org/techniques/writing/>)

Define Unfamiliar Terms and Concepts

- Minimize the use of abbreviations, acronyms and jargon – use plain language when possible.
- Don't assume prior knowledge on the part of the reader – always define unknown terms, acronyms and abbreviations.
- Definitions are not insulting to the reader even though he or she may already know the term.
- If it can be done simply, define the term within the body of the text.
- Use footnotes for more lengthy definitions.
- Use appendixes or URL links to provide background or to introduce larger concepts.

Use Terms Consistently

- Inconsistent use of terms is a bad habit in the security industry and is confusing to the reader.
- Pick the term that you think is best and use consistently throughout report.
- Make sure everyone on your team is using the same term.
- Provide a footnote that references other terms that may be used.

Examples of different words used to describe the same thing in one report:

Security Room
Security Monitoring Center
Security Control Room
Security Office
Security Dispatch

Use Facts to make Direct, Powerful Statements

- Use direct fact-filled statements whenever possible.
- Avoid “wishy-washy”, ambiguous statements.
- Use actual numbers and exact facts when possible.
- Cite reference documents, sources, external standards and best practices when possible.
- Use benchmarking standards with other similar facilities – top executives love this, particularly when facilities being benchmarked against are well-known or are trend setters in their industry.

- Many times we write wishy-washy because we have failed to take the time to get the facts – if facts are available, get them and use them.
- OK to say that you don't know, but say this clearly and explain why information was unobtainable. (Being too lazy to get all the facts is not a good excuse.....)

Examples of statements used to describe history of thefts at a company:

Weak Statement

“The theft of laptop computers has increased quite a bit in recent years.”

Powerful Statement

Examples of statements used to benchmark security measures used at comparable facilities:

Weak Statement

“Most of the other buildings in downtown Portland have security in the lobby.”

Powerful Statement

Use Photos and Charts to Enhance Your Report

- A picture is worth a 1000 words, but pictures are commonly overused in many consultant's reports.
- Every photo and chart should have a specific purpose and add real value to report; such as to document specific vulnerabilities.
- Avoid using general photos to introduce every topic (“here's a guard, here's a camera”, etc.)
- Don't use photos as a filler or as a crutch for poor writing.

- Most reports now distributed electronically – consider file size of report and ability to be viewed on mobile devices. 2 megabyte (MB) maximum file size for entire report is suggested.
- Reduce photos to be as small as possible while at the same time remaining clear enough to communicate the desired message.
- Use text and leader lines to point out things you want the reader to see in the photo - don't assume that they will see what you see.

Have Your Report Reviewed By your Editorial Team Before Sending to Client

- Every report needs to be reviewed by someone else before sending it to the client - no exceptions!
- Its best to have two or more reviewers.
- If you work for a larger firm, have your report reviewed by one or more of your co-workers.
- If you are a sole practitioner, consider having have your spouse, adult child, or a trusted friend review your work.
- If a member of IAPSC, consider making arrangement with fellow member to act as your reviewer and vice versa.

Avoid Common Beginner's Mistakes

- Don't forget to point out the things that the client is doing right as well as the things that he is doing wrong. Many consultant's focus exclusively on the deficiencies in the client's security program and fail to acknowledge the many things he is doing right.
- Bad facts (getting someone's name or title wrong) or bad math (column of numbers that doesn't add up) can instantly destroy your credibility. If you get the simple things wrong, how can they trust you with the important things?

- Don't confuse opinions with facts. There is a place for both, make it clear when you are expressing your opinion as opposed to stating facts.
- Keep sarcasm and attempts at humor out of the report. These can make you look unprofessional and sometimes backfire. Keep the tone of the report businesslike and professional.
- Don't overstate or exaggerate conditions in either a positive or negative way. State the facts clearly and let them speak for themselves.
- Don't make statements that may appear to be personal attacks against specific people or organizations. When you need to be critical of someone, try to criticize the behavior, not the person. State the facts in such a way that would allow the reader to draw a similar conclusion to your own.
- Don't go crazy with colors, fonts and formatting within your report. Suggest no more than two colors and four fonts in any one report. Keep it clean, crisp and simple.
- Be careful when quoting estimated costs in your report. No matter how much you qualify them, numbers tend to linger in the client's mind forever. Better to leave them out than guess.
- When cutting and pasting content from other reports (something that you should rarely do anyway), be sure that it doesn't still have previous client's name or other information on it.
- Be careful when directly copying content written by others (text from reference books, magazine articles, etc.) into your report. Do this sparingly, obtain prior permission from the author if necessary and be sure to credit the source.
- Don't make sales pitches for additional consulting services within your recommendations or other main sections of the report. (It's OK to insert one or two paragraphs at the end of the report offering to help with implementation of recommendations or provide other services.)

If you have additional questions about security report writing, feel free to contact the presenter directly:

Michael A. Silva, Silva Consultants
 PO Box 8799, Covington, Washington 98042
 Phone: 888-645-2299 Email: mikes@silvaconsultants.com