Example Proposal

for an

Information Security Health Check
Objective

- Appropriate information security controls and processes within {client} to safeguard business critical information with minimum impact on normal business.

Scope

- To carry out an information security health check (gap analysis) for {client} in {location} against BS ISO/IEC 17799 and information security management good practice
- To produce an action plan to enable {client} to secure business critical information with the minimum impact on normal business operation and optionally to achieve BS ISO/IEC 17799 certification
- To advise {client} on logical and physical controls to implement the recommendations from the health check

Quotation: Information Security Health Check (gap analysis)

- Site visits to {location} in order to:
  - interview IT staff to assess the extent of existing procedural compliance with BS ISO/IEC 17799 in IT areas
  - interview IT staff to assess the extent of existing technical counter-measures to BS ISO/IEC 17799 standards and examine those measures
  - interview selected representatives of business units to assess the extent of existing procedural compliance with BS ISO/IEC 17799 in non-IT areas
  - gain an understanding of the firm's culture and business, to establish any special needs with respect to BS ISO/IEC 17799

- Author a report on the findings of above, showing compliance and non-compliance in all BS ISO/IEC 17799 areas, together with recommendations for:
  - responsibilities
  - reporting mechanisms
  - awareness education
  - procedural changes
  - contractual changes
  - and technical changes, to apply BS ISO/IEC 17799 throughout the business

- Present our report to {client} and agree an action plan, with timescales, to implement the recommendations in the report

*All travel expenses within the UK have been included below. Figures quoted assume visits only to the locations specified. Additional fees will be payable for visits to sites other than those shown.*

Example fixed fee (single UK site) ................................................................. £ 5,700
Example fixed fee (two UK sites) ................................................................. £ 7,500
Example health check programme

The following steps are typical of those carried out during our BS ISO/IEC 17799 Health Check review. The focus and bias of each review will vary, dependant on staff attitude, the technology involved and vulnerabilities exposed during the process.

1. Pre-visit Actions
   1.1. Confirm staff to be interviewed
   1.2. Confirm staff roles
   1.3. Agree timetable of interviews
   1.4. Confirm IT systems and applications in use
   1.5. Obtain any relevant existing IT and personnel documentation
   1.6. Obtain any existing security policy
   1.7. Obtain any recent audit reports

2. Day one (on client site)
   2.1. Meet to confirm structure of review
   2.2. Interview staff as per timetable
   2.3. Inspect general physical environment
   2.4. Observe and review staff behaviour
   2.5. Inspect physical IT installation

3. Day two (on client site)
   3.1. Continue to interview staff as per timetable
   3.2. Inspect general physical environment
   3.3. Observe and review staff behaviour
   3.4. Any mop up interviews from day one

4. Day three (at First Base)
   4.1. Conduct gap analysis
   4.2. Analyse interviews for additional vulnerabilities
   4.3. Analyse observations for vulnerabilities

5. Day four (at First Base)
   5.1. Compose report and recommendations

6. Day five (on site/at First Base)
   6.1. Present report and agree action plan
   6.2. Agree review timetable
Contract Terms & Conditions

1. These terms and conditions are in addition to our standard terms and conditions of sale and are to the exclusion of all other terms and conditions including any which the client may purport to apply in any manner.

2. The prices quoted for services or products are exclusive of VAT which shall be due at the rate ruling on the date of the VAT invoice.

3. This quotation supercedes all previous quotations, either written or verbal.

4. Prices quoted for services are valid for 30 days from the date shown.

5. Prices quoted for products are valid for 7 days from the date shown.

6. First Base may by giving notice to the Buyer at any time before delivery increase the price of products to reflect any increase in the cost to First Base which is due to factors occurring after the date of this quotation provided that the client may cancel this contract within three days of any such notice from First Base.

7. Fixed maximum price quotations are based upon the terms of reference agreed between the client and First Base. Additional fees will be charged on a per diem basis should any terms of reference be changed by the client either verbally or in writing at any stage in the project.

8. Travelling, hotel and living expenses will be passed on at cost.

9. Mileage will be charged at 65p per mile.

10. Travelling time, for journeys of more than two hours, may be charged at 50% of the prevailing consultancy fee, pro rata.

11. Invoices for services other than training will be raised on a weekly basis and payable within 14 days of invoice date.

12. Training services are due for payment in full 14 days prior to training.

13. Any hardware or software acquired on behalf of the client must be paid for in full with the order. Any increase in price for products as per condition 6 above shall be paid in full within seven days of the invoice date.

14. Orders must be confirmed in writing and signed by a duly authorised person, with an official order number when used, before any work can commence.

15. Clients cancelling orders for products or consultancy services within 21 days of the first agreed delivery date will be invoiced 75% of the total order value.

16. Clients cancelling orders for training services within 21 days of the first agreed delivery date will be invoiced 100% of the total order value.

17. Postponement or alteration of booked consultancy or training days may be treated as a cancellation by First Base.

18. Course delegate substitutions are permissible, providing that substitutes have sufficient technical knowledge to meet the course pre-requisites.