Appendix A: Sample Security Risk Profile

Resource Name: _____
Business Owner: _____
Information Security Team Contact: _____

A. GENERAL INFORMATION

1. Please select which groups of individuals have access to your information resource:

- ☐ Employees
- ☐ External Clients
- ☐ Partners
- ☐ Outsourcers
- ☐ Regulators
- ☐ Government Agencies
- ☐ Vendors
- ☐ Other

2. Has a penetration test been performed on the application?

- ☐ Yes
- ☐ No

2.1 Please enter the date of the most recent penetration test: _____
2.2 Who performed the most recent penetration test? _____
2.3 Please briefly describe any outstanding security issues: _____

_____

_____

B. INFORMATION SENSITIVITY

3. Please specify the client data used or collected (select all that apply):

Client Data	Contains Data Value (YES/NO)
Financial institution account information	
Credit card information	

Continued...

(*Continued*)

Client Data	Contains Data Value (YES/NO)
International identifying number (for example, Social Security)	
Home address	
Home or cell phone	
Medical information	
Birth date	
Personal private information (for example, mother's first/ middle/maiden name, city of birth, first school, and so on)	
Cultural information (racial or ethnic origin, political opinion, religion, trade union membership, sexual preference, criminal record)	

4. Please specify the employee data used or collected: (select all that apply)

Employee Data	Contains Data Value (YES/NO)
Birth date	
Credit card information	
Cultural information (racial or ethnic origin, political opinion, religion, trade union membership, sexual preference, criminal record)	
Dependents or beneficiaries	
Financial institution deposit information	
Hire date	
Home address	
Home or cell phone	
International identifying number (for example, Social Security)	
Marital status	
Medical information	
Performance reviews/evaluations	
Personal private information (for example, mother's first/middle/maiden name, city of birth, first school, and so on)	
Salary/compensation information	

5. Please specify the type of corporate (internal business information) data used or collected (select all that apply):

Corporate Data	Contains Data Value (YES/NO)
Client lists	
Financial forecasts	
Legal documents/contracts	
Merger or acquisition plans	
Strategic plans	

6. Please specify the type of third-party data used or collected (select all that apply):

Third-Party Data	Contains Data Value (YES/NO)
Intellectual property	
Licensed software in internally developed applications	
Subject to Non-Disclosure Agreement (NDA)	

7. Does the information resource use or process any other confidential or restricted data?

☐ Yes, please specify: _____

☐ No

8. Does the information resource administer use or grant access to sensitive data (or privileges) on other systems?

☐ Yes

☐ No

8.1 Please describe how this application administers access to sensitive data on other systems or grants access to sensitive data:

_____

_____

9. Does the information resource process any financial transactions?

☐ Yes

☐ No

9.1 If information resource initiates or accepts financial transaction (noncustomer transactions – internal to the organization only), please specify approximately how much money is processed:

☐ < $10,000

☐ $10,000 to $49,999

☐ $50,000 to $499,999

☐ $500,000 to $1,000,000

☐ > $1,000,000

10. Could mishandled information damage the organization by resulting in faulty business transactions, loss of money, or jail time?

- ☐ Yes
- ☐ No

10.1 If information was compromised by an unauthorized outside party, select the resulting level of potential damage:

- ☐ Criminal Prosecution
- ☐ < $500,000
- ☐ $500,000 to $999,999
- ☐ $1,000,000 to $4,999,999
- ☐ $5,000,000 to $9,999,999
- ☐ > $10,000,000

C REGULATORY REQUIREMENTS

11. Is the information resource subject to any regulatory requirements?

- ☐ Yes
- ☐ No

11.1 Please select the *regulatory requirements* that are applicable (select all that apply):

- ☐ Federal Financial Institutions Examination Council (FFIEC)
- ☐ Gramm-Leach-Bliley Act (GLBA)
- ☐ Health Insurance Portability and Accountability Act (HIPAA)
- ☐ Office of Foreign Asset Control (OFAC)
- ☐ Subject to regulation in multiple jurisdictions (that is, European Union, BAFIN, Asia Pacific)
- ☐ Other, please specify: _____

11.2 Please briefly describe which aspects of the regulation apply to the information resource:

_____

_____

12. Are there any other *requirements* (for example, contractual) that mandate information security controls for confidentiality, integrity, availability, or accountability?

- ☐ Yes
- ☐ No

12.1 Please provide any detail on other requirements that may be applicable for the information resource:

_____

_____

D. BUSINESS REQUIREMENTS

13. Please rate the overall confidentiality needs (the consequence of unauthorized disclosure or compromise of data stored, processed, or transmitted by the resource) of the information resource:
- ☐ High
- ☐ Moderate
- ☐ Low

14. Please rate the overall integrity needs (basically the consequences of corruption or unauthorized modification/destruction of data stored, processed, or transmitted by the resource) of the information resource:
- ☐ High
- ☐ Moderate
- ☐ Low

15. Please rate the overall availability needs (basically the consequences of loss or disruption of access to data the resource stores, processes, or transmits) of the information resource to non-Company users:
- ☐ High
- ☐ Moderate
- ☐ Low
- ☐ N/A

16. Please rate the overall availability needs (basically the consequences of loss or disruption of access to data the resource stores, processes, or transmits) of the information resource to Company users (excluding access to support the application or system itself):
- ☐ High
- ☐ Moderate
- ☐ Low
- ☐ N/A

17. Please rate the overall accountability needs (basically the consequences of the inability or compromised ability to hold users accountable for their actions in the resource) of the information resource to its general users:
- ☐ High
- ☐ Moderate
- ☐ Low

18. Please rate the overall accountability needs (basically the consequences of the inability or compromised ability to hold users accountable for their actions in the resource) of the information resource to its support or administrative users:
- ☐ High
- ☐ Moderate
- ☐ Low

19. Please rate the overall reputational damage to the organization if it was known to the user community or industry that the information resource has been breached or defaced in some manner:

- ☐ High
- ☐ Moderate
- ☐ Low

E. DEFINITIONS

Use the following definitions for Low, Moderate, and High ratings in this questionnaire:

Rating	Definition
Low	A compromise would be limited and generally acceptable for the organization, resulting in minimal monetary, productivity, or reputational losses There would be only minimal impact on normal operations and/or business activity
Moderate	A compromise would be marginally acceptable for the organization, resulting in certain monetary, productivity, or reputational losses Normal operations and/or business activity would be noticeably impaired, including the potential for breaches of contractual obligations
High	A compromise would be unacceptable for the organization, resulting in significant monetary, productivity, or reputational losses The ability to continue normal operations and/or business activity would be greatly impaired, potentially resulting in noncompliance with legal or regulatory requirements and/or loss of public confidence in the organization