CYBERISK PROFILE REPORT

TYPE
PLATINUM

Company Information

Company Name	**ABC Company**
Address	88888 Ontario Street
City	Toronto , Ontario l4l 8f8
Phone Number	222 444 5555
Industry Classification	Education

Security Contact

Name	Mr. X
Email	X@gmail.com
Phone Number	99999999999

Management Contact

Name	MRS.Y
Email	Y@gmail.com
Phone Number	44444444444

Date of Analysis

August 03, 2018

CYBERISK PROFILE

The first step of any Cyber Security Implementation Program (CSIP) is identifying and classifying applications, databases, systems, and information. Part of this process is to determine the overall Cyber Risk Appetite. Risk appetite is the level of tolerance that an organization has for risk. One aspect of the definition is understanding how much risk an organization is willing to tolerate, and the other is thinking about how much an organization is willing to invest or spend to manage the risk. Risk appetite sets the boundaries for prioritizing which risks need to be treated. Calculating cyber risk through ongoing assessment using defined and proven methodologies and both quantitative metrics and qualitative risk elements is critical to an organization determining how much risk they are willing to accept to achieve specific business goals or objectives. Further, determining cyber risk appetite cannot be a point-in-time exercise. It must become an ongoing process involving constant evaluation and re-evaluation. Cyber risk appetite ties together operational risk, cyber risk, and enterprise risk in cross functional conversations.

A practical classification direction (in descending order of importance) is:

1. Mission and Business Critical Systems

In aggregate, these are the vital organs of the business where the most sensitive information resides, including intellectual property, information about physical assets, and systems required to run the business. This includes information that can also impact life or death.

2. Core infrastructure, extended ecosystem

Common examples include supply chain management (SCM) applications and partner portals.

3. External, public-facing systems and points of interaction

Common examples include web servers and systems with IP addresses accessible through the internet.

IDENTIFY **PROTECT** **DETECT** **RESPOND** **RECOVER**

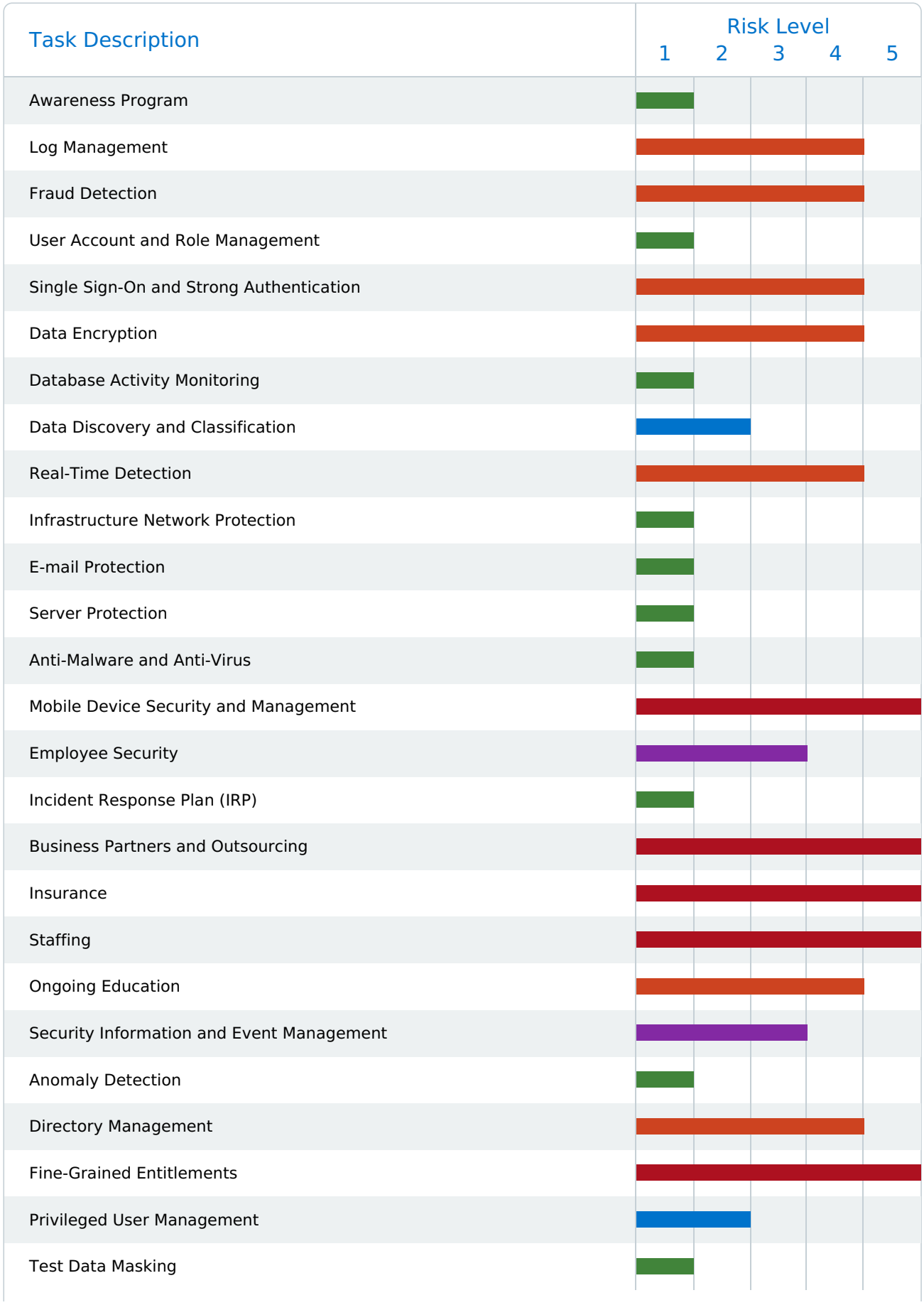
Cyberisk Chek is your first step in identifying key areas of concern and developing an action plan to protect your interests.

CYBERISK OVERALL IMPRESSION

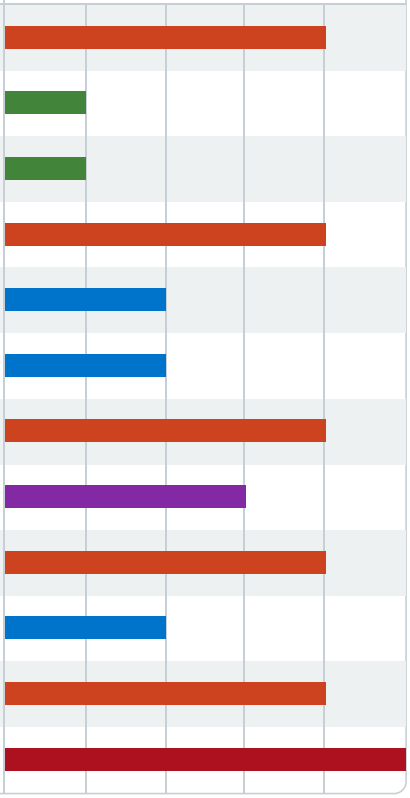
Task Description	Risk Level 1 2 3 4 5
Overall risk tolerance	
Your organization’s current exposure to cyber risk	
Your level of preparedness to overcome a breach or claim	
Adequate processes in place to prevent, detect, contain, and respond to a cyber attack	
Plan is in place for how you will respond to a cyber attack	
Has the plan been fully tested so there is no delayed response	
Overall Impression Average Risk Value	
Detailed Summary Average Risk Value	
Combined Total Risk Profile Value	Moderate Risk
Cyber Risk Preparedness %age™	66%

cyberisk chek™

DETAILED SUMMARY



Task Description	Risk Level 1 2 3 4 5
Data Loss Prevention (DLP)	
Key Lifecycle Management	
Application Dynamic Vulnerability Analysis and Testing	
Static Source Code Analysis	
SOA Message Protection	
Patch Management	
Endpoint Management	
Virtualization Protection	
Outsourcing and Managed Security Services	
Managed Security Services (Cloud Security Services)	
Threat Intelligence	
Security Budget	



ACTION PLAN

Priority One

The following criteria were compiled based upon the information provided. All items noted were allocated into the **extreme risk of security** controls being compromised with the possibility of catastrophic financial losses resulting:

1. Mobile Device Security and Management
2. Business Partners and Outsourcing
3. Insurance
4. Staffing
5. Fine-Grained Entitlements
6. Security Budget

Priority Two

The following criteria were compiled based upon the information provided. All items noted were allocated into the **high risk of security** controls being compromised with the potential for significant losses resulting:

1. Log Management
2. Fraud Detection
3. Single Sign-On and Strong Authentication
4. Data Encryption
5. Real-Time Detection
6. Ongoing Education
7. Directory Management
8. Data Loss Prevention (DLP)
9. Static Source Code Analysis
10. Endpoint Management
11. Outsourcing and Managed Security Services
12. Threat Intelligence

Priority Three

The following criteria were compiled based upon the information provided. All items noted were allocated into the **elevated risk of security** controls being compromised with the potential for material financial losses resulting:

1. Employee Security
2. Security Information and Event Management
3. Virtualization Protection

CYBER SECURITY INFORMATION RISK RATING SCALE

Level	Preparedness (%)	Risk Rating Category
Level 5	0-19%	**Extreme Risk** Extreme risk of security controls being compromised with the possibility of catastrophic financial losses resulting.
Level 4	20-39%	**High Risk** High risk of security controls being compromised with the potential for significant losses resulting.
Level 3	40-59%	**Elevated Risk** Elevated risk of security controls being compromised with the potential for material financial losses resulting.
Level 2	60-79%	**Moderate Risk** Moderate risk of security controls being compromised with the possibility of limited financial losses occurring as a result.
Level 1	80-100%	**Minimal Risk** Minimal risk of security controls being compromised with measurable negative impacts as a result.

Service-oriented architecture (SOA) is a style of software design where services are provided to the other components by application components, through a communication protocol over a network. A service is a discrete unit of functionality that can be accessed remotely and acted upon and updated independently, such as retrieving a credit card statement online.

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

An **incident response plan (IRP)** is a set of written instructions for detecting, responding to and limiting the effects of an information security event.

cyberisk check 2018 ©

Additional Information: www.cyberiskchekinfo.com