\*Organization Profile: Atlas Company\*

- Organization Name: Atlas Company

- Location: Colombo, Sri Lanka

- Industry: Manufacturing and Export

- Number of Employees: 250

- Revenue: $20 million annually

- Key Information Assets: Product Designs, Customer Database, Financial Records, Supply Chain Information, Intellectual Property

\*Information Asset Risk Worksheet 1: Product Designs\*

- Asset Description: Atlas Company's product designs for their manufacturing operations.

- Asset Owner: Head of Design Department

- Asset Location: Secure servers within the organization's IT infrastructure

- Potential Threats:

1. Unauthorized Access: Internal employees or external attackers gaining unauthorized access to design files.

2. Data Theft: Competitors or malicious actors stealing product designs.

3. Insider Threat: Disgruntled employees leaking confidential designs.

4. Data Corruption: Accidental deletion or alteration of design files.

5. Natural Disasters: Loss of data due to fires, floods, or other natural disasters.

2nd

\*Information Asset Risk Worksheet 1: Product Designs\*

Information Asset Name: Product Designs

Asset Description: Blueprints and design specifications of Atlas Axillia's stationery products.

Asset Owner: Research and Development Department

Asset Custodian: Chief Product Officer

Threats:

1. Intellectual Property Theft:

- Likelihood: Moderate

- Impact: Critical

2. Unauthorized Access:

- Likelihood: Low

- Impact: High

3. Industrial Espionage:

- Likelihood: Low

- Impact: Critical

\*Worksheet 2: Employee Data\*

Asset Description:

- Employee database containing personal information (e.g., name, address, Social Security numbers, salary details, and performance records).

Threats:

1. Unauthorized Access: Malicious actors gaining unauthorized access to the employee database.

2. Insider Threat: Employees or contractors with access abusing their privileges or stealing data.

3. Data Breach: External hackers exploiting vulnerabilities to steal or expose sensitive employee data.

4. Data Loss: Accidental deletion or corruption of employee records due to system failures.

5. Compliance Violation: Failure to adhere to data protection regulations, leading to legal repercussions.

Assessment of Impact and Likelihood:

- Impact: High

- Likelihood: Moderate

Risk Level:

- High Risk

2nd

\*Information Asset Risk Worksheet 2: Employee Data\*

Information Asset Name: Employee Data

Asset Description: Personal information, payroll data, and performance records of all employees.

Asset Owner: Human Resources Department

Asset Custodian: HR Manager

Threats:

1. Unauthorized Access:

- Likelihood: Moderate

- Impact: High

2. Data Breach:

- Likelihood: Low

- Impact: Critical

3. Insider Threat:

- Likelihood: Moderate

- Impact: High

4. Data Loss:

- Likelihood: Low

- Impact: Moderate

\*Information Asset Risk Worksheet 3: Financial Records\*

- Asset Description: Financial records, including income statements, balance sheets, and tax documents.

- Asset Owner: CFO (Chief Financial Officer)

- Asset Location: Secure financial software and physical file storage.

- Potential Threats:

1. Insider Fraud: Unauthorized manipulation of financial records by employees.

2. External Hacking: Cyberattacks aimed at stealing financial data for monetary gain.

3. Data Loss: Accidental deletion or loss of financial records.

4. Regulatory Non-compliance: Fines and legal consequences due to failure to adhere to financial regulations.

5. Supplier Risk: Financial data of suppliers being compromised, affecting supply chain stability.

2nd

\*Information Asset Risk Worksheet 3: Financial Reports\*

Information Asset Name: Financial Reports

Asset Description: Annual financial reports, budget data, and profit projections.

Asset Owner: Finance Department

Asset Custodian: Chief Financial Officer

Threats:

1. Insider Fraud:

- Likelihood: Moderate

- Impact: High

2. Unauthorized Disclosure:

- Likelihood: Low

- Impact: Moderate

3. Data Manipulation:

- Likelihood: Low

- Impact: High

\*Information Asset Risk Worksheet 4: Supply Chain Information\*

- Asset Description: Information about suppliers, inventory levels, and logistics.

- Asset Owner: Supply Chain Manager

- Asset Location: Supply chain management software and databases.

- Potential Threats:

1. Supplier Data Breach: Unauthorized access to supplier information.

2. Inventory Theft: Theft or mismanagement of inventory data affecting operations.

3. Disruption: Natural disasters or supply chain attacks impacting the supply chain.

4. Regulatory Changes: Non-compliance with changing trade or logistics regulations.

5. Data Leakage: Unintentional disclosure of supply chain data to competitors.

2nd

\*Information Asset Risk Worksheet 4: Supplier Contracts\*

Information Asset Name: Supplier Contracts

Asset Description: Contracts and agreements with suppliers for raw materials and goods.

Asset Owner: Procurement Department

Asset Custodian: Procurement Manager

Threats:

1. Contract Breach:

- Likelihood: Moderate

- Impact: High

2. Vendor Risk:

- Likelihood: Moderate

- Impact: Moderate

3. Legal and Regulatory Compliance:

- Likelihood: Low

- Impact: Critical

\*Information Asset Risk Worksheet 5: Intellectual Property\*

- Asset Description: Valuable intellectual property, including patents, trademarks, and proprietary technology.

- Asset Owner: Chief Technology Officer (CTO)

- Asset Location: Secure digital repositories and legal documentation.

- Potential Threats:

1. Intellectual Property Theft: Competitors or cybercriminals attempting to steal valuable IP.

2. Insider Threat: Employees attempting to leak or misuse intellectual property.

3. IP Infringement: Legal issues related to IP violations.

4. Data Corruption: Accidental damage to IP files.

5. Data Backup Failure: Loss of IP data due to backup system failures.

\*Information Asset Risk Worksheet 6: Customer Order Database\*

Information Asset Name: Customer Order Database

Asset Description: Database containing customer orders, delivery schedules, and payment information.

Asset Owner: Sales and Marketing Department

Asset Custodian: IT Manager

Threats:

1. Data Corruption:

- Likelihood: Low

- Impact: Moderate

2. Unauthorized Access:

- Likelihood: Moderate

- Impact: High

3. System Downtime:

- Likelihood: Low

- Impact: Moderate