\*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

3rd

**Information Asset Risk Worksheet 2: Product Designs**

1. **Information Asset Name:** Product Designs
2. **Description:** Proprietary product designs and blueprints, including innovative features and manufacturing processes.
3. **Value:** Very High
4. **Potential Threats:** a. Industrial espionage by competitors. b. Unauthorized access by current or former employees. c. Cyberattacks targeting design files.
5. **Likelihood:** Low
6. **Impact:** Very High
7. **Risk Level:** High

\*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

3rd

**Information Asset Risk Worksheet 1: Employee Data**

1. **Information Asset Name:** Employee Data
2. **Description:** Personal information of all employees, including names, addresses, social security numbers, contact details, and salary details.
3. **Value:** High
4. **Potential Threats:** a. Unauthorized access to employee data. b. Data breaches or leaks leading to identity theft. c. Insider threats from disgruntled employees.
5. **Likelihood:** Moderate
6. **Impact:** High
7. **Risk Level:** High

\*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

3rd

**Information Asset Risk Worksheet 6: Supply Chain Information**

1. **Information Asset Name:** Supply Chain Information
2. **Description:** Supplier lists, vendor contracts, and logistics information.
3. **Value:** High
4. **Potential Threats:** a. Disruption of the supply chain by competitors. b. Insider threats compromising vendor relationships. c. Cyberattacks on logistics systems.
5. **Likelihood:** Moderate
6. **Impact:** High
7. **Risk Level:** High

\*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.

2nd

Information Asset Risk Worksheet 9: Intellectual Property (IP)

Information Asset Name: Intellectual Property (IP)

Description: Patents, trademarks, and copyrights protecting company innovations and brand identity.

Value: Very High

Potential Threats:

a. IP theft or infringement by competitors.

b. Insider threats leaking IP.

c. Legal disputes and reputation damage.

Likelihood: Low

Impact: Very High

Risk Level: High

\*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

\*Information Asset Risk Worksheet 7: Research and Development (R&D) Data \*

\*Asset Name:\* Research and Development (R&D) Data

\*Asset Description:\* R&D data includes ongoing research, prototypes, and innovative ideas of Atlas Axillia.

\*Potential Threats:\*

1. IP Theft: External entities attempting to steal or replicate R&D innovations.

2. Insider Threat: Employees leaking sensitive R&D data to competitors.

3. Industrial Espionage: Competitors infiltrating Atlas Axillia to steal R&D information.

\*Risk Assessment:\*

- \*Likelihood:\* Low

- \*Impact:\* Very High

- \*Risk Level:\* High

\*Risk Mitigation:\*

- Implement strict access controls for R&D data repositories.

- Monitor and log access to sensitive R&D information.

- Conduct regular security awareness programs for employees working on R&D projects.

2nd

\*Information Asset Risk Worksheet 7: Product Development Plans \*

\*2. Asset Name:\* Product Development Plans

\*Description:\* Contains information about upcoming product designs, features, and development strategies.

\*Potential Threats:\*

1. Intellectual Property Theft: External entities attempting to steal or copy product development plans.

2. Insider Threat: Employees disclosing confidential plans to competitors.

3. Data Loss: Accidental deletion or corruption of development data.

4. Industrial Espionage: Competitors trying to infiltrate and steal plans.

\*Risk Assessment:\*

- \*Likelihood:\* Low

- \*Impact:\* Very High

- \*Risk Level:\* High

\*Risk Mitigation:\*

- Implement robust access controls for development plans.

- Regularly back up development data and store backups offsite.

- Conduct background checks on employees with access to sensitive information.

---

\*Information Asset Risk Worksheet 8: Marketing Strategies\*

\*Asset Name:\* Marketing Strategies

\*Asset Description:\* Marketing strategies include market research, advertising plans, and customer targeting information.

\*Potential Threats:\*

1. Competitor Espionage: Competitors attempting to access and copy marketing strategies.

2. Insider Threat: Employees disclosing confidential marketing strategies to external entities.

3. Data Leakage: Unintentional leakage of marketing strategies through third-party vendors.

\*Risk Assessment:\*

- \*Likelihood:\* Low

- \*Impact:\* High

- \*Risk Level:\* Moderate

\*Risk Mitigation:\*

- Limit access to marketing strategies to a need-to-know basis.

- Implement non-disclosure agreements with third-party vendors.

- Monitor and control employee communications regarding marketing strategies.

Worksheet 9: IT Infrastructure and Network Security

Information Asset Description:

The IT Infrastructure and Network Security includes servers, firewalls, routers, and other networking equipment.

Threats:

DDoS Attacks: Overwhelming the network with excessive traffic, causing service disruption.

Unauthorized Access: Intruders gaining unauthorized access to critical network components.

Malware Infections: Introduction of malicious software compromising network integrity.

Vulnerabilities:

Weak Firewall Configurations: Inadequate firewall rules or outdated firmware.

Lack of Intrusion Detection Systems (IDS): Insufficient monitoring for suspicious network activities.

Inadequate Patch Management: Failure to timely apply security patches and updates.

Risk Level: High

**Information Asset Risk Worksheet 10: Manufacturing Processes**

1. **Information Asset Name:** Manufacturing Processes
2. **Description:** Proprietary manufacturing processes, machinery specifications, and quality control procedures.
3. **Value:** Very High
4. **Potential Threats:** a. Industrial espionage by competitors. b. Sabotage by disgruntled employees. c. Cyberattacks targeting production data.
5. **Likelihood:** Low
6. **Impact:** Very High
7. **Risk Level:** High

Certainly, I can provide you with an example of seven Information Asset Risk Worksheets for Atlas Axillia, a company based in Sri Lanka that specializes in stationery and office supplies. Please note that the specific details and risks mentioned in these worksheets are fictional and created for illustrative purposes.

\*\*Information Asset Risk Worksheet 1: Customer Database\*\*

1. \*\*Information Asset\*\*: Customer Database

2. \*\*Description\*\*: This database contains customer contact information, purchase history, and preferences.

3. \*\*Potential Threats\*\*:

- Unauthorized access to customer data.

- Data breaches leading to customer information exposure.

- Inaccurate data entry or data corruption.

4. \*\*Risk Impact\*\*:

- Financial loss due to data breaches.

- Damage to customer trust and reputation.

5. \*\*Risk Likelihood\*\*:

- Moderate, as customer data is valuable to attackers.

6. \*\*Risk Mitigation\*\*:

- Implement access controls and encryption.

- Regularly audit and monitor database access.

- Conduct employee training on data handling best practices.

\*\*Information Asset Risk Worksheet 2: Product Design Plans\*\*

1. \*\*Information Asset\*\*: Product Design Plans

2. \*\*Description\*\*: Contains confidential product designs, prototypes, and research.

3. \*\*Potential Threats\*\*:

- Industrial espionage or theft of design plans.

- Unauthorized access by competitors.

- Accidental leakage of sensitive design information.

4. \*\*Risk Impact\*\*:

- Loss of competitive advantage.

- Potential financial losses due to product design theft.

5. \*\*Risk Likelihood\*\*:

- Low, but the impact would be significant.

6. \*\*Risk Mitigation\*\*:

- Restrict access to design files to authorized personnel only.

- Implement encryption and secure storage.

- Conduct regular security audits.

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

1. \*\*Information Asset\*\*: Financial Data

2. \*\*Description\*\*: Contains financial records, transaction details, and payroll information.

3. \*\*Potential Threats\*\*:

- Fraudulent transactions.

- Unauthorized access to payroll data.

- Financial data breaches.

4. \*\*Risk Impact\*\*:

- Financial losses due to fraud or data breaches.

- Legal and regulatory penalties.

5. \*\*Risk Likelihood\*\*:

- Moderate, as financial data is a common target.

6. \*\*Risk Mitigation\*\*:

- Implement strong access controls and authentication.

- Regularly audit financial data access.

- Encrypt sensitive financial information.

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

1. \*\*Information Asset\*\*: Supplier Contracts

2. \*\*Description\*\*: Contains confidential agreements, pricing details, and supplier contact information.

3. \*\*Potential Threats\*\*:

- Unauthorized access by competitors.

- Contract breaches or disputes.

- Leakage of sensitive pricing information.

4. \*\*Risk Impact\*\*:

- Loss of competitive advantage.

- Legal issues and financial losses due to contract breaches.

5. \*\*Risk Likelihood\*\*:

- Low to moderate, depending on competitor interest.

6. \*\*Risk Mitigation\*\*:

- Restrict access to contract details.

- Monitor and log access to sensitive supplier information.

- Educate employees about the importance of confidentiality.

\*\*Information Asset Risk Worksheet 5: Employee Personal Data\*\*

1. \*\*Information Asset\*\*: Employee Personal Data

2. \*\*Description\*\*: Contains employee personal information, including Social Security numbers, addresses, and banking details.

3. \*\*Potential Threats\*\*:

- Data breaches or theft of employee information.

- Identity theft or financial fraud.

- Unauthorized access to sensitive HR records.

4. \*\*Risk Impact\*\*:

- Legal and regulatory consequences.

- Damage to employee trust.

5. \*\*Risk Likelihood\*\*:

- Moderate, as employee data is a common target.

6. \*\*Risk Mitigation\*\*:

- Implement strict access controls.

- Encrypt employee data at rest and in transit.

- Train employees on data protection and privacy.

\*\*Information Asset Risk Worksheet 6: Intellectual Property (IP) Assets\*\*

1. \*\*Information Asset\*\*: Intellectual Property (IP) Assets

2. \*\*Description\*\*: Contains patents, trademarks, and proprietary product information.

3. \*\*Potential Threats\*\*:

- IP theft by competitors or insiders.

- Unauthorized access to IP repositories.

- Infringement claims or legal disputes.

4. \*\*Risk Impact\*\*:

- Loss of IP value and market position.

- Legal actions and financial losses.

5. \*\*Risk Likelihood\*\*:

- Moderate, as IP is highly valuable.

6. \*\*Risk Mitigation\*\*:

- Implement IP protection measures.

- Monitor access to IP repositories.

- Educate employees on IP rights and confidentiality.

\*\*Information Asset Risk Worksheet 7: Marketing Campaign Data\*\*

1. \*\*Information Asset\*\*: Marketing Campaign Data

2. \*\*Description\*\*: Contains customer engagement data, marketing strategies, and campaign results.

3. \*\*Potential Threats\*\*:

- Data breaches leading to exposure of marketing strategies.

- Unauthorized access to customer engagement data.

- Competitive analysis through leaked campaign information.

4. \*\*Risk Impact\*\*:

- Loss of marketing effectiveness.

- Damage to the company's marketing strategies.

5. \*\*Risk Likelihood\*\*:

- Moderate, as marketing data is valuable to competitors.

6. \*\*Risk Mitigation\*\*:

- Secure access to marketing data.

- Implement encryption for sensitive campaign information.

- Educate marketing teams on data confidentiality.

Please note that these risk worksheets are fictional and should serve as examples to help you create similar documents for Atlas Axillia or any other organization. Actual risks may vary, and it's important for organizations to conduct thorough risk assessments and take appropriate measures to mitigate risks to their information assets.

Certainly, I can help you create information asset risk worksheets for Atlas Axillia, a hypothetical company in Sri Lanka. Please keep in mind that since I don't have access to specific internal technical information, the components will be fictional and based on general industry knowledge.

---

\*\*Organization: Atlas Axillia Co. Sri Lanka\*\*

\*\*Information Asset Risk Worksheets\*\*

\*Worksheet 1: Customer Database\*

\*\*Information Asset Description:\*\*

The Customer Database contains personal information, including names, addresses, contact details, and purchase history of Atlas Axillia's customers.

\*\*Threats:\*\*

1. Unauthorized Access: Hackers or disgruntled employees gaining unauthorized access to the database.

2. Data Breach: Inadvertent or deliberate disclosure of customer information, potentially leading to legal consequences.

3. Data Corruption: Accidental or intentional alteration of customer records, causing misinformation or loss of trust.

\*\*Vulnerabilities:\*\*

1. Weak Password Policies: Insufficiently strong passwords or infrequent password updates.

2. Insufficient Access Controls: Lack of proper access restrictions to sensitive customer data.

3. Lack of Encryption: Failure to encrypt data both in transit and at rest.

\*\*Risk Level: High\*\*

---

\*Worksheet 2: Financial Transactions System\*

\*\*Information Asset Description:\*\*

The Financial Transactions System manages all financial transactions, including invoicing, payments, and payroll.

\*\*Threats:\*\*

1. Fraudulent Transactions: Unauthorized or fabricated financial transactions.

2. Malware Attack: Introduction of malicious software targeting financial systems.

3. Insider Threats: Disgruntled employees manipulating financial records.

\*\*Vulnerabilities:\*\*

1. Outdated Software: Running outdated financial software with known vulnerabilities.

2. Lack of Intrusion Detection: Insufficient monitoring for unusual financial activities.

3. Insufficient Audit Trails: Inadequate records for tracking and verifying financial transactions.

\*\*Risk Level: Medium\*\*

---

\*Worksheet 3: Intellectual Property Repository\*

\*\*Information Asset Description:\*\*

The Intellectual Property Repository contains proprietary designs, patents, and product development plans.

\*\*Threats:\*\*

1. Intellectual Property Theft: Unauthorized access leading to theft or replication of unique designs.

2. Industrial Espionage: Competitors attempting to gather sensitive information for competitive advantage.

3. Disgruntled Employee Actions: Employees with access attempting to steal or leak IP.

\*\*Vulnerabilities:\*\*

1. Weak Authentication: Insufficient login security measures for accessing sensitive IP.

2. Inadequate Access Monitoring: Lack of real-time monitoring for unusual access patterns.

3. Poor Data Loss Prevention Measures: Inadequate measures to prevent unauthorized data transfers.

\*\*Risk Level: High\*\*

---

\*Worksheet 4: Supply Chain Management System\*

\*\*Information Asset Description:\*\*

The Supply Chain Management System handles supplier contracts, inventory levels, and shipping information.

\*\*Threats:\*\*

1. Supply Chain Disruption: Disruptions or delays in the procurement and delivery process.

2. Vendor Compromise: Compromised supplier systems leading to potential security breaches.

3. Inaccurate Inventory Data: Mismanagement leading to stockouts or overstocking.

\*\*Vulnerabilities:\*\*

1. Lack of Supplier Security Checks: Insufficient vetting of supplier cybersecurity practices.

2. Inadequate Inventory Tracking: Poor visibility into inventory levels and trends.

3. Weak Contract Management: Inefficiencies in tracking and managing supplier contracts.

\*\*Risk Level: Medium\*\*

---

\*Worksheet 5: Employee Records and HR System\*

\*\*Information Asset Description:\*\*

The Employee Records and HR System contains personal and employment-related information of all employees.

\*\*Threats:\*\*

1. Unauthorized Access: Unauthorized personnel accessing sensitive employee information.

2. Data Loss: Accidental or deliberate deletion or loss of critical HR data.

3. Compliance Violations: Failure to comply with data protection regulations, leading to legal consequences.

\*\*Vulnerabilities:\*\*

1. Insufficient Access Controls: Lack of proper access restrictions to HR records.

2. Inadequate Backup Procedures: Lack of regular and secure data backups.

3. Weak Data Privacy Policies: Inadequate policies for safeguarding employee data.

\*\*Risk Level: High\*\*

---

\*Worksheet 6: Marketing and Customer Communications Platform\*

\*\*Information Asset Description:\*\*

The Marketing and Customer Communications Platform contains marketing materials, customer email lists, and campaign data.

\*\*Threats:\*\*

1. Phishing Attacks: Malicious emails attempting to trick customers or employees.

2. Data Leakage: Inadvertent sharing of sensitive customer information.

3. Brand Impersonation: Fake communications appearing to be from Atlas Axillia.

\*\*Vulnerabilities:\*\*

1. Lack of Employee Training: Insufficient training in identifying and responding to phishing attempts.

2. Insecure Communication Channels: Using unencrypted or unsecured channels for customer communications.

3. Insufficient Email Security: Weak email filtering and anti-phishing measures.

\*\*Risk Level: Medium\*\*

---

\*Worksheet 7: IT Infrastructure and Network Security\*

\*\*Information Asset Description:\*\*

The IT Infrastructure and Network Security includes servers, firewalls, routers, and other networking equipment.

\*\*Threats:\*\*

1. DDoS Attacks: Overwhelming the network with excessive traffic, causing service disruption.

2. Unauthorized Access: Intruders gaining unauthorized access to critical network components.

3. Malware Infections: Introduction of malicious software compromising network integrity.

\*\*Vulnerabilities:\*\*

1. Weak Firewall Configurations: Inadequate firewall rules or outdated firmware.

2. Lack of Intrusion Detection Systems (IDS): Insufficient monitoring for suspicious network activities.

3. Inadequate Patch Management: Failure to timely apply security patches and updates.

\*\*Risk Level: High\*\*

---

Please note that these worksheets are fictional and should serve as a starting point for assessing information asset risks. Actual risk assessments would require input from security experts, IT personnel, and other relevant stakeholders within the organization.