1. **Managing IoT Risks**

- Map the IoT Attack Surface
  Build in Security by Design

---

2. **Securing Web and Cloud Interfaces**

- Identify Threats to IoT Web and Cloud Interfaces
  Prevent Injection Flaws
  Prevent Session Management Flaws
  Prevent Cross-Site Scripting Flaws
  Prevent Cross-Site Request Forgery Flaws
  Prevent Unvalidated Redirects and Forwards

---

3. **Securing Data**

- Use Cryptography Appropriately
  Protect Data in Motion
  Protect Data at Rest
  Protect Data in Use

---

4. **Controlling Access to IoT Resources**

- Identify the Need to Protect IoT
  Implement Secure Authentication
  Implement Secure Authorization
  Implement Security Monitoring on IoT Systems

---

5. **Securing IoT Networks**

- Ensure the Security of IP Networks
  Ensure the Security of Wireless Networks
  Ensure the Security of Mobile Networks
  Ensure the Security of IoT Edge Networks

---

6. **Ensuring Privacy**

- Improve Data Collection to Reduce Privacy Concerns
Protect Sensitive Data
Dispose of Sensitive Data

---

7. Managing Software and Firmware Risks

- Manage General Software Risks
Manage Risks Related to Software Installation and Configuration
Manage Risks Related to Software Patches and Updates
Manage Risks Related to IoT Device Operating Systems and Firmware

---

8. Promoting Physical Security

- Protect Local Memory and Storage
Prevent Physical Port Access