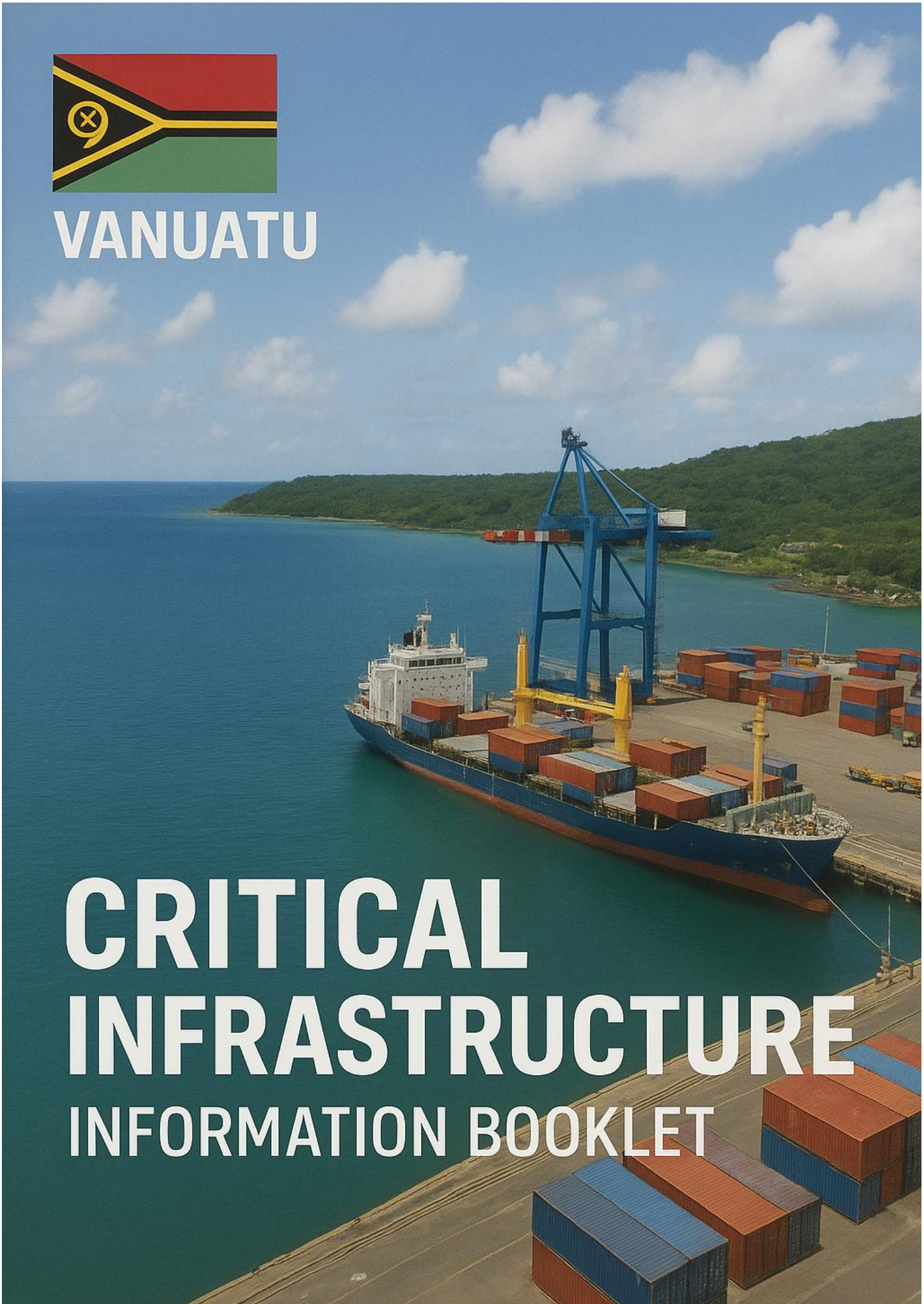

VANUATU

CRITICAL INFRASTRUCTURE

INFORMATION BOOKLET

Critical Infrastructure Information Booklet

What is critical infrastructure?

Critical infrastructure are the essential systems and services that Vanuatu relies on for government operations, communication, financial or banking system, education, healthcare, energy, transport, national security and other everyday services.

When these services work well, people are safe, feel connected and can access the goods and services they need. When these systems are disrupted, they can have a debilitating effect on our health, national security, and economic stability.

Why is critical infrastructure important?

Caring for our critical infrastructure keeps our communities strong.

When the critical infrastructure is damaged, it can trigger widespread impacts, including the shutdown essential services, reduce the government and emergency services ability to respond, potentially increasing the risks to public health and safety.

Who protects critical infrastructure?

Protecting critical infrastructure is a shared responsibility involving various sectors.

Key groups include:

- Technical specialists who manage, monitor and maintain essential systems such as power, water, digital services and communications
- Government employees who develop policies, coordinate resources and support the delivery of services
- Police, fire, medical and disaster response teams
- Many essential services are operated by private organisations who have a role in maintaining and protecting infrastructure
- You, the public contribute by being prepared, reporting issues and following advice

Interconnected nature of critical infrastructure

Critical infrastructure is interconnected and depends on other systems. When one system fails it can affect other systems.

Think of it as a ripple effect. When you drop a stone into a calm pool of water the stone causes ripples in the water. When one critical infrastructure system fails the first ripple hits the closest system, the second ripple spreads further out to affect more systems and so on.

Here are some ripple effect examples when electricity fails:

The first ripple

- Water treatment plants and pumping stations run on electricity, if there is no back up generator then water supply will be disrupted.

- Clean water supply and wastewater services will be disrupted affecting homes, schools, businesses, hospitals, factories and government facilities.

- Communication networks run on electricity and are virtually integrated into nearly every aspect of life and modern infrastructure systems. When disrupted they will cease to support mobile towers, the Internet, and the technologies we use to monitor and control water, power, and fuel distribution, deliver services, coordinate emergency responses and manage air traffic control.

Second ripple

- Emergency services may lose the ability to effectively dispatch services in an emergency.

- Transport and emergency service networks rely on regular fuel supplies. However, fuel terminals and pumping stations need electricity to work. Airports, ports and

local transport are critical to the distribution and delivery of fuel, food and essential goods. Any disruption to these systems can reduce the availability of fuel, threaten food security, and hinder medical support, impacting community safety and mobility.

Third ripple

- Hospitals rely on electricity, water and communication systems to work effectively. If these systems fail, essential medical equipment stops working. Although, emergency generators can maintain operations temporarily, continued delivery of services depends on fuel availability. Without fuel resupplies generators will eventually stop working.

- Banks and financial institutions depend on electricity to process transactions, operate ATM machines and support point of sale card purchases. Disruptions can prevent customers from accessing funds, purchasing essential items and businesses may need to close.
- Without power, water, communications and safe transport schools will be forced to close. This will shift the caring burden onto families impacting workforce availability.
- Government and public service functions close due to power and communication outages, digital services go offline which affects the issuing of licences, permits, visas, record management and payments, as employees cannot access essential databases and information.

Understanding how different infrastructure systems depend on one another within and between systems helps us plan for disruptions and develop backup strategies.

Common threats to Infrastructure

Critical infrastructure can be affected by a wide rage of risks. Understanding where these risks come from can help us prepare, prevent and respond when incidents occur.

Natural Threats

- Earthquakes
- Floods
- Cyclones
- Volcanic eruption

Man-Made Threats

- Cyberattacks (e.g., ransomware)
- Vandalism / sabotage (e.g., attacks on transportation hubs)
- Insider threats

Operational issues (a bit like feeling fatigued or malnourished)

- Equipment failure
- Poor maintenance
- Communication issues

Vanuatu case study examples

Natural disasters

- **Earthquake (December 2024)**:
  The landing station infrastructure at Vanuatu's single submarine communications cable (ICN1) was damaged during the earthquake, causing internet outages.

- **Cyclones Judy and Kevin (March 2023)**:
  Two Category 4 cyclones caused flooding, damaged infrastructure, and roads leading to power outages and a breakdown in communications systems and preventing delivery of emergency supplies and food.

Man-made incidents

- **Ransomware (November 2022)**
  A ransomware attack on the Vanuatu Government broadband network caused widespread outage of email and government online services, shutting down ministries and departments, and affecting online payment of suppliers.

Operational issues

- **Luganville water network (2017 / 2018)**
  An audit of the water network identified several issues including aging infrastructure, insufficient water carrying capacity, a lack of proactive maintenance and no water quality testing capability.

National Security & Infrastructure Protection

Why It Matters

- Malicious actors and cyber criminals may target critical infrastructure, such as government service, power, communications and transport, because disrupting these systems has strategic value and can quickly weaken a country's ability to function and respond.
- Outdated or poorly maintained infrastructure can create points of failure that can be exploited. Poor maintenance, a lack of redundancy, or being slow to modernise increase the likelihood of system failure during a crisis.
- Attacks or failures in critical infrastructure have both physical and psychological impacts. When essential services fail, communities experience uncertainty, frustration and fear, which can amplify tensions and erode public confidence and trust in government and its ability to protect its people.

Government Response

- Government Departments monitor key infrastructure, detect vulnerabilities, anticipate threats, build redundancy strategies into critical systems and coordinate emergency responses.

- Cybersecurity agencies, such as the Computer Emergency Response Team (CERT) track and respond to suspicious online activity and provides advice to the private sector.

Conclusion

Our critical infrastructure keeps our communities safe, connected and informed. Protecting them is up to all of us. Let's work together to keep our critical infrastructure safe and secure.

Resource

- CISA interdependencies (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn)