

# LEGAL\_QUICK\_REFERENCE\_CARD

---

- [SOUTHGATE TERMINAL](#)
  - [Legal Team Quick Reference Card](#)
    - [75-Minute Compliance & Risk Management Guide](#)
  - [PURPOSE](#)
  - [PHASE 1 \(0-15 Minutes\) - Policy Gaps & Insurance Concerns](#)
    - [EARLY WARNING SIGNALS](#)
    - [IMMEDIATE ASSESSMENT PRIORITIES](#)
    - [ESSENTIAL DOCUMENTS](#)
    - [INSURANCE DECISION FRAMEWORK](#)
    - [KEY QUESTIONS TO RESOLVE](#)
  - [PHASE 2 \(15-35 Minutes\) - Vendor Crisis & Privilege Concerns](#)
    - [ESCALATING LEGAL COMPLEXITIES](#)
    - [CRITICAL LEGAL DECISIONS](#)
    - [KEY DOCUMENTS NEEDED](#)
    - [VENDOR INCIDENT MANAGEMENT](#)
    - [CFO BRIEFING REQUIREMENTS](#)
  - [PHASE 3 \(35-55 Minutes\) - Regulatory Pressure Mounting](#)
    - [COMPLIANCE CHALLENGES INTENSIFYING](#)
    - [REGULATORY DECISION MATRIX](#)
    - [CRITICAL DOCUMENTS](#)
    - [NOTIFICATION PRIORITIZATION](#)
    - [INSURANCE FINAL DETERMINATION](#)
  - [PHASE 4 \(55-75 Minutes\) - Ministerial Scrutiny & Final Positions](#)
    - [PEAK LEGAL PRESSURE](#)
    - [FINAL PHASE DECISIONS](#)
    - [ESSENTIAL FINAL DOCUMENTS](#)

- [CFO FINAL BRIEFING](#)
- [MINISTERIAL SUBMISSION COMPONENTS](#)
- [LEGAL RISK ASSESSMENT FRAMEWORK](#)
  - [IMMEDIATE EVALUATION \(Any Phase\)](#)
  - [EVIDENCE PRESERVATION REQUIREMENTS](#)
  - [PRIVILEGE PROTECTION PROTOCOL](#)
- [REGULATORY COMPLIANCE QUICK GUIDE](#)
  - [NOTIFICATION DECISION TREE](#)
  - [NOTIFICATION ESSENTIALS](#)
  - [REGULATORY PRIORITIES](#)
- [INSURANCE MANAGEMENT GUIDE](#)
  - [COVERAGE DETERMINATION CHECKLIST](#)
  - [INSURER COMMUNICATION](#)
  - [DOCUMENTATION FOR INSURERS](#)
- [QUICK DECISION TEMPLATES](#)
  - [Media Blackout Determination](#)
  - [Insurance Position Statement](#)
  - [Regulatory Notification](#)
  - [Vendor Liability Assessment](#)
- [COORDINATION PROTOCOLS](#)
  - [WITH EXECUTIVE TEAM](#)
  - [WITH TECHNICAL TEAM](#)
  - [WITH MEDIA TEAM](#)
  - [WITH OPERATIONS TEAM](#)
- [LEGAL TEAM PRINCIPLES](#)

# SOUTHGATE TERMINAL

---

## Legal Team Quick Reference Card

---

### 75-Minute Compliance & Risk Management Guide

---

## PURPOSE

---

This card guides Legal Team decision-making during the port cybersecurity incident, managing insurance, regulatory compliance, and legal risk without revealing specific scenario details.

---

## PHASE 1 (0-15 Minutes) - Policy Gaps & Insurance Concerns

---

### EARLY WARNING SIGNALS

- **Policy Issues:** Expired contingency plans discovered
- **System Anomalies:** Vessel tracking visibility problems
- **Insurance Queries:** Coverage clarification requests
- **Media Interest:** Communication restriction questions

### IMMEDIATE ASSESSMENT PRIORITIES

1. **Contingency Documentation:** Review expired policy implications
2. **Insurance Coverage:** Analyse applicable clauses (4.7 vs 7.4)
3. **Communication Restrictions:** Determine media blackout requirements
4. **Incident Classification:** Begin preliminary categorisation

### ESSENTIAL DOCUMENTS

- `Insurance_Clause_Interpretation.pdf` - Coverage analysis

- Legal Precedent Summary Sheet.pdf - Reference cases
- Crisis\_Communications\_SOP.pdf - Communication protocols
- Breach\_Classification\_Decision\_Tree.pdf - Classification guide

## INSURANCE DECISION FRAMEWORK

**Clause 4.7 (Standard Coverage) Applies If:** - Data inaccuracy affecting operations - Technical failure likely cause - Single system primary impact - Standard operational disruption

**Clause 7.4 (Enhanced Coverage) Applies If:** - Multiple systems affected - Cyber attack indicators present - Systemic operational risk evident - Coordinated malicious activity suspected

## KEY QUESTIONS TO RESOLVE

1. Is this technical failure or cyber attack?
  2. What systems are affected and how?
  3. What are our notification obligations?
  4. Can external communications proceed?
- 

## PHASE 2 (15-35 Minutes) - Vendor Crisis & Privilege Concerns

---

### ESCALATING LEGAL COMPLEXITIES

- **Vendor Breach:** Third-party security failures
- **Privilege Risk:** Legal communications potentially exposed
- **Board Attention:** Governance-level concerns
- **Financial Queries:** CFO insurance determination needs

### CRITICAL LEGAL DECISIONS

1. **Privilege Protection:** How to handle compromised communications?
2. **Vendor Liability:** Assessment of third-party responsibility?
3. **Insurance Position:** Preliminary determination for CFO?

#### 4. **Disclosure Obligations:** What must be reported now?

### KEY DOCUMENTS NEEDED

- `Vendor_Incident_Coordination_Protocol.pdf` - Vendor procedures
- `Legal_Risk_Escalation_Flowchart.pdf` - Escalation criteria
- `Breach_Disclosure_Checklist.pdf` - Notification guide
- Previous phase documents remain active

### VENDOR INCIDENT MANAGEMENT

**Immediate Actions:** 1. Document vendor system compromise 2. Assess privilege breach scope 3. Notify insurers of third-party issue 4. Coordinate evidence preservation

**Liability Considerations:** - Vendor contract terms and SLAs - Indemnification clauses - Insurance coverage for third-party failures - Potential recovery actions

### CFO BRIEFING REQUIREMENTS

1. Current insurance clause determination
2. Coverage limits and deductibles
3. Notification requirements status
4. Financial exposure assessment

---

## PHASE 3 (35-55 Minutes) - Regulatory Pressure Mounting

---

### COMPLIANCE CHALLENGES INTENSIFYING

- **Multiple Notifications:** Various regulators activated
- **Safety Implications:** WorkSafe potential involvement
- **Operational Incidents:** Container misrouting legal impact
- **Documentation Demands:** Insurers requiring details

REGULATORY DECISION MATRIX

- 1. **Cybersecurity Act:** 24-hour breach notification?
- 2. **WorkSafe:** Immediate if safety risk exists?
- 3. **Port Authority:** Operational disruption threshold?
- 4. **Maritime Security:** Navigation system compromise?

CRITICAL DOCUMENTS

- `Regulatory_Timeline_Compliance.pdf` - All deadlines
- `Insurance_Clause_Interpretation.pdf` - Final determination
- `Breach_Disclosure_Checklist.pdf` - Notification steps
- All previous documents remain relevant

NOTIFICATION PRIORITIZATION

**Immediate (0-2 hours):** - Safety-related incidents - Criminal activity evidence - Court-ordered disclosures

**Short-term (2-24 hours):** - Cyber breach notifications - Insurance formal notices - Regulatory compliance reports

**Standard (24-72 hours):** - Stakeholder notifications - Industry body reports - Follow-up documentation

INSURANCE FINAL DETERMINATION

**Evidence Assessment for Classification:** 1. System compromise scope 2. Attack pattern indicators 3. Operational impact severity 4. Recovery complexity

**Documentation Required:** - Incident timeline - System affected list - Evidence preservation records - Mitigation measures taken

---

## PHASE 4 (55-75 Minutes) - Ministerial Scrutiny & Final Positions

---

### PEAK LEGAL PRESSURE

- **Board Questions:** Vendor negligence implications
- **CFO Demands:** Written insurance confirmation
- **Breach Notices:** Final approval needed
- **Minister Briefing:** Government reporting required

### FINAL PHASE DECISIONS

1. **Insurance Position:** Final written determination
2. **Breach Notification:** Language approval
3. **Vendor Liability:** Board briefing position
4. **Ministerial Response:** Legal components

### ESSENTIAL FINAL DOCUMENTS

- `Post-Breach Reform Guidance.pdf` - Future improvements
- All previous phase documents
- Compiled evidence packages
- Draft notifications

### CFO FINAL BRIEFING

**Must Include:** 1. Definitive clause determination (4.7 or 7.4) 2. Coverage amounts and exclusions 3. Supporting evidence summary 4. Risk factors identified 5. Written confirmation statement

### MINISTERIAL SUBMISSION COMPONENTS

- Incident classification
- Regulatory compliance status
- Legal risk assessment
- Remediation commitments

# LEGAL RISK ASSESSMENT FRAMEWORK

---

## IMMEDIATE EVALUATION (Any Phase)

1. CRIMINAL ACTIVITY?  
→ If YES: Law enforcement notification
2. SAFETY COMPROMISE?  
→ If YES: WorkSafe/Maritime notifications
3. DATA BREACH?  
→ If YES: Privacy/Cybersecurity Act compliance
4. SYSTEMIC FAILURE?  
→ If YES: Enhanced insurance coverage

## EVIDENCE PRESERVATION REQUIREMENTS

1. **Immediate:** Implement legal hold
2. **Coordinate:** Technical team preservation
3. **Document:** Chain of custody
4. **Protect:** Attorney-client privilege

## PRIVILEGE PROTECTION PROTOCOL

- Mark all legal advice clearly
  - Limit distribution lists
  - Use secure communication
  - Document privilege claims
-



# REGULATORY COMPLIANCE QUICK GUIDE

---

## NOTIFICATION DECISION TREE

```
Safety Risk? → WorkSafe (Immediate)
Cyber Attack? → Cybersecurity Act (24 hrs)
Port Operations? → Port Authority (Section 12.3)
Navigation? → Maritime Security (Immediate)
Data Breach? → Privacy Act (72 hrs)
```

## NOTIFICATION ESSENTIALS

**Every Notification Needs:** 1. Incident description 2. Timeline of events 3. Systems affected 4. Mitigation measures 5. Contact information

## REGULATORY PRIORITIES

1. **Life Safety:** Always first priority
  2. **Legal Obligations:** Statutory requirements
  3. **Contractual:** Insurance and agreements
  4. **Voluntary:** Industry best practice
- 

# INSURANCE MANAGEMENT GUIDE

---

## COVERAGE DETERMINATION CHECKLIST

- ☐ Number of systems affected?
- ☐ Evidence of coordination?
- ☐ Malicious indicators?
- ☐ Operational impact level?
- ☐ Recovery complexity?

## INSURER COMMUNICATION

**Initial Notice Should Include:** 1. Incident occurrence time 2. Initial impact assessment 3. Preservation measures taken 4. Investigation status 5. Preliminary classification

**Avoid Stating:** - Definitive cause - Liability admissions - Coverage assumptions - Third-party blame

## DOCUMENTATION FOR INSURERS

1. Technical logs and evidence
  2. Decision timeline
  3. Mitigation actions
  4. Cost estimates
  5. Recovery plans
- 

## QUICK DECISION TEMPLATES

---

### Media Blackout Determination

"Based on clause [X.X] requirements and current evidence of [incident type], we [do/do not] require communication restrictions. Media team may proceed with [specific limitations]."

### Insurance Position Statement

"Preliminary assessment indicates clause [4.7/7.4] applies based on [evidence factors]. Coverage includes [amounts] subject to [deductibles/exclusions]. Final determination pending investigation completion."

### Regulatory Notification

"Pursuant to [Act/Regulation Section], we hereby notify of an incident affecting [systems] detected at [time]. Current status: [description]. Full report to follow within required timeframe."

## Vendor Liability Assessment

"Initial review indicates vendor [name] [may have/has not] breached obligations under [contract section]. Recommend [immediate action] while preserving recovery options."

---

## COORDINATION PROTOCOLS

---

### WITH EXECUTIVE TEAM

- Provide clear recommendations
- Explain legal risks/benefits
- Support business decisions
- Document authorisations

### WITH TECHNICAL TEAM

- Coordinate evidence preservation
- Understand technical facts
- Avoid speculation
- Maintain privilege

### WITH MEDIA TEAM

- Approve all external statements
- Balance transparency/protection
- Provide compliant language
- Monitor disclosure risks

### WITH OPERATIONS TEAM

- Understand safety implications
- Document operational decisions
- Assess regulatory triggers

- Support continuity needs
- 

## LEGAL TEAM PRINCIPLES

---

1. **Document Everything:** Decisions, rationale, timing
  2. **Preserve Evidence:** Technical and business records
  3. **Meet Deadlines:** Regulatory compliance is critical
  4. **Protect Privilege:** Maintain confidentiality
  5. **Support Business:** Enable operations within law
- 

**Remember:** Your role is protecting the organisation while ensuring compliance. When in doubt, preserve evidence and meet regulatory deadlines first.

**Reference:** LEGAL-QRC-01 | **Version:** 1.0 | **Classification:** Legal Team Use