Webinar:
SOCI in 2024: Leveraging AI to Streamline Compliance

ReadiNow | LexisNexis® | *Regulatory Compliance*

WHO IS LEXISNEXIS

LexisNexis | Regulatory Compliance

WEBINAR | SOCI in 2024: Leveraging AI to Streamline Compliance

LEXISNEXIS LEGAL & PROFESSIONAL FAST FACTS

10.5k employees

We are a data and analytics company with 10,500 colleagues serving customers in more than 150 countries.

We serve Lawyers, Solicitors, Barristers, Judges, In-House Counsel Company Secretaries and GRC professionals, globally.

1.8k technologists

We have more than 1,800 technologists with advanced technology skills working in our local innovation centers around the world.

2.5pb Content

Our global content collection contains roughly 2.5 petabytes of data, which is 150x the size of Wikipedia.

144b documents

Our global legal and news database contains 144 billion documents and records with 1.2 million new legal documents added daily.

39k sources

Nexis news and business content includes over 39,000 premium sources in 45 languages, covering more than 180 countries. It has data including 500 million company profiles with a content archive that dates back 45 years.

293m dockets

LexisNexis content includes more than 293 million court dockets and documents, over 159 million patent documents, 4.25 million State Trial Orders, and 1.45 million jury verdict and settlement documents.

144m patent doc's

PatentSight includes objective ratings of the innovative strength (Patent Asset Index) of more than 144 million patent documents from more than 100 countries.

55k News Articles

In 2022, Law360 produced over 55,000 news and analysis articles. Legal analytics tool Lex Machina has normalized over 102 million counsel mentions and over 54 million party mentions since 2016.

Rule of Law

LexisNexis Legal & Professional is a leading global provider of information and analytics that enable professionals in legal, corporate, government and non-profit organisations to improve decision-making and achieve better business outcomes.

WE HELP YOU ON YOUR PATH TO COMPLIANCE

Action Oriented and Practical

→ Easy-to-navigate topics, organised by operational business processes.

→ Provides guidance in easy-to-understand business English.

→ Practical Tools include guidance notes, checklists and more.

Regulatory Alerts

→ Alerts customers to changes, and how these changes impact an organisation's legal responsibilities.

→ 3 types of Alerts- FYI, Action Required and News

Legal Registers

→ WHAT are my responsibilities?

→ WHAT do I need to do?

→ HOW do I do it?

→ WHAT are the legal consequences?

→ WHERE can I get more information?

Expert Authorship

→ We use leading local and international legal and industry experts to interpret all the relevant legislative and regulatory materials.

→ Provides significant savings in research time and cost.
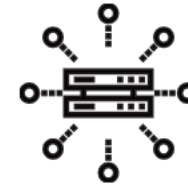
Technology Options

→ Content is imported into your existing GRC / ERM system via our API.

→ We work with a panel of carefully selected software partners to ensure that we can offer a complete package of content and software.

SOCI Regulation at a High Level

The 2023 Critical Infrastructure Resilience Strategy defines *critical infrastructure* as:

Those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.

The *Security of Critical Infrastructure Act 2018* (Cth) (SOCI) defines each class of critical infrastructure asset. A single critical infrastructure asset includes multiple parts which function together as a system or network. This includes premises, computers, and data.

SOCI LEGISLATION AT A HIGH LEVEL

SOCI has undergone extensive changes since its inception in 2018 - first in 2021 when critical infrastructure increased from 4 sectors to 11 sectors and 22 asset classes, and then in 2022 when risk management program obligations were added.
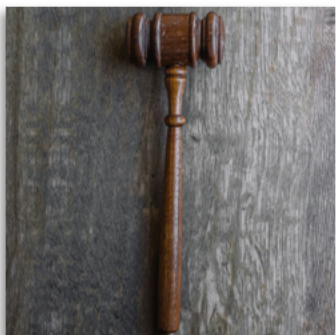
Effective DEC 2021

Security Legislation Amendment (Critical Infrastructure) Act 2021

Expands Sectors:
- *New government assistance obligations*
- *Provide notice of any cybersecurity incident w impact on CI assets*

Effective APR 2022

Security Legislation Amendment (Critical Infrastructure Protection) Act 2022

Responsible entities to create/maintain critical infrastructure risk management program

Enhanced cybersecurity obligations for operators of systems of national significance

Rules

Security of Critical Infrastructure (Definitions) Rules 2021/ (Application) Rules 2022

Requirements

Risk Management Program (CIRMP)

WHERE CHANGE IS HAPPENING

SOCI OUTLINES:

→ **The legal obligations you have if you own, operate, or have direct interests in critical infrastructure assets**

→ **How the government can support you if an incident occurs that impacts your critical infrastructure asset**

SOCI OBLIGATIONS

PROVIDE

... operational and ownership information to the Register of Critical Infrastructure Assets

REPORT

... cyber incidents which impact the delivery of essential services to the Australian Cyber

ADOPT

... maintain and comply with a written risk management program

For assets deemed as Systems of National Significance Enhanced Cyber Security Obligations (ECSO)

» Develop cyber security incident response plans to prepare for a cyber security incident.

» Undertake cyber security exercises to build cyber preparedness.

» Undertake vulnerability assessments to identify vulnerabilities for remediation.

» Provide system information to develop and maintain a near real-time threat picture.

SOCI DISCLOSURE

WHERE CHANGE IS HAPPENING

GOVERNMENT ASSISTANCE

The SOCI Act also includes government assistance measures, which outline how the government can help industry respond to cyber security incidents.

These measures apply only to incidents that will cause serious harm to Australia's prosperity, national security, or defence.

CRITICAL INFRASTRUCTURE ASSETS

The SOCI Act protects information about critical infrastructure assets.

It is an offence to disclose information about these assets, even if you are a responsible entity, unless your disclosure complies with the SOCI Act.

What You Need to Do to Prepare

Critical Infrastructure Risk Management Programs

The responsible entities are required to adopt, maintain and comply with a critical infrastructure risk management program (CIRMP) by 18 August 2023.

The **CIRMP** is an 'all-hazards' risk management program and must, for each critical infrastructure asset the responsible entity is responsible for:

→ **identify each hazard**

→ **minimise or eliminate any material risk of such a hazard occurring; and**

→ **mitigate the relevant impact of such a hazard on the asset.**

2024
AUG
18

Responsible entities will need to demonstrate compliance with a designated cyber security framework or equivalent (Australian Standard AS ISO/IEC 27001:2015, Essential Eight, NIST's Framework for Improving Critical Infrastructure Cybersecurity, US Dept. Energy's Cybersecurity Capability Maturity Model or AEMO's The 2020-21 AESCSF Framework Core).

Critical Infrastructure Risk Management Programs

CISC to commence compliance activities in FY24-25, particularly in relation to:

→ the Register of Critical Infrastructure Assets reporting obligation;
→ the mandatory cyber security incident notification obligation;
→ the CIRMP obligations; and
→ notification obligations in relation to data storage or processing providers.

2024

SEP

28

First annual report on CIRMPs due

Changes in Contemplation

2024

MAR

1

Submissions on the proposed changes outlined in the Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (Consultation Paper) closed on 1 March 2024.

The Australian Government is seeking feedback on 9 proposed legislative measures outlined in the Consultation Paper, being:

1. Mandatory standard for consumer-grade Internet of Things (IoT) technology
2. No-fault ransomware reporting obligations
3. Limited use for information shared with ASD and the Cyber Coordinator
4. A Cyber Incident Review Board to conduct no-fault reviews of incidents
5. Clarifying SOCI Act obligations for data storage systems for business1critical data
6. Last resort consequence management powers for the Minister of Home Affairs
7. Amending protected information provisions to enable information sharing with government
8. Powers to remedy serious deficiencies in risk management programs
9. Consolidating telecommunications security requirements under the SOCI Act.

SOCI: Change is inevitable

Cyber Security Legislative Reforms

Consultation on proposed new cyber security legislation and on changes to the Security of Critical Infrastructure Act 2018

How to engage us

Consultations

Contracts and tenders

Industry engagement

Committees and fora

The protection of our cyber security and critical infrastructure is vital to Australia's national security and economic stability.

Increasing connectivity brings great benefits, but also great risk. Today, a cyber incident can spread instantaneously, disrupting interconnected systems and networks across the economy.

Such incidents have affected many ... lessons learned from them.

Australian Government Doubles Down On Cybersecurity in Wake of Major Attacks

Government proposes more modern and comprehensive cybersecurity regulations for businesses, government, and critical infrastructures providers Down Under.

John Leyden, Contributing Writer
March 27, 2024

5 Min Read

...essing gaps in existing cybercrime laws, Australian legislators hope to ...try's Security of Critical Infrastructure (SOCI) Act 2018 to place a greater ...eat prevention, information sharing, and cyber incident response.

Labor plan would give home affairs minister powers over critical infrastructure during cyber-attacks

Clare O'Neil releases consultation paper on new cybersecurity legislation, which proposes changes to Security of Critical Infrastructure Act

Get our morning and afternoon news emails, free app or daily news podcast

SOCI: Change is inevitable

Greater Internal Controls Required

- Increased Requirements to protect data storage systems that store business critical data
- Increased Cyber controls as new threats emerge

Greater Power for Minister of Home Affairs

- Introducing 'last resort consequence' management power for the Minister of Home Affairs to provide directions to critical infrastructure entity in event of incidents
- Providing a power for the Secretary of Home Affairs or the "relevant Commonwealth regulator" to direct a critical infrastructure entity to address deficiencies in its risk management program

Legislation Consolidation

- Consolidating telecommunications security requirements under the SOCI Act.
- Simplifying information sharing to make it easier for critical infrastructure entities to respond to high-risk, time-sensitive incidents

Source
- 2023-2030 Australian Cyber Security Strategy
- Australian Cyber Security Strategy: Cyber Security Legislative Reforms | Consultation Paper

SOCI: Managing Change

Identify Changes

Change Assessments

Implement Management Systems

LexisNexis®

ReadiNow

Change Alerts	**Obligation Management**
Assessment & Controls	**Reporting**

Demo of ReadiNow. Please watch the full webinar recording to view.

SOCI: Managing Change

Identify Changes

Change Assessments

Implement Management Systems

NEWS

Australian Government

LexisNexis®

ReadiNow

Change Alerts	Obligation Management
Assessment & Controls	Reporting

SOCI: Managing Change

Identify Changes

Change Assessments

Implement Management Systems

LexisNexis®

ReadiNow

| Change Alerts | Obligation Management |
| Assessment & Controls | Reporting |

Critical Infrastructure Register

Critical Infrastructure Risk Management

Vulnerability Management

Cyber Incident Management

Solutions

Governance, Risk & Compliance

BCM

Risk

Compliance

Audit

Incident

WHS

Vendor

Complaints

Key Indicators

IT/Cyber Solutions

IT Risk

IT Incident

ITDR

IT Compliance

Environment, Social & Governance

Materiality Assessments

Disclosure

Metrics

+ Any custom Use Case Applications

Framework Specific

CPS230

SOCI

Configurable Forms & Screens

Dashboards

Analytics

Workflow

Mobile

Role Based Security

Document Generation

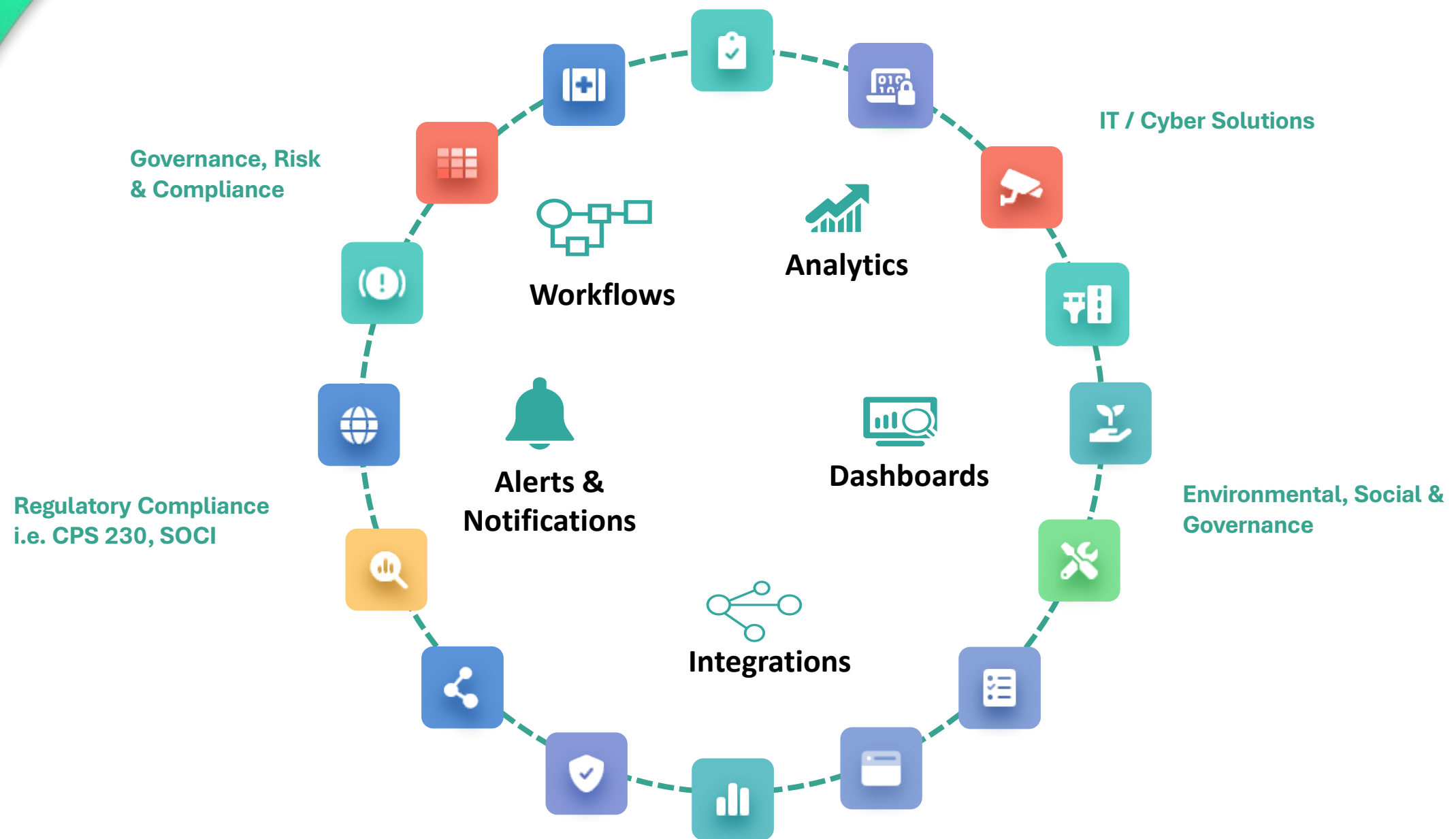Alerts & Notifications

Integrations

Workflows

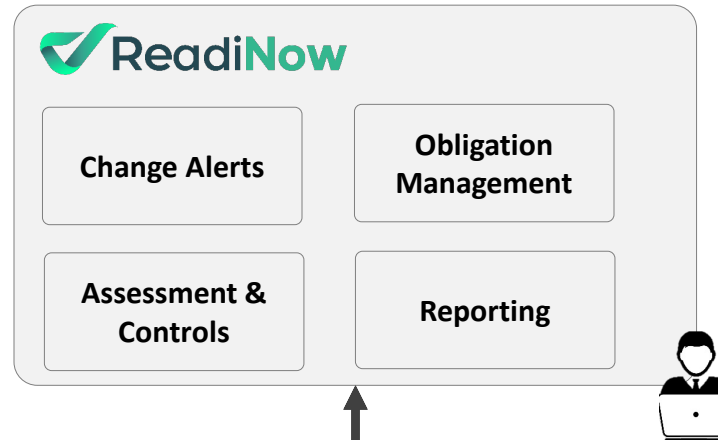Analytics

Alerts & Notifications

Dashboards

Integrations

Governance, Risk & Compliance

IT / Cyber Solutions

Regulatory Compliance i.e. CPS 230, SOCI

Environmental, Social & Governance

SOCI: Managing Change

Identify Changes

Change Assessments

Implement Management Systems

LexisNexis®

ReadiNow

| Change Alerts | Obligation Management |
| Assessment & Controls | Reporting |

Critical Infrastructure Register

Critical Infrastructure Risk Management

Vulnerability Management

Cyber Incident Management

SOCI: Managing Change

Executive Dashboard that covers key SOCI metrics including

- Critical Infrastructure Register
- Incident Management
- Vulnerability Management
- Obligation Management
- Notifications

Critical Infrastructure Register

Critical Infrastructure Risk Management

Vulnerability Management

Cyber Incident Management
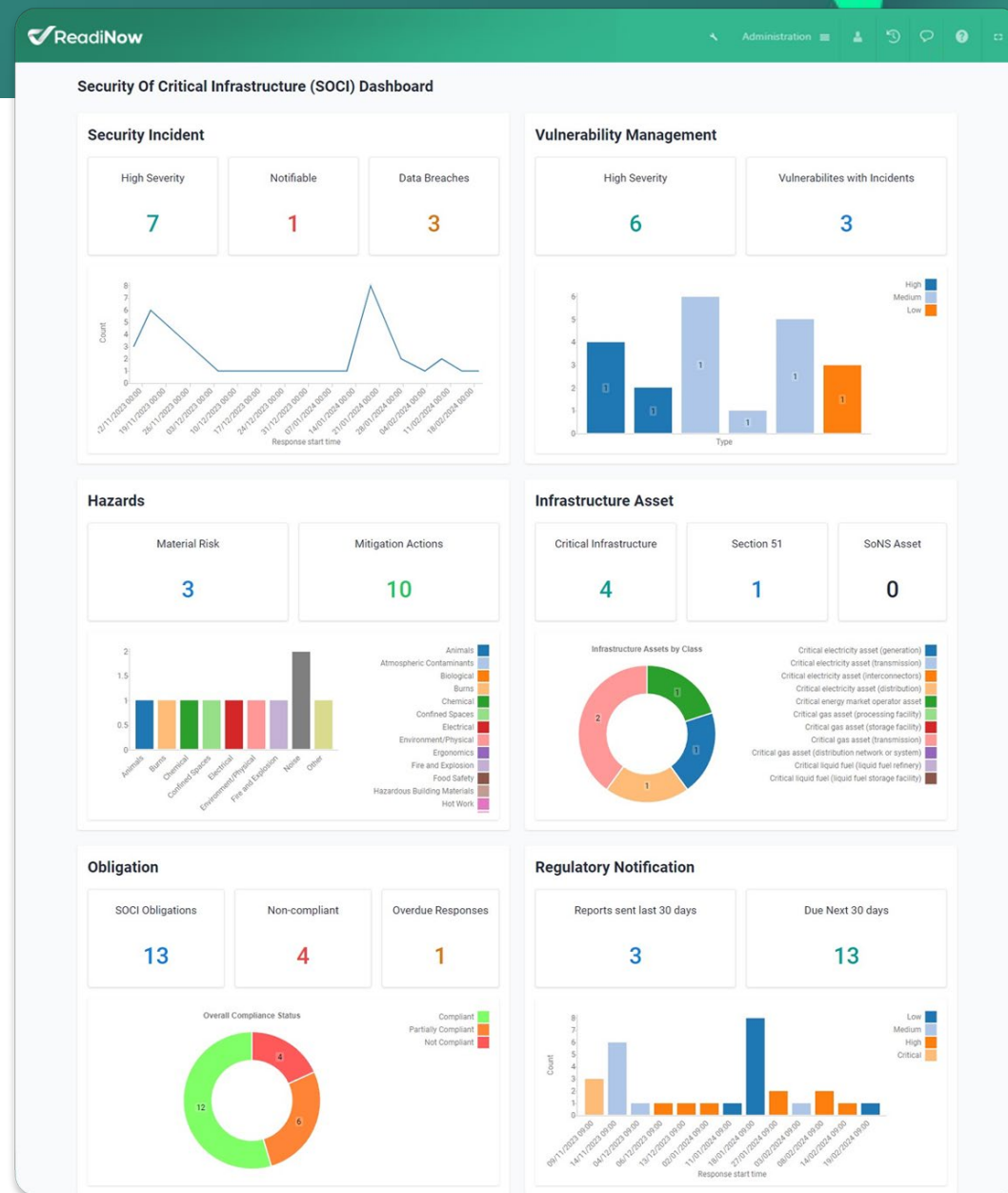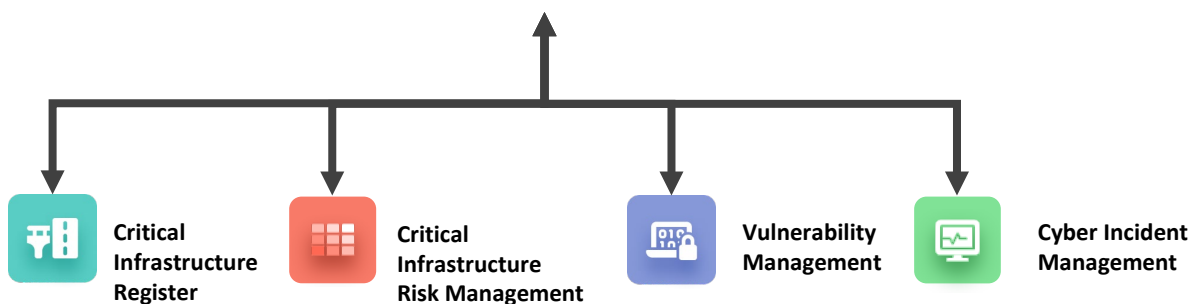
Demo of ReadiNow. Please watch the full webinar recording to view.

Leveraging AI for SOCI Compliance

Understanding AI types

Identifying use cases

Key considerations & Implications

Determining technology

Understanding AI Types

Generative AI

📷 Text Generation

🎙 Audio Generation

🎧 Audio to text

📱 Image Generation

Predictive AI

✓ Predictive Models

🏅 Image Recognition

🎥 Video Recognition

Understanding AI Types

Text Generation

- Generation of Risk Descriptions
- Creation of Risk Reports
- Automated report creation for compliance audits.
- Generating policy and procedure drafts based on regulations.
- Creation of regulatory update summaries.
- Drafting risk management strategies.
- Automatic generation of meeting minutes for GRC committee meetings.
- Summarizing risk assessment findings.
- Generation of risk-based scenarios for testing.

Audio Generation

- Voice-based alerts for compliance breaches.
- Customized audio instructions for employees during compliance training.
- AI-generated advisories for stakeholders.
- Audio summaries of regulatory changes.
- Voice prompts for guided risk assessments.
- Simulation sounds for risk scenarios.
- Automated voice messages for incident reporting.

Audio to text

- Transcription of GRC committee meetings.
- Automated transcription of whistleblower recordings.
- Converting recorded interviews during audits into text.
- Documentation of verbal agreements or understandings.

Predictive Models

- Predicting potential areas of non-compliance.
- Forecasting risk trends.
- Predictive analysis for fraud detection.
- Forecasting regulatory changes based on historical data.
- Modeling potential impacts of risks on organizational objectives.
- Estimating potential financial penalties for non-compliance.

Image Recognition

- Scanning documents for confidential information.
- Verifying authenticity of documents during audits.
- Recognition and tagging of GRC-related assets in images.
- Analyzing workplace images for safety or compliance violations.
- Identifying unauthorized printed materials in secure zones.
- Automating the categorization of paper-based records.
- Scanning images for potential cyber threats.

Video Recognition

- Monitoring facility videos for compliance with safety standards.
- Analyzing behavior patterns for fraud detection.

Implementing AI in SOCI Use Cases

AI Suggestions/Generative

- Suggesting Controls/Risk Treatment Plans

- Suggesting actions to take post incident

- Drafting Risk Reports

- Automated creation for compliance

  audits.

- Summarizing Incident findings.
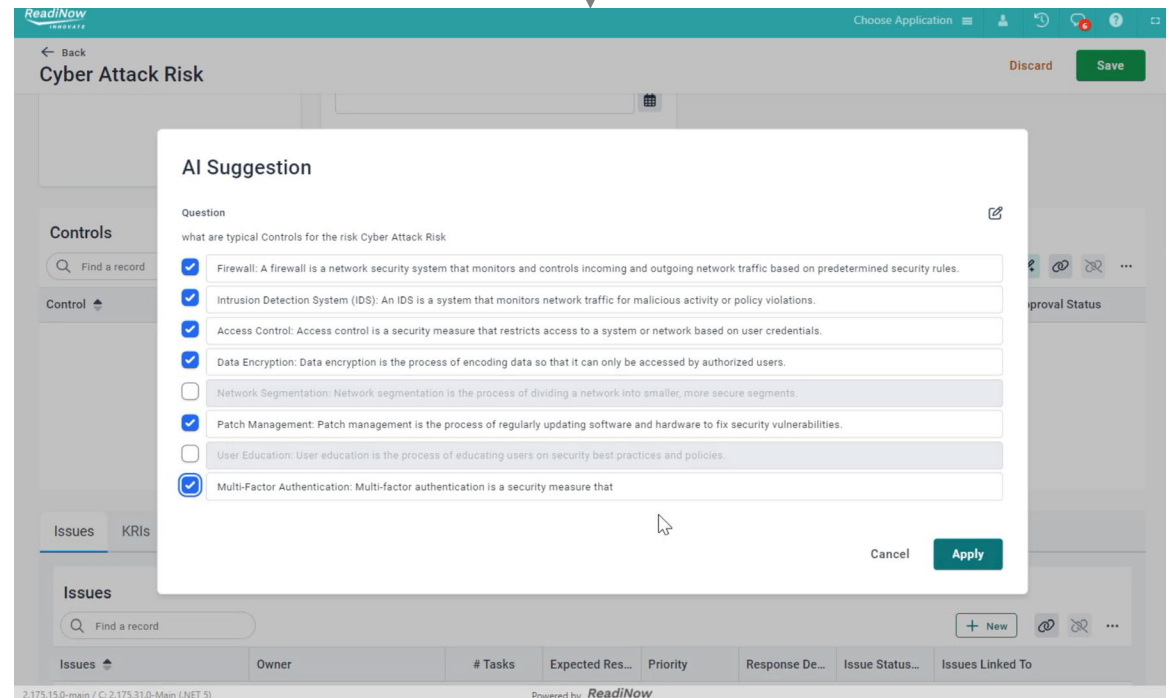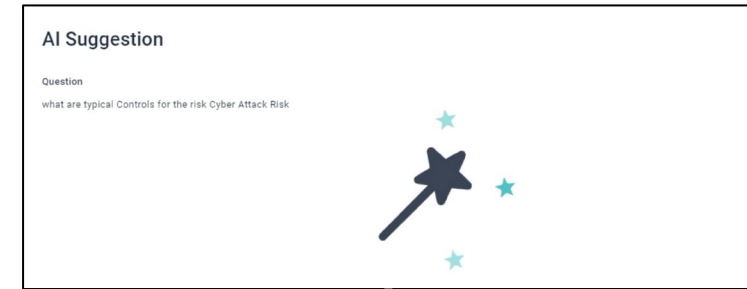
Implementing AI in SOCI Use Cases

AI Scanning/Pattern Finding

- Automated Vulnerability Scanning

- Pattern recognition in network traffic

- Forensic Analysis for Incident Investigation

- Identifying security configuration anomalies

- Risk concentrations

Implementing AI in SOCI Use Cases

AI Predictive Analytics

- Predictive vulnerability identification

- Risk Trending/Forecasting

- Predictive threat intelligence

- Compliance Risk Analysis
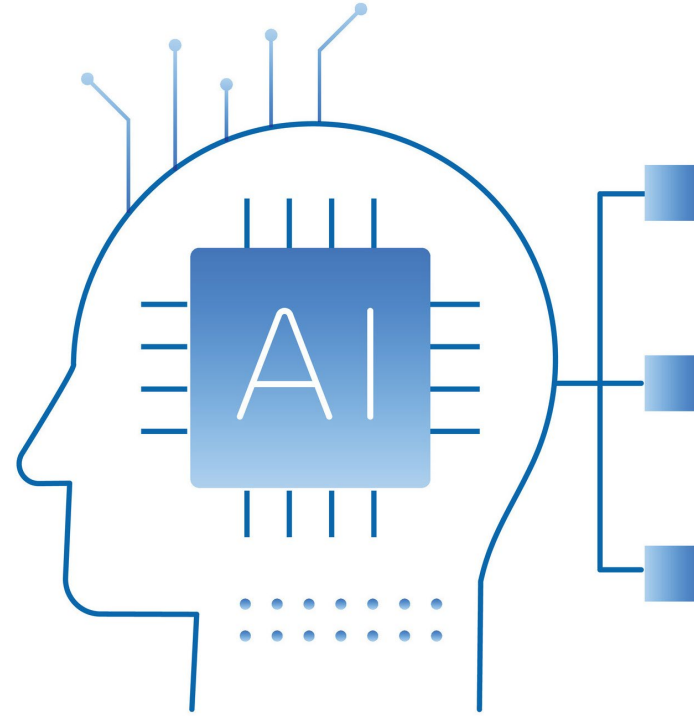
Key Considerations & Implications

Security/Data Privacy

Accuracy/Bias

Data Quality

Resources

Process Maturity

Webinar:
SOCl in 2024: Leveraging AI to Streamline Compliance

Questions

Feedback Form
Please complete the
30 second feedback form

ReadiNow   LexisNexis | *Regulatory Compliance*

Thanks for joining us!

Learn more about ReadiNow's dedicated SOCI Module: