CASE STUDY

encasedIT by WG

WG Advisory is revolutionizing the IT consulting industry with **encasedIT™**, a first of its kind dynamic platform built on modern-cloud architecture and flexible infrastructure providing scalability and reliability.

Our cybersecurity module enables school boards to utilize industry-leading frameworks, such as **NIST CSF v2** and **CIS-18**, to develop and manage robust cybersecurity programs that would otherwise be impossible with limited budgets and resources. The single-pane-of-glass dashboard supports data-driven roadmaps and trend analysis, empowering technology-centric initiatives.

*"With **encasedIT™**, we can highlight risks, gaps, and actionable tasks which is exactly what we need to inform the Board and senior management, ensuring we implement the controls and tools that align with our strategic initiative."*

- Brian Whitelaw, CISM, CRISC, CGEIT

Cybersecurity Program Management in Canadian School Boards: Enabling Desired Outcomes

Far too many school boards buy cybersecurity tools without defining accountability and objectives.

This has created a funding crisis where security leaders are left pleading for budgets to acquire technology that merely fulfills "check-box" compliance. Consequently, a culture of reactive, "ad hoc" measures has emerged, aimed solely at safeguarding the infrastructure.

In May of 2024, the Government of Ontario tabled Bill 194 which introduced the *Enhancing Digital Security and Trust Act*, 2024 (the EDST Act or EDSTA), and amendments to Ontario's long-standing public sector privacy law, the *Freedom of Information and Protection of Privacy Act* (FIPPA). The EDST Act will apply across the provincial and municipal public sectors, including school boards, school authorities, children's aid societies, colleges, universities and hospitals.

The legislation introduces several provisions expected to be included in the scope and implementation of cybersecurity initiatives. These provisions require public sector entities to develop and implement comprehensive cybersecurity programs, designate specific individuals responsible for cybersecurity, establish incident response and recovery plans, implement oversight and metrics, and submit regular progress reports on these efforts.

In a school board, system downtime directly correlates with learning loss, prompting boards to consider paying million-dollar ransoms to restore online learning programs. Regardless of mandates, school boards need mature and manageable cybersecurity programs.

This case study illustrates how a Canadian School Board leveraged **encasedIT™** to develop a cybersecurity program built upon three fundamental principles:

1. The program must follow leading cybersecurity frameworks like NIST, CIST-18, ISO 27001
2. The program takes a "strategy first, tools second" approach
3. The program must deliver actionable roadmaps that align with budget and resource constraints

Tackling Cybersecurity in Education

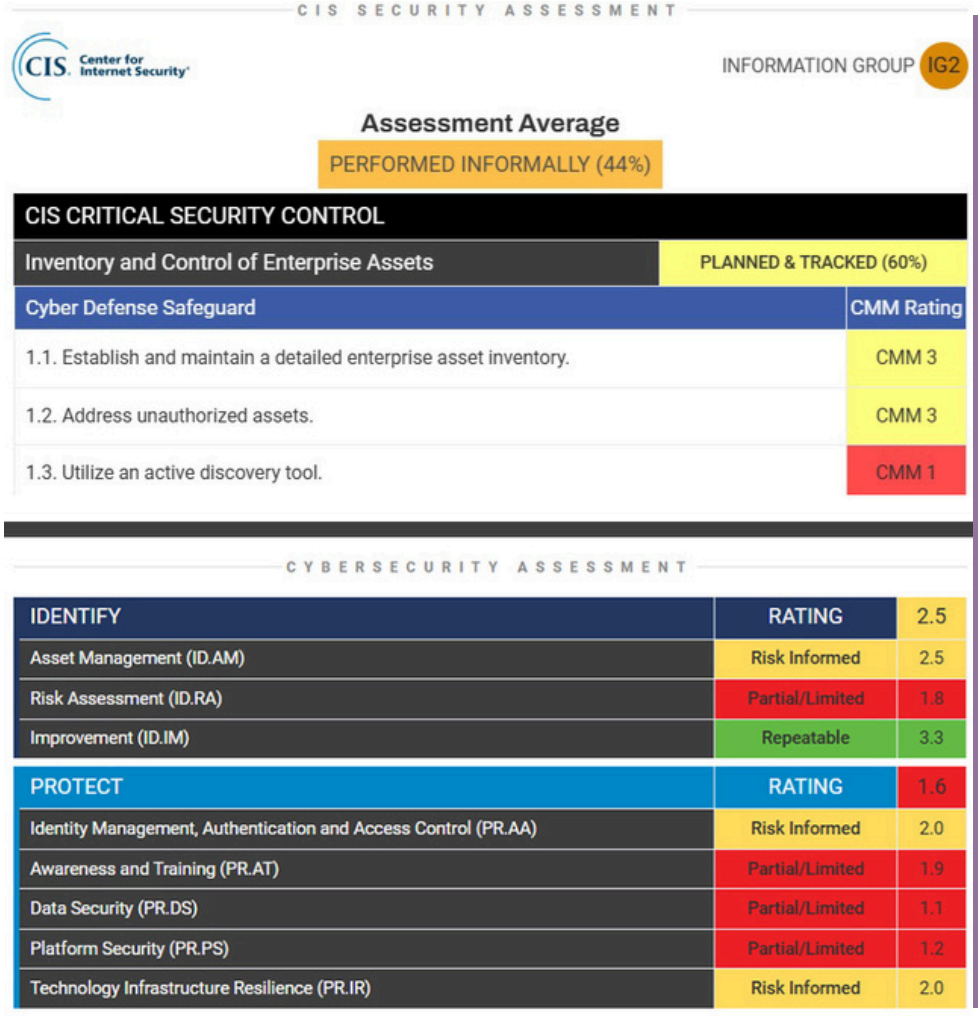
School boards are facing an alarming rise in cyberattacks, with record increases reported. According to Securin research, over the past three years, 50% of cyberattacks targeting educational institutions have "spiraled into full-blown ransomware attacks that have led to prolonged operational shutdowns, significant financial losses, and a growing distrust in the education system's cybersecurity defenses."

CHALLENGES

1. Boards often lack cybersecurity expertise, making oversight difficult
2. Limited resources hinder effective allocation of staff and budget to address security threats
3. The proliferation of data within educational institutions is simply too much to manage
4. Lack of visibility and understanding around cloud security has a negative impact on risk management

Approach

Selecting a respected framework and knowing when/how to effectively apply it to your organization is a critical first step. For school boards, an approach supported by **encasedIT** is to consider leveraging both NIST CSF v2 and CIS-18 controls as part of the cybersecurity program.



CIS SECURITY ASSESSMENT

CIS Center for Internet Security

INFORMATION GROUP IG2

Assessment Average

PERFORMED INFORMALLY (44%)

CIS CRITICAL SECURITY CONTROL	
Inventory and Control of Enterprise Assets	PLANNED & TRACKED (60%)
Cyber Defense Safeguard	**CMM Rating**
1.1. Establish and maintain a detailed enterprise asset inventory.	CMM 3
1.2. Address unauthorized assets.	CMM 3
1.3. Utilize an active discovery tool.	CMM 1

CYBERSECURITY ASSESSMENT

IDENTIFY	RATING	2.5
Asset Management (ID.AM)	Risk Informed	2.5
Risk Assessment (ID.RA)	Partial/Limited	1.8
Improvement (ID.IM)	Repeatable	3.3
PROTECT	**RATING**	**1.6**
Identity Management, Authentication and Access Control (PR.AA)	Risk Informed	2.0
Awareness and Training (PR.AT)	Partial/Limited	1.9
Data Security (PR.DS)	Partial/Limited	1.1
Platform Security (PR.PS)	Partial/Limited	1.2
Technology Infrastructure Resilience (PR.IR)	Risk Informed	2.0

CIS-18 is a good choice for organizations that want to quickly implement practical security controls.

CIS-18 provides guidance to prioritize the implementation of CIS Controls in an effort to assist enterprises of every size.

NIST CSV v2 brings a range of benefits to boards of all sizes.

NIST CSV v2 demonstrates that cybersecurity is no longer an IT problem — but an organization-wide problem that requires input from management and boards

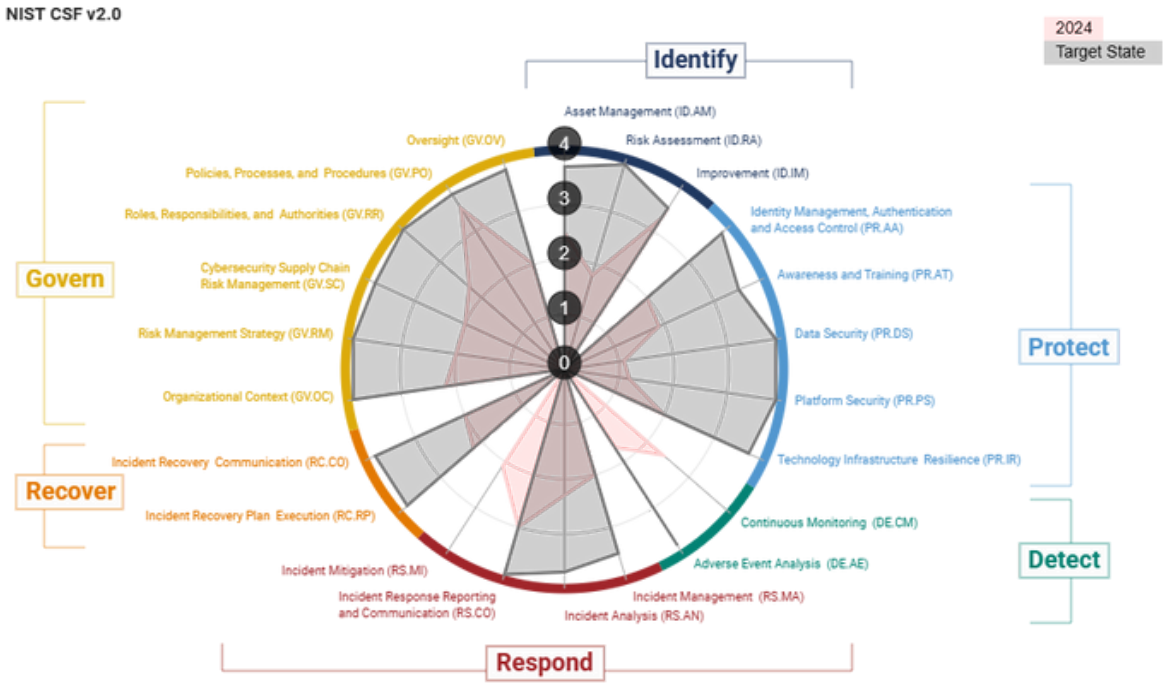
CIS controls are cross-compatible by design, so boards can adapt to meet CIS controls while working on meeting NIST CSF standards—both frameworks are fully integrated into the **encasedIT**™ platform.

Underpin Cybersecurity Programs with Trend Analysis Graphs and Roadmaps

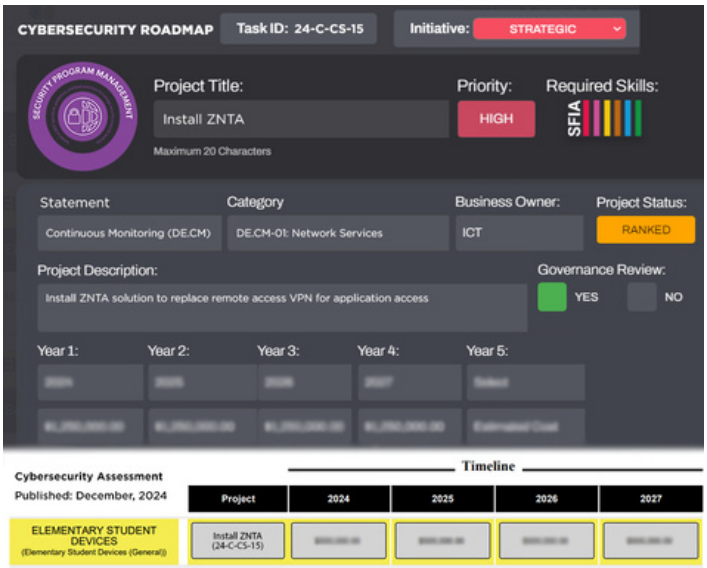
Cybersecurity program management faces several challenges including, scope planning, continuous learning, risk management, and overall program delivery. Effective cybersecurity programs require the development of comprehensive policies and procedures.

encasedIT™ creates a detailed project roadmap that breaks down each initiative into manageable tasks that can be tracked using the integrated project management dashboard.

Multiple Cybersecurity Frameworks for School Boards of All Sizes



Dynamic spider graphs allow the board to track progress and set target states for both NIST CSF v2 and CIS-18 assessments.



SFIA Skills Framework Integration
Users can add required skills for project delivery by integrating with the SFIA framework.

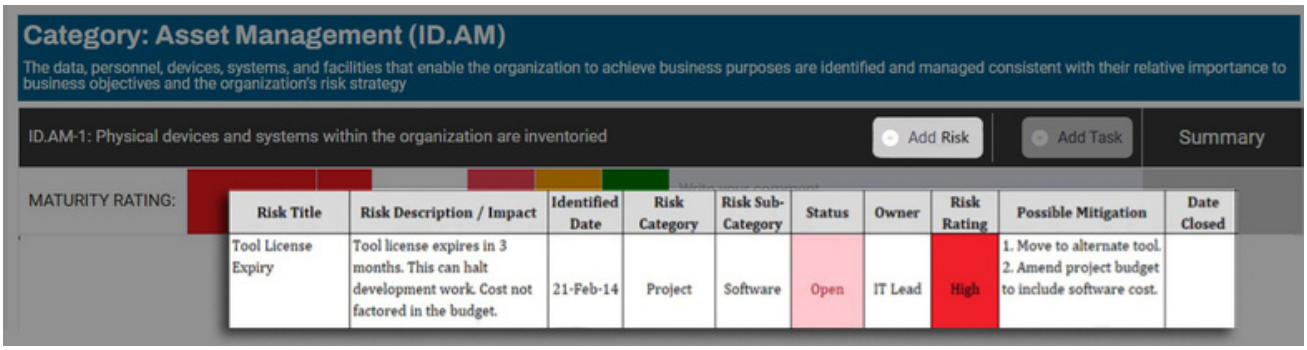
Single Pane-of-Glass Dashboard
Manage the entire cybersecurity roadmap effortlessly with a unified dashboard.

Outcomes & Benefits

The combination of "risk" and "maturity" within **encasedIT™** allows school boards to manage cybersecurity risks in a dynamic register and conduct periodic updates that generate maturity trend analysis graphs. This innovative approach eliminates the need for cumbersome, outdated spreadsheets and other inefficient methods typically used to manage risk, streamlining the process and enabling school boards to focus on proactive cybersecurity strategies.

This interactive approach ensures risk management remains dynamic, rather than a static process that often results in outdated, inaccurate data. By providing real-time insights and trend analysis, **encasedIT™** fosters a more responsive and informed decision-making environment, ultimately enhancing the overall security posture of the institution.

Risk Management and Maturity Tracking



Dynamic Trend Analysis Visualization
Shows current posture and desired target state.

Periodic Updates
Track progress towards the target state with regular updates.

Downloadable Visuals
Illustrate progress with downloadable visuals for senior leadership.

Who We Are

Technology without business application has no value.

In 2019, WG Advisory started the development of **encasedIT™** as a way to underpin the collaboration between business and information technology. We continue to unlock capabilities that include a live interactive dashboard acting as the central gateway to your organization's IT management program. Dynamic roadmaps, trend analysis graphs, and formal project governance tools provide IT leaders with the insight and vision required to keep up with the continued acceleration of digital transformation.

We ensure projects move from concept to completion.

CONTACT US: info@wgadvisory.ca | www.wgadvisory.ca

What We Do

Capabilities of **encasedIT™** include:

- IT Strategic Planning Developed on a Customizable Framework
- Business Continuity & Disaster Recovery Program Management
- Cybersecurity Program Management Built on NIST CSF v2
- IT Skills Framework Built on SFIA v9
- Cloud Maturity Assessments
- Information Management Maturity Assessments
- IT Maturity Risk Assessments
- Single Pane of Glass Dashboard Includes Roadmaps & Project Governance
- Intake for All Modules and Assessments

Created in partnership with The Arc Narrative
marketing@thearcnarrative.com