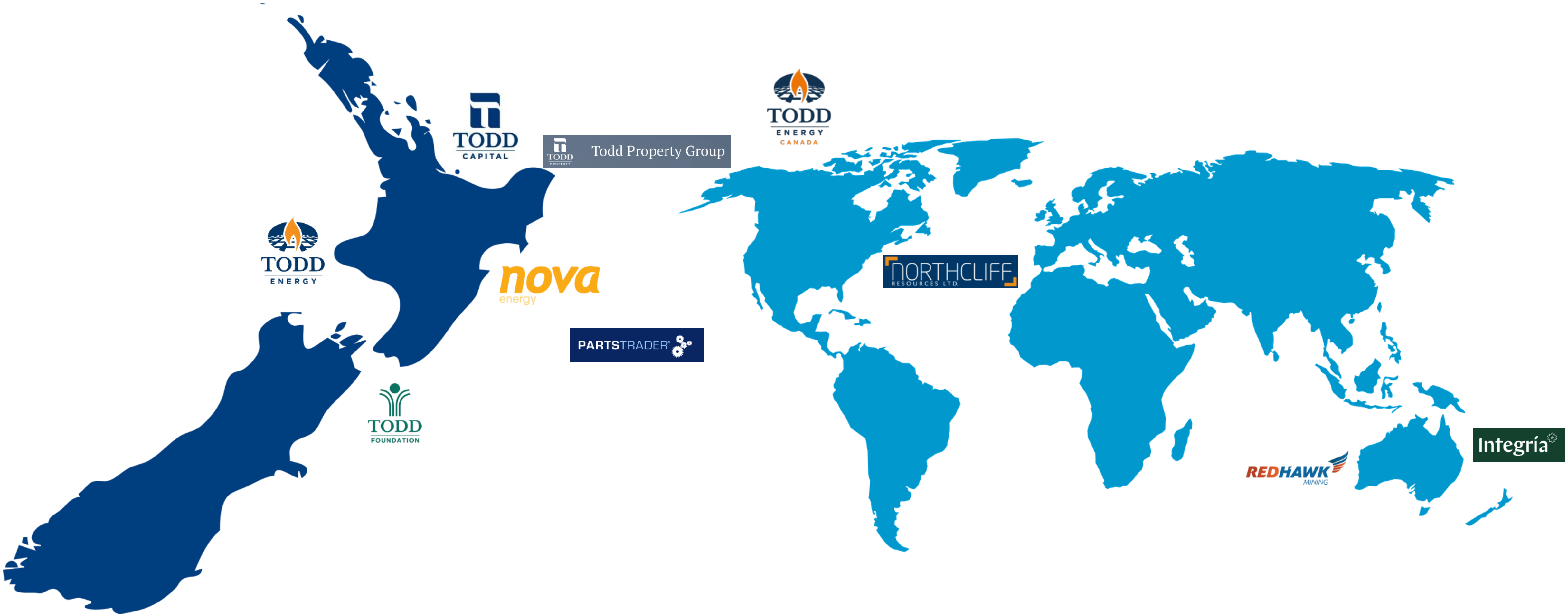
TLP: AMBER

Todd Corporation



Operational Technology (OT) vs. Information Technology (IT)

OT - Programmable systems or devices that interact with the physical environment (or mange devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or controls of devices, processes, and events

Examples include: Safety Instrumented Systems (SIS), process control systems etc.

IT - Any services, equipment, or interconnected system(s) or subsystem(s), of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management movement, control, display, switching, interchange transmission, or reception of data or information

NIST Computer Security Resource Center - https://csrc.nist.gov/glossary

TLP: AMBER

15
22
25
25
29
9.

Recipe for Cybersecurity Program Success

TODD CORPORATION

Serves

Your Entire Organisation

Prep Time

Continuous Improvement

Top 5 Ingredients

1. Asset Management
2. Vulnerability and Patch Management
3. Continuous Monitoring and Threat Intelligence
4. Defence in Depth
5. Incident Response Planning

Ingredient 1 - External Audits

Start with a foundation of independent external audits to validate the effectiveness of your security measures and identify areas for improvement.

Self audit is a great pulse check, but a sole reliance is an issue:

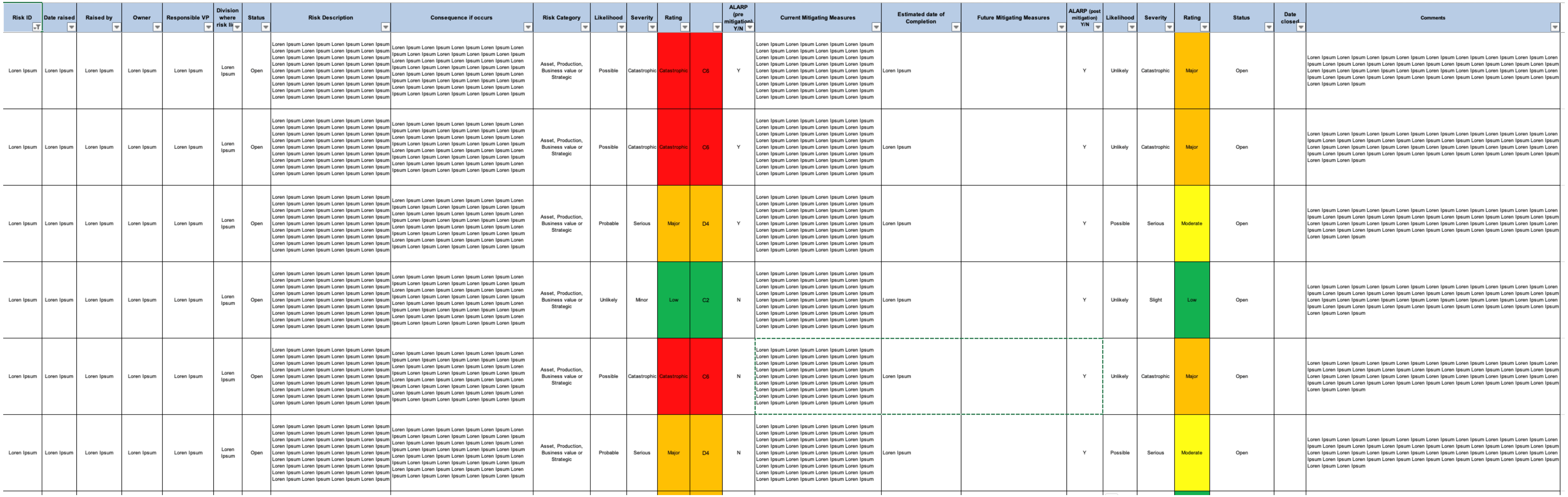
1. Lack of Objectivity
2. Conflict of Interest
3. Conflict of Interest
4. Limited Perspective
5. Overlooking Compliance Issues

External audits have their advantages:

1. Objective and Unbiased Evaluation
2. Enhanced Credibility with Stakeholders
3. Assurance of Regulatory Compliance
4. Identification of Risks and Weaknesses
5. Recommendations for Process Improvements

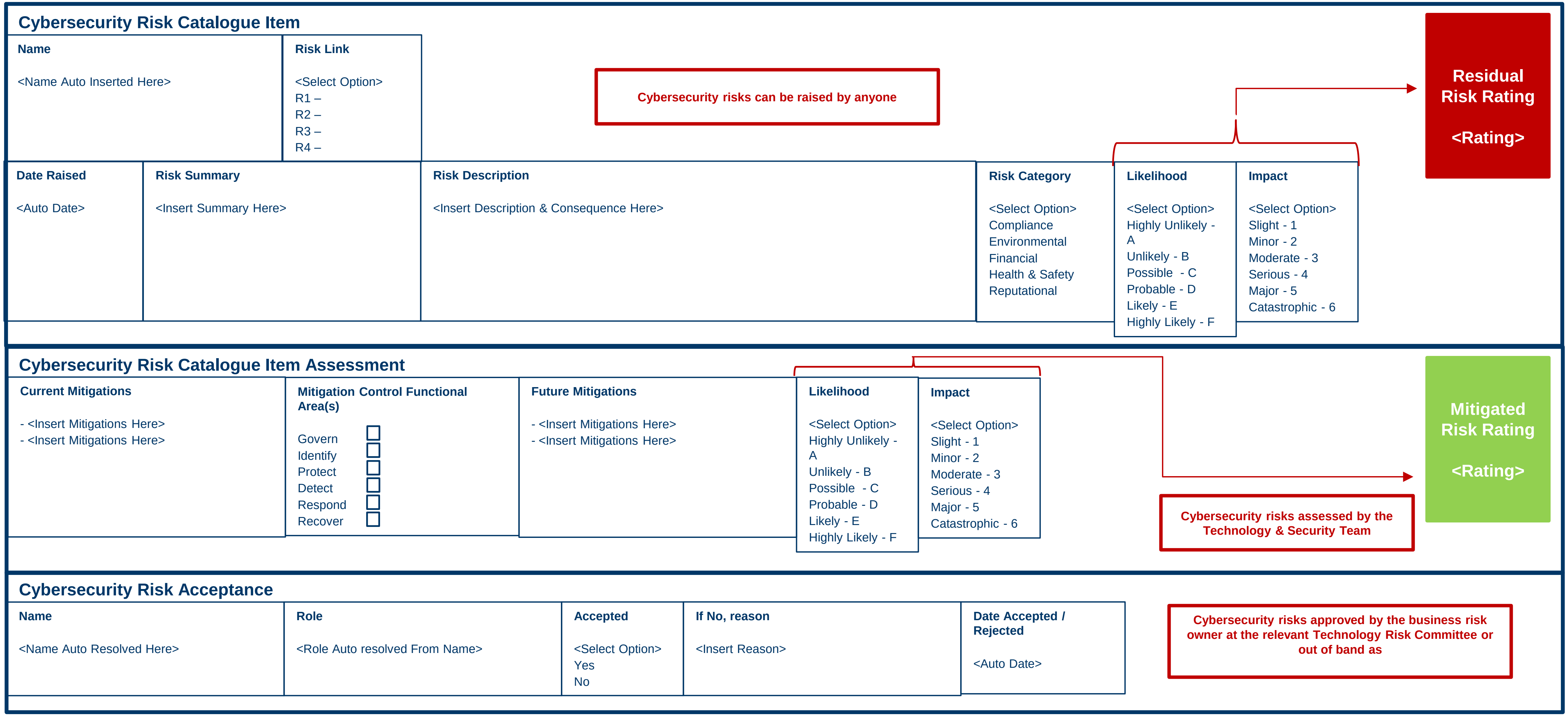
Ingredient 2 - Risk Assessment

Add a structured risk assessment process to identify, evaluate, and prioritise risks based on potential impact and likelihood.



Risk ID	Date raised	Raised by	Owner	Responsible VP	Division where risk li	Status	Risk Description	Consequence if occurs	Risk Category	Likelihood	Severity	Rating		ALARP (pre mitigation) Y/N	Current Mitigating Measures	Estimated date of Completion	Future Mitigating Measures	ALARP (post mitigation) Y/N	Likelihood	Severity	Rating	Status	Date closed	Comments
Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Open	Loren Ipsum Loren Ipsum	Loren Ipsum Loren Ipsum	Asset, Production, Business value or Strategic	Possible	Catastrophic	Catastrophic	C6	Y	Loren Ipsum Loren Ipsum	Loren Ipsum		Y	Unlikely	Catastrophic	Major	Open		Loren Ipsum Loren Ipsum
Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Open	Loren Ipsum Loren Ipsum	Loren Ipsum Loren Ipsum	Asset, Production, Business value or Strategic	Possible	Catastrophic	Catastrophic	C6	Y	Loren Ipsum Loren Ipsum	Loren Ipsum		Y	Unlikely	Catastrophic	Major	Open		Loren Ipsum Loren Ipsum
Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Open	Loren Ipsum Loren Ipsum	Loren Ipsum Loren Ipsum	Asset, Production, Business value or Strategic	Probable	Serious	Major	D4	Y	Loren Ipsum Loren Ipsum	Loren Ipsum		Y	Possible	Serious	Moderate	Open		Loren Ipsum Loren Ipsum
Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Open	Loren Ipsum Loren Ipsum	Loren Ipsum Loren Ipsum	Asset, Production, Business value or Strategic	Unlikely	Minor	Low	C2	N	Loren Ipsum Loren Ipsum	Loren Ipsum		Y	Unlikely	Slight	Low	Open		Loren Ipsum Loren Ipsum
Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Open	Loren Ipsum Loren Ipsum	Loren Ipsum Loren Ipsum	Asset, Production, Business value or Strategic	Possible	Catastrophic	Catastrophic	C6	N	Loren Ipsum Loren Ipsum	Loren Ipsum		Y	Unlikely	Catastrophic	Major	Open		Loren Ipsum Loren Ipsum
Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Loren Ipsum	Open	Loren Ipsum Loren Ipsum	Loren Ipsum Loren Ipsum	Asset, Production, Business value or Strategic	Probable	Serious	Major	D4	N	Loren Ipsum Loren Ipsum	Loren Ipsum		Y	Possible	Serious	Moderate	Open		Loren Ipsum Loren Ipsum

Ingredient 2 - Cybersecurity Risk Catalogue User Interface



Cybersecurity Risk Catalogue Item

Name <Name Auto Inserted Here>	**Risk Link** <Select Option> R1 – R2 – R3 – R4 –

Date Raised <Auto Date>	**Risk Summary** <Insert Summary Here>	**Risk Description** <Insert Description & Consequence Here>	**Risk Category** <Select Option> Compliance Environmental Financial Health & Safety Reputational	**Likelihood** <Select Option> Highly Unlikely - A Unlikely - B Possible - C Probable - D Likely - E Highly Likely - F	**Impact** <Select Option> Slight - 1 Minor - 2 Moderate - 3 Serious - 4 Major - 5 Catastrophic - 6

Cybersecurity risks can be raised by anyone

Residual Risk Rating

<Rating>

Cybersecurity Risk Catalogue Item Assessment

Current Mitigations - <Insert Mitigations Here> - <Insert Mitigations Here>	**Mitigation Control Functional Area(s)** Govern □ Identify □ Protect □ Detect □ Respond □ Recover □	**Future Mitigations** - <Insert Mitigations Here> - <Insert Mitigations Here>	**Likelihood** <Select Option> Highly Unlikely - A Unlikely - B Possible - C Probable - D Likely - E Highly Likely - F	**Impact** <Select Option> Slight - 1 Minor - 2 Moderate - 3 Serious - 4 Major - 5 Catastrophic - 6

Mitigated Risk Rating

<Rating>

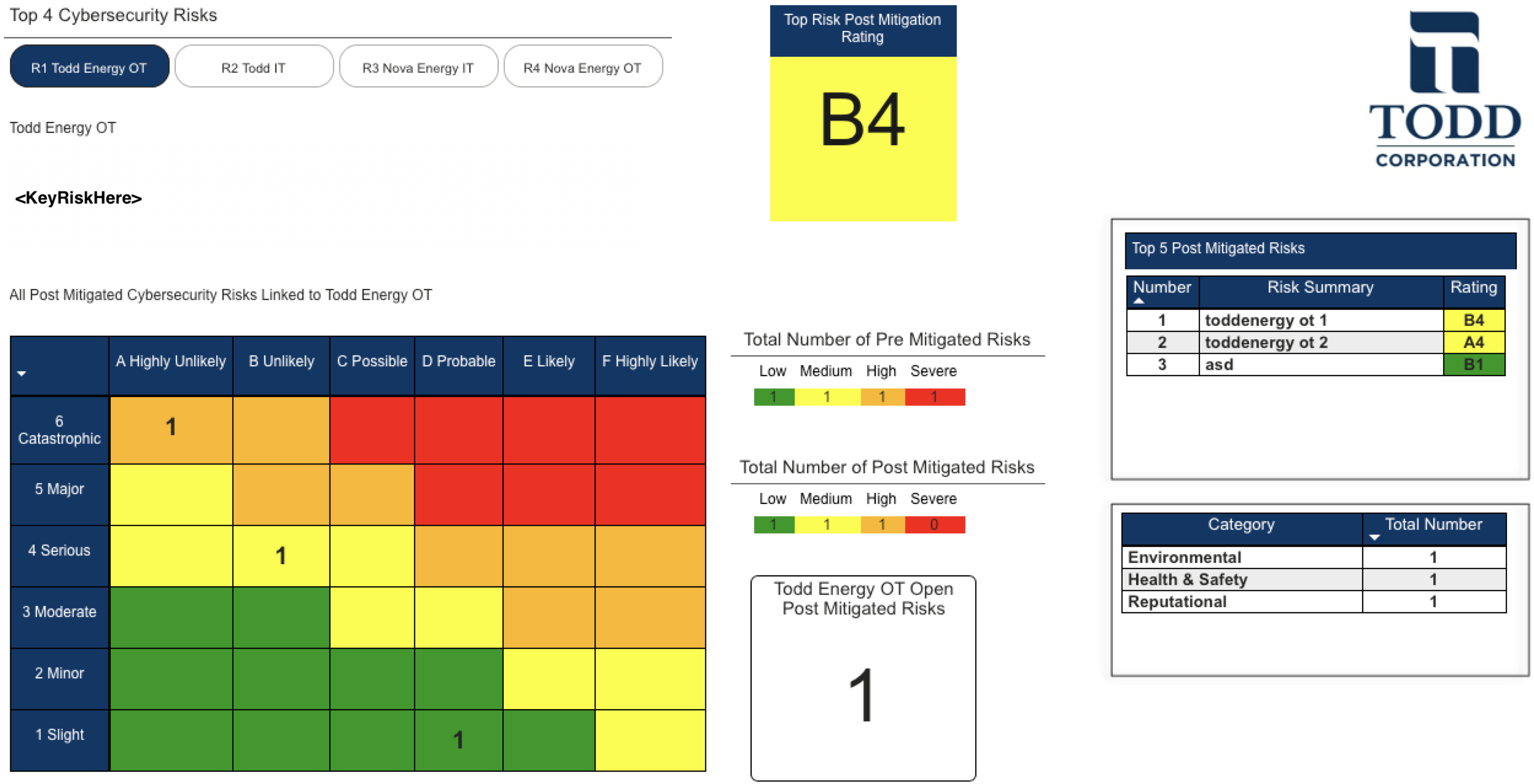
Cybersecurity risks assessed by the Technology & Security Team

Cybersecurity Risk Acceptance

Name <Name Auto Resolved Here>	**Role** <Role Auto resolved From Name>	**Accepted** <Select Option> Yes No	**If No, reason** <Insert Reason>	**Date Accepted / Rejected** <Auto Date>

Cybersecurity risks approved by the business risk owner at the relevant Technology Risk Committee or out of band as

Ingredient 2 - Cybersecurity Risks Dashboard(s)



Top 4 Cybersecurity Risks

Todd Energy OT

<KeyRiskHere>

Top Risk Post Mitigation Rating

B4

All Post Mitigated Cybersecurity Risks Linked to Todd Energy OT

▾	A Highly Unlikely	B Unlikely	C Possible	D Probable	E Likely	F Highly Likely
6 Catastrophic	🟧 1	🟧	🟥	🟥	🟥	🟥
5 Major	🟨	🟧	🟧	🟥	🟥	🟥
4 Serious	🟨	🟨 1	🟨	🟧	🟧	🟧
3 Moderate	🟩	🟩	🟨	🟨	🟧	🟧
2 Minor	🟩	🟩	🟩	🟩	🟨	🟨
1 Slight	🟩	🟩	🟩	🟩 1	🟩	🟨

Total Number of Pre Mitigated Risks

Low	Medium	High	Severe
1	1	1	1

Total Number of Post Mitigated Risks

Low	Medium	High	Severe
1	1	1	0

Todd Energy OT Open Post Mitigated Risks

1

Top 5 Post Mitigated Risks

Number ▲	Risk Summary	Rating
1	**toddenergy ot 1**	**B4**
2	**toddenergy ot 2**	**A4**
3	**asd**	**B1**

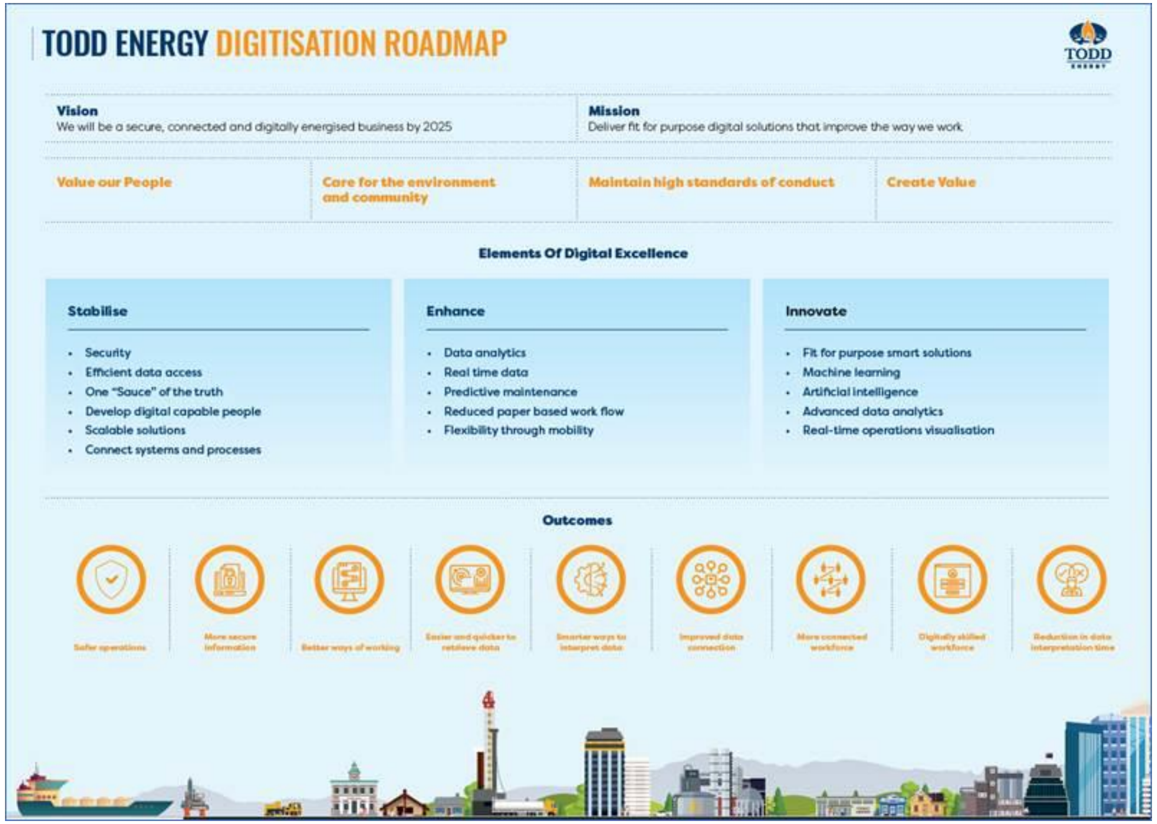
Category	Total Number ▾
Environmental	**1**
Health & Safety	**1**
Reputational	**1**

TLP: AMBER

Ingredient 3 - Strategic Enhancement Plan

TODD
CORPORATION

Mix in a well-defined enhancement plan, outlining steps for closing gaps and continuously improving security across the organisation.



TODD ENERGY DIGITISATION ROADMAP

TODD ENERGY

Vision
We will be a secure, connected and digitally energised business by 2025

Mission
Deliver fit for purpose digital solutions that improve the way we work

Value our People

Care for the environment and community

Maintain high standards of conduct

Create Value

Elements Of Digital Excellence

Stabilise

- Security
- Efficient data access
- One "Sauce" of the truth
- Develop digital capable people
- Scalable solutions
- Connect systems and processes

Enhance

- Data analytics
- Real time data
- Predictive maintenance
- Reduced paper based work flow
- Flexibility through mobility

Innovate

- Fit for purpose smart solutions
- Machine learning
- Artificial intelligence
- Advanced data analytics
- Real-time operations visualisation

Outcomes

Safer operations

More secure information

Better ways of working

Easier and quicker to retrieve data

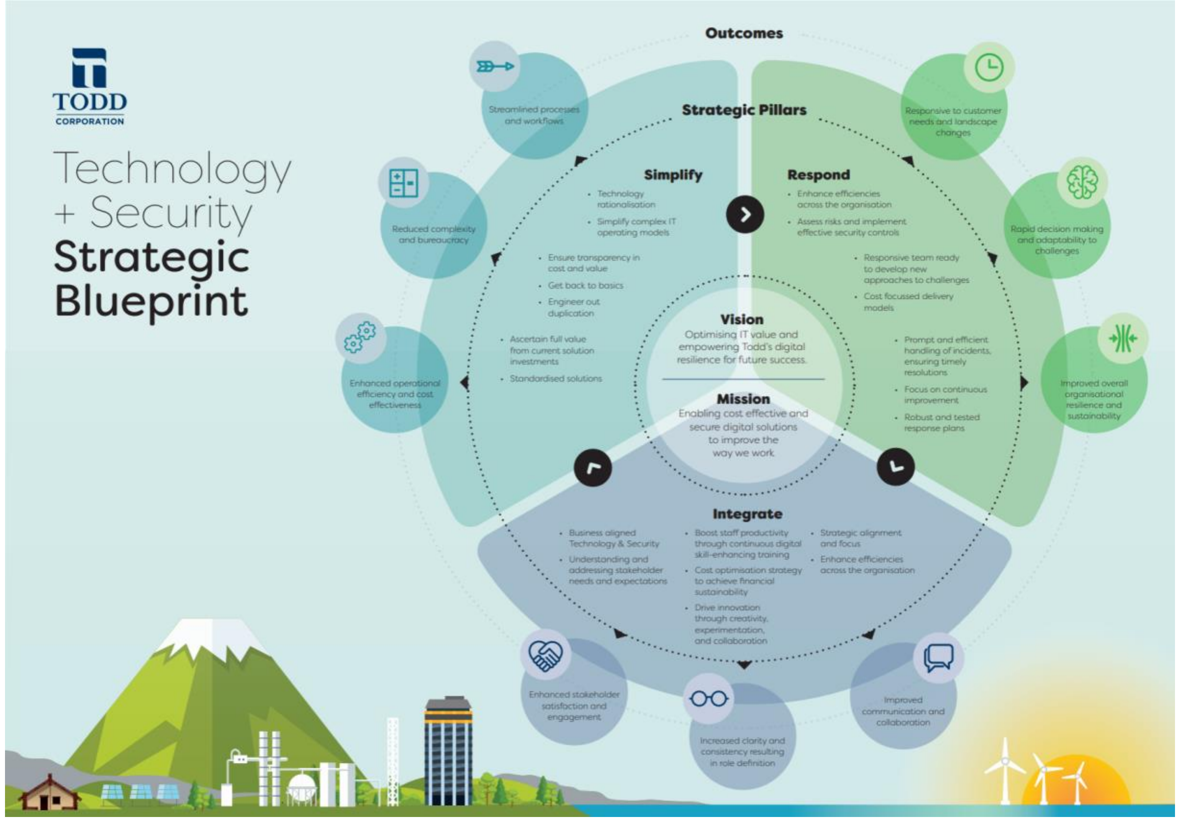
Smarter ways to interpret data

Improved data connection

More connected workforce

Digitally skilled workforce

Reduction in data interpretation time



TODD
CORPORATION

Technology
+ Security
Strategic
Blueprint

Outcomes

Streamlined processes and workflows

Reduced complexity and bureaucracy

Enhanced operational efficiency and cost effectiveness

Responsive to customer needs and landscape changes

Rapid decision making and adaptability to challenges

Improved overall organisational resilience and sustainability

Enhanced stakeholder satisfaction and engagement

Increased clarity and consistency resulting in role definition

Improved communication and collaboration

Strategic Pillars

Simplify

- Technology rationalisation
- Simplify complex IT operating models
- Ensure transparency in cost and value
- Get back to basics
- Engineer out duplication
- Ascertain full value from current solution investments
- Standardised solutions

Respond

- Enhance efficiencies across the organisation
- Assess risks and implement effective security controls
- Responsive team ready to develop new approaches to challenges
- Cost focussed delivery models
- Prompt and efficient handling of incidents, ensuring timely resolutions
- Focus on continuous improvement
- Robust and tested response plans

Integrate

- Business aligned Technology & Security
- Understanding and addressing stakeholder needs and expectations
- Boost staff productivity through continuous digital skill-enhancing training
- Cost optimisation strategy to achieve financial sustainability
- Drive innovation through creativity, experimentation, and collaboration
- Strategic alignment and focus
- Enhance efficiencies across the organisation

Vision
Optimising IT value and empowering Todd's digital resilience for future success.

Mission
Enabling cost effective and secure digital solutions to improve the way we work

Vision
We will be a secure, connected, and digitally energised business by 2025.

Vision
Optimising IT value and improving Todd's digital resilience for future success.

Ingredient 3 - Technology & Security Strategy & Roadmap: 2025 to 2027

Our Vision

Optimising IT value and improving Todd's digital resilience for future success.

Our Mission

Enabling cost effective digital solutions to improve the way we work.

BUSINESS SUPPORT

60% of IT is dedicated to supporting and securing the business: IT will enable modern ways of working to ensure the business is future fit.

<CorporateStrategyGoesHere>

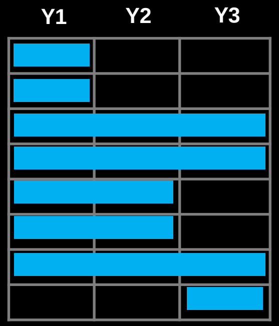
-10% by 2028

Total IT Spend to Revenue Ratio

1.5% to 3.5%

IT Initiatives in Support of Business Initiatives

- Establish governance
- Simplify and rationalise the IT team
- Strengthen cybersecurity resilience
- Leverage specialist external service providers
- Transition select services to cloud
- Implement HRIS
- Digitise processes to streamline workflows
- Adopt sustainable technology practices



What success looks like:

FY23 — FY27

IT Value 72% — >75%

IT Satisfaction 69%

Improve IT Value and IT Satisfaction scores

FY24 — FY27

IT Engagement 55% — >67%

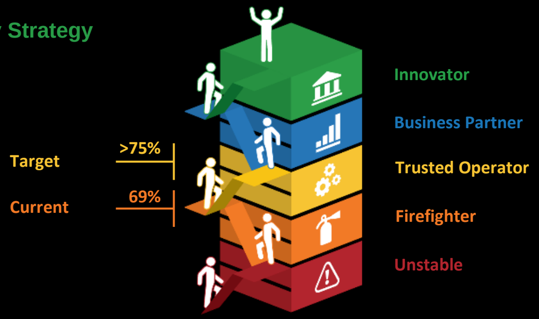
Raise IT team engagement scores

IT EXCELLENCE

30% of IT is dedicated to improving operational excellence: IT will be a trusted operator to increase efficiency, lower costs, and reduce IT risk.

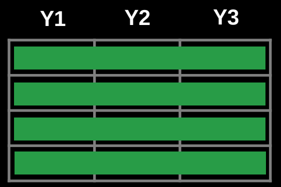
Our Technology & Security Strategy

- Simplify
- Integrate
- Respond



IT Initiatives in Support of IT Excellence

- Annual improvement plan
- Manage and improve core IT processes
- Team productivity reporting
- Architecture over engineering



What does success look like:

OT Environment	FY27	IT Environment
Level 3 Defined	NIST Cybersecurity Framework	Level 4 Managed

Cybersecurity target maturity scores

Critical & significantly important core IT processes

✓ Effective	✓ Somewhat Effective	✗ Somewhat Ineffective	✗ Not Effective

Effectiveness of important processes in the green

DATA & AI

10% of IT is dedicated to advancing data and AI capabilities: IT will prioritise critical industry drivers to generate insights, accelerate AI-driven innovation, and enhance productivity and operational efficiency.

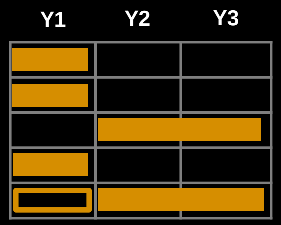
Our Data and AI Commitment

We are committed to responsible data management, rapid insight generation, and automation of routine tasks to drive business efficiency. By aligning with key industry drivers, we seek to unlock actionable insights and foster AI-driven innovation that maximises productivity and optimises core business processes.

+10% by 2028

IT Initiatives in Support of Data & AI

- Centralise data capabilities
- Implement modern data platform
- Improve data maturity and data quality
- Develop an AI roadmap
- Deliver AI capabilities



What does success look like in 2027:

+20%

Improve data quality in business-critical datasets

25% to 30%

Percentage of business processes augmented by AI automation

TLP: AMBER

Ingredient 4 - Board and Management Buy-In

‘Although cyber leaders, business leaders and boards of directors are now communicating more directly and more often, they continue to speak different languages.’
(World Economic Forum)

38%

of directors say cybersecurity is the most difficult area for the board to oversee.
(DiligentInstitute)

Date August 2024 & September 2024

TODD
CORPORATION

Ingredient 4 - Board & ExCom Cybersecurity Dashboard

Top 4 Security Risks

R1	A cyber-attack…
R2	A cyber-attack…
R3	A cyber-attack…
R4	A cyber-attack…

	Severe	High	Medium	Low
#	1	2	1	0

	A Highly Unlikely	B Unlikely	C Possible	D Probable	E Likely	F Highly Likely
6 Catastrophic	🟧	🟧	🟥	🟥 R1	🟥	🟥
5 Major	🟨	🟧	🟧	🟥 R2	🟥	🟥
4 Serious	🟨	🟨	🟨	🟧 R3	🟧	🟧
3 Moderate	🟩	🟩	🟨	🟨 R4	🟧	🟧
2 Minor	🟩	🟩	🟩	🟩	🟨	🟨
1 Slight	🟩	🟩	🟩	🟩	🟩	🟨

Notable Security Events / Incidents

Event(s) / Incident(s)	Risk Link	Date(s)	Event / Incident	Action(s)	Comment(s)

Security Event	An occurrence indicating that the security of a system or network may have been breached or compromised
Security Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Date August 2024 & September 2024

Ingredient 4 - Board & ExCom Cybersecurity Dashboard

TODD CORPORATION

Security Resilience Program

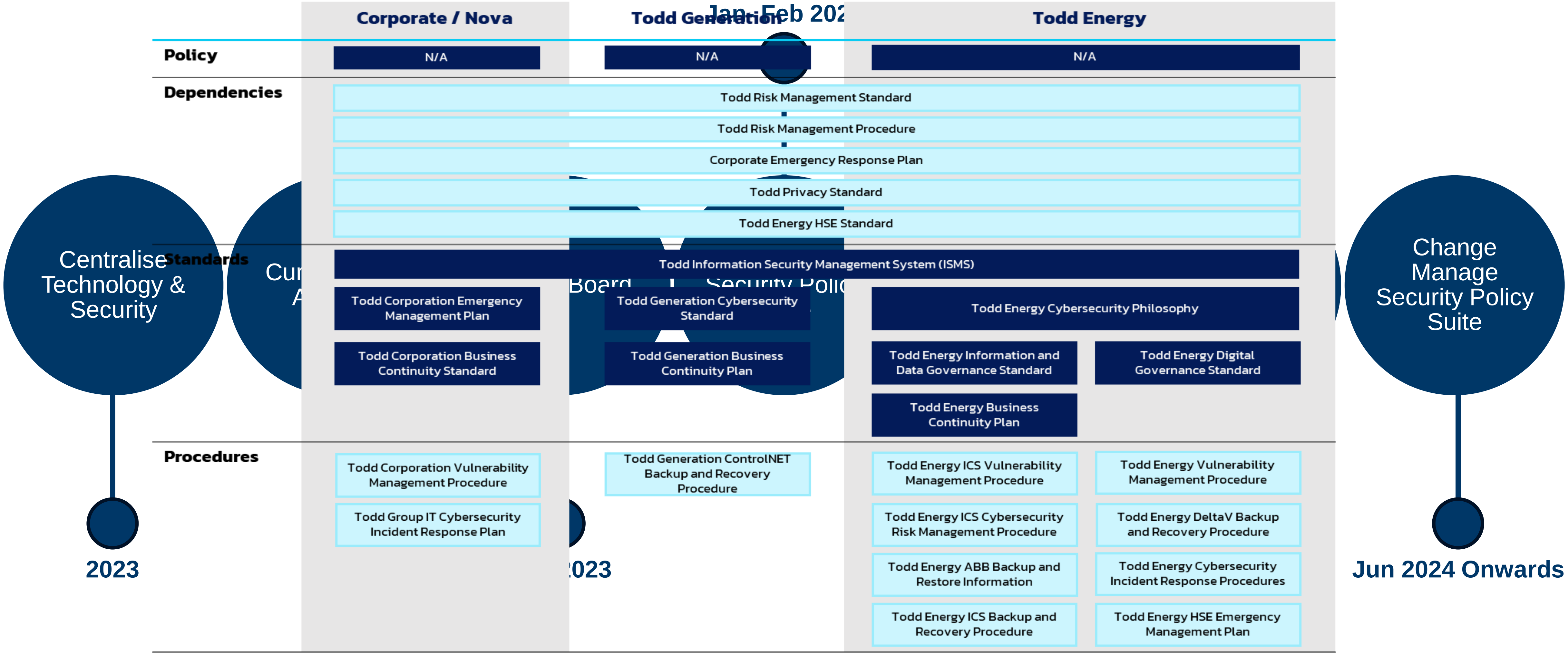
Project / Initiative	Description	Completion Date	Status	Note(s)
			On Hold	.
			🟩	
			🟨	
			🟥	

New Zealand National Cyber Security Centre Top Business Highlights – August 2024 & September 2024

Phishing campaign impersonates Fortune 100 companies https://labs.guard.io/echospoofing-a-massive-phishing-campaign-exploiting-proofpoints-email-protection-to-dispatch-3dd6b5417db6	**Iranian-linked cyber actors targeting of US presidential candidates** https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us	**Australia partners with Google for critical infrastructure security** https://www.csiro.au/en/news/All/News/2024/August/CSIRO-and-Google-Partner-to-Help-Secure-Critical-Infrastructure-from-Risky-Software-Components
227 gigabytes of sensitive US information published https://www.bleepingcomputer.com/news/security/national-public-data-confirms-breach-exposing-social-security-numbers	**47 currency exchanges taken down in Operation Final Exchange** https://www.bleepingcomputer.com/news/security/germany-seizes-47-crypto-exchanges-used-by-ransomware-gangs/	**A gift, a scandal, and a QR code** https://www.stuff.co.nz/nz-news/350416267/new-qr-code-scam-may-be-its-way-police

Ingredient 5 - Policies

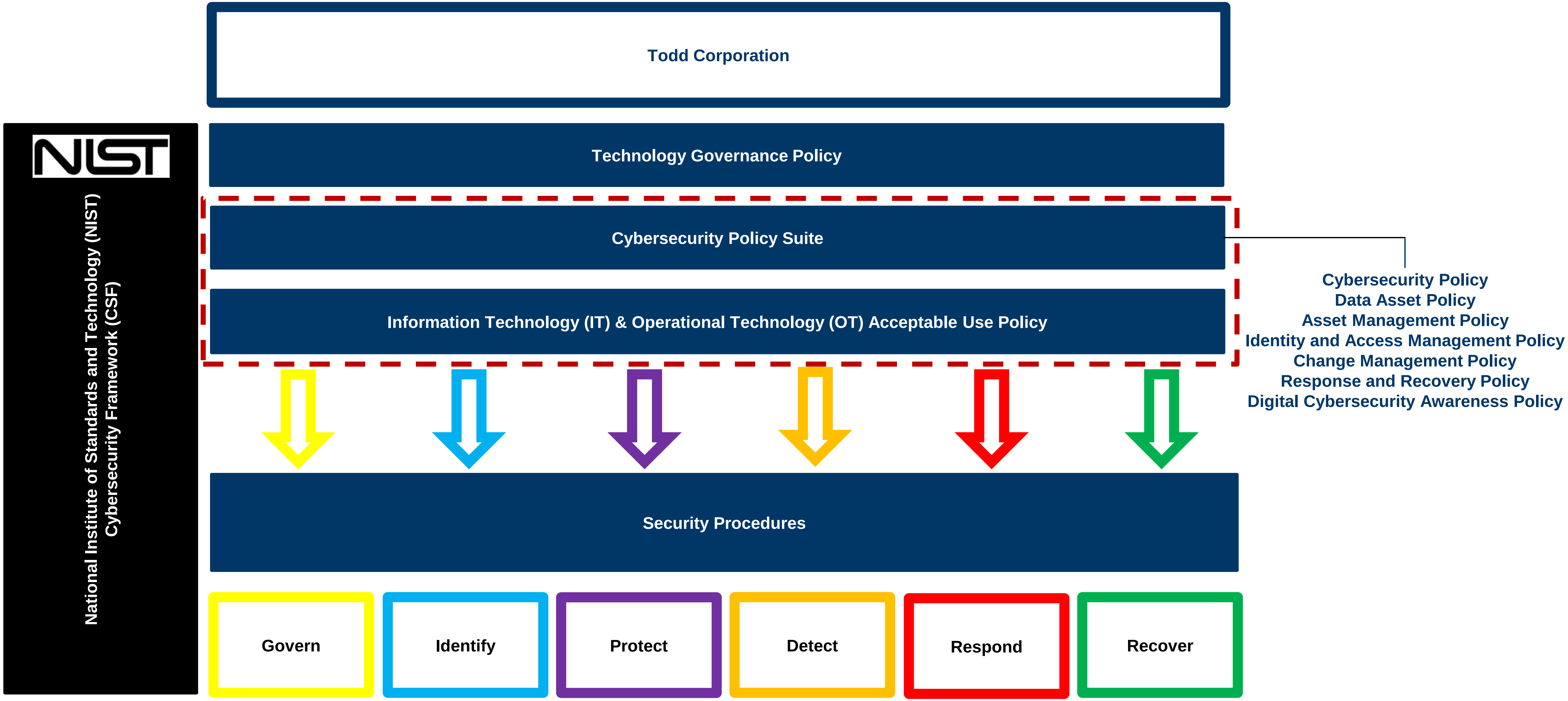
Sprinkle in clearly defined security policies that align with best practices and ensure all employees and stakeholders know the rules of the game.



	Corporate / Nova	Todd Generation	Todd Energy
Policy	N/A	N/A	N/A
Dependencies	Todd Risk Management Standard Todd Risk Management Procedure Corporate Emergency Response Plan Todd Privacy Standard Todd Energy HSE Standard		
Standards	Todd Information Security Management System (ISMS)		
	Todd Corporation Emergency Management Plan Todd Corporation Business Continuity Standard	Todd Generation Cybersecurity Standard Todd Generation Business Continuity Plan	Todd Energy Cybersecurity Philosophy Todd Energy Information and Data Governance Standard Todd Energy Digital Governance Standard Todd Energy Business Continuity Plan
Procedures	Todd Corporation Vulnerability Management Procedure Todd Group IT Cybersecurity Incident Response Plan	Todd Generation ControlNET Backup and Recovery Procedure	Todd Energy ICS Vulnerability Management Procedure Todd Energy Vulnerability Management Procedure Todd Energy ICS Cybersecurity Risk Management Procedure Todd Energy DeltaV Backup and Recovery Procedure Todd Energy ABB Backup and Restore Information Todd Energy Cybersecurity Incident Response Procedures Todd Energy ICS Backup and Recovery Procedure Todd Energy HSE Emergency Management Plan

Centralise Technology & Security
2023
Cur
A
Board
2023
Jan-Feb 202
Security Polic
Change Manage Security Policy Suite
Jun 2024 Onwards

Ingredient 5 - High Level Cybersecurity Policy Framework



Todd Corporation

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

Technology Governance Policy

Cybersecurity Policy Suite

Information Technology (IT) & Operational Technology (OT) Acceptable Use Policy

Cybersecurity Policy
Data Asset Policy
Asset Management Policy
Identity and Access Management Policy
Change Management Policy
Response and Recovery Policy
Digital Cybersecurity Awareness Policy

Security Procedures

Govern

Identify

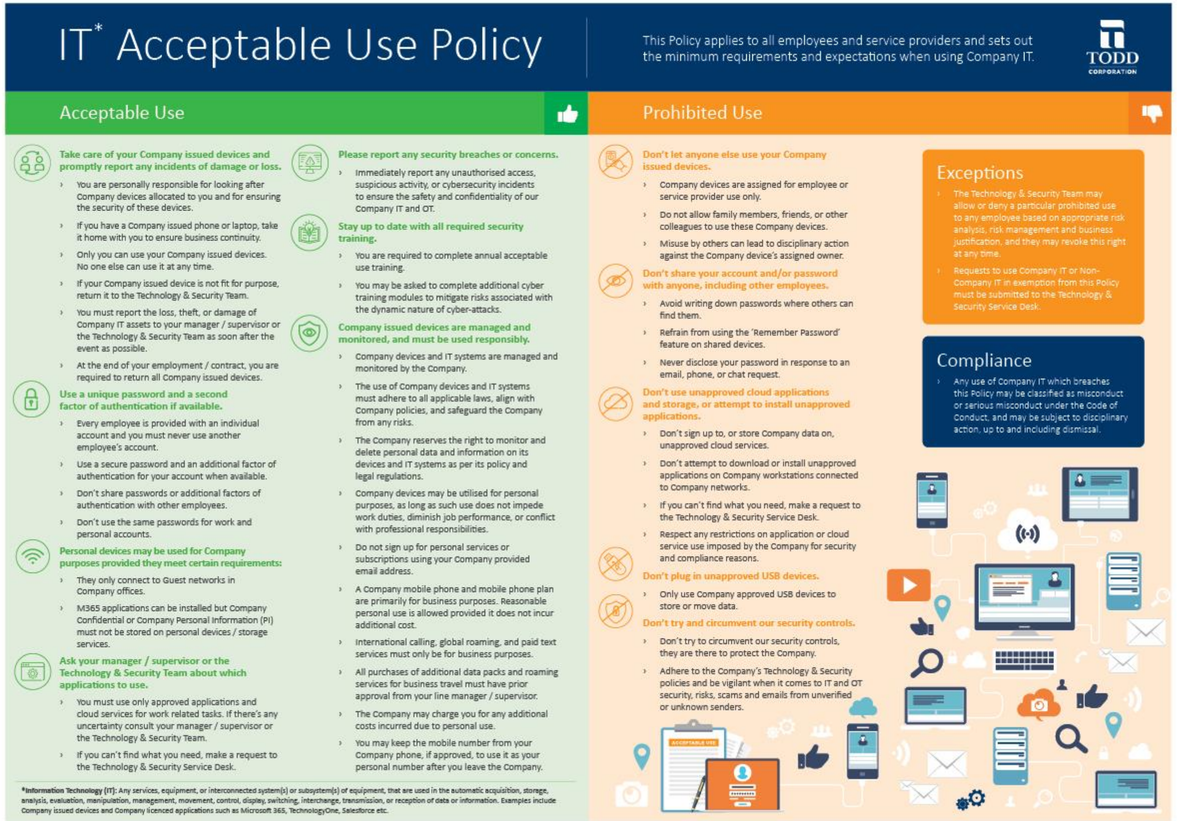
Protect

Detect

Respond

Recover

Ingredient 5 - IT & OT Acceptable Use Policies



IT* Acceptable Use Policy

This Policy applies to all employees and service providers and sets out the minimum requirements and expectations when using Company IT.

TODD CORPORATION

Acceptable Use

Take care of your Company issued devices and promptly report any incidents of damage or loss.

- You are personally responsible for looking after Company devices allocated to you and for ensuring the security of these devices.
- If you have a Company issued phone or laptop, take it home with you to ensure business continuity.
- Only you can use your Company issued devices. No one else can use it at any time.
- If your Company issued device is not fit for purpose, return it to the Technology & Security Team.
- You must report the loss, theft, or damage of Company IT assets to your manager / supervisor or the Technology & Security Team as soon after the event as possible.
- At the end of your employment / contract, you are required to return all Company issued devices.

Use a unique password and a second factor of authentication if available.

- Every employee is provided with an individual account and you must never use another employee's account.
- Use a secure password and an additional factor of authentication for your account when available.
- Don't share passwords or additional factors of authentication with other employees.
- Don't use the same passwords for work and personal accounts.

Personal devices may be used for Company purposes provided they meet certain requirements:

- They only connect to Guest networks in Company offices.
- M365 applications can be installed but Company Confidential or Company Personal Information (PI) must not be stored on personal devices / storage services.

Ask your manager / supervisor or the Technology & Security Team about which applications to use.

- You must use only approved applications and cloud services for work related tasks. If there's any uncertainty consult your manager / supervisor or the Technology & Security Team.
- If you can't find what you need, make a request to the Technology & Security Service Desk.

Please report any security breaches or concerns.

- Immediately report any unauthorised access, suspicious activity, or cybersecurity incidents to ensure the safety and confidentiality of our Company IT and OT.

Stay up to date with all required security training.

- You are required to complete annual acceptable use training.
- You may be asked to complete additional cyber training modules to mitigate risks associated with the dynamic nature of cyber-attacks.

Company issued devices are managed and monitored, and must be used responsibly.

- Company devices and IT systems are managed and monitored by the Company.
- The use of Company devices and IT systems must adhere to all applicable laws, align with Company policies, and safeguard the Company from any risks.
- The Company reserves the right to monitor and delete personal data and information on its devices and IT systems as per its policy and legal regulations.
- Company devices may be utilised for personal purposes, as long as such use does not impede work duties, diminish job performance, or conflict with professional responsibilities.
- Do not sign up for personal services or subscriptions using your Company provided email address.
- A Company mobile phone and mobile phone plan are primarily for business purposes. Reasonable personal use is allowed provided it does not incur additional cost.
- International calling, global roaming, and paid text services must only be for business purposes.
- All purchases of additional data packs and roaming services for business travel must have prior approval from your line manager / supervisor.
- The Company may charge you for any additional costs incurred due to personal use.
- You may keep the mobile number from your Company phone, if approved, to use it as your personal number after you leave the Company.

Prohibited Use

Don't let anyone else use your Company issued devices.

- Company devices are assigned for employee or service provider use only.
- Do not allow family members, friends, or other colleagues to use these Company devices.
- Misuse by others can lead to disciplinary action against the Company device's assigned owner.

Don't share your account and/or password with anyone, including other employees.

- Avoid writing down passwords where others can find them.
- Refrain from using the 'Remember Password' feature on shared devices.
- Never disclose your password in response to an email, phone, or chat request.

Don't use unapproved cloud applications and storage, or attempt to install unapproved applications.

- Don't sign up to, or store Company data on, unapproved cloud services.
- Don't attempt to download or install unapproved applications on Company workstations connected to Company networks.
- If you can't find what you need, make a request to the Technology & Security Service Desk.
- Respect any restrictions on application or cloud service use imposed by the Company for security and compliance reasons.

Don't plug in unapproved USB devices.

- Only use Company approved USB devices to store or move data.

Don't try and circumvent our security controls.

- Don't try to circumvent our security controls, they are there to protect the Company.
- Adhere to the Company's Technology & Security policies and be vigilant when it comes to IT and OT security, risks, scams and emails from unverified or unknown senders.

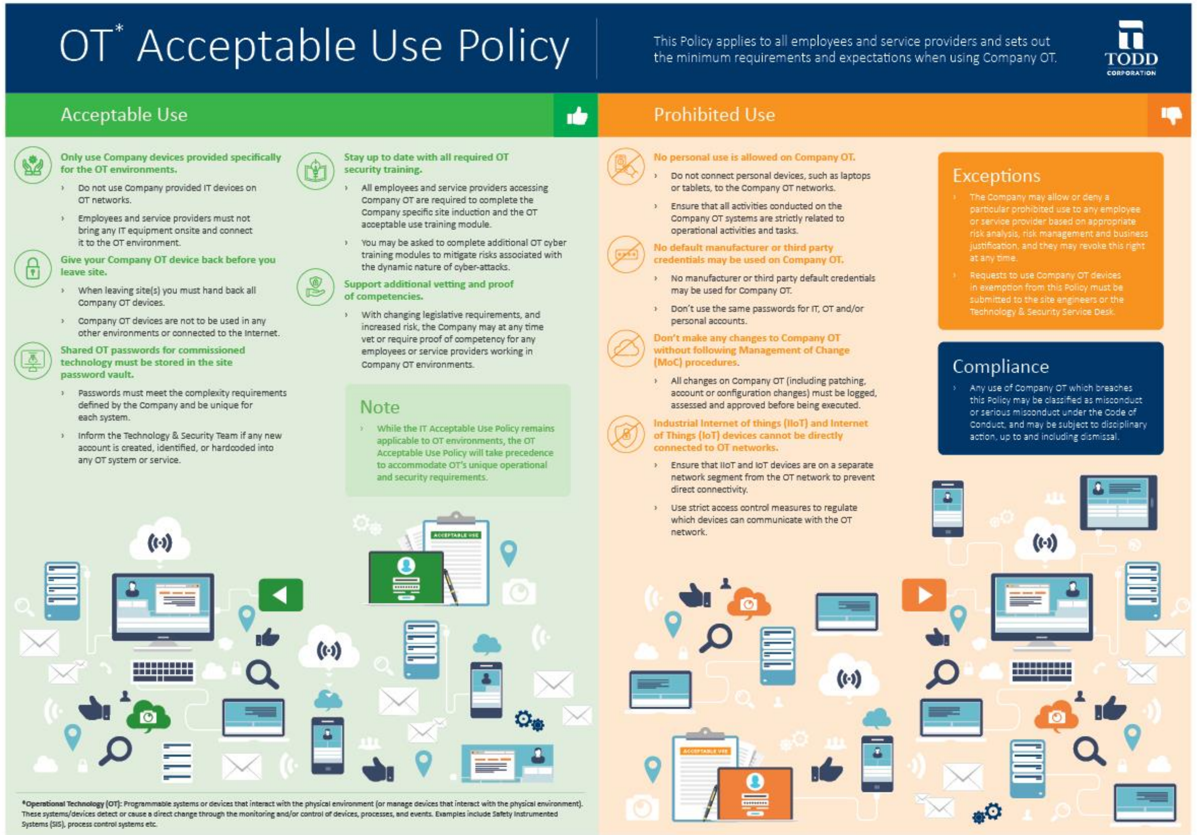
Exceptions

- The Technology & Security Team may allow or deny a particular prohibited use to any employee based on appropriate risk analysis, risk management and business justification, and they may revoke this right at any time.
- Requests to use Company IT or Non-Company IT in exemption from this Policy must be submitted to the Technology & Security Service Desk.

Compliance

- Any use of Company IT which breaches this Policy may be classified as misconduct or serious misconduct under the Code of Conduct, and may be subject to disciplinary action, up to and including dismissal.

*Information Technology (IT): Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Examples include Company issued devices and Company licenced applications such as Microsoft 365, TechnologyOne, Salesforce etc.



OT* Acceptable Use Policy

This Policy applies to all employees and service providers and sets out the minimum requirements and expectations when using Company OT.

TODD CORPORATION

Acceptable Use

Only use Company devices provided specifically for the OT environments.

- Do not use Company provided IT devices on OT networks.
- Employees and service providers must not bring any IT equipment onsite and connect it to the OT environment.

Give your Company OT device back before you leave site.

- When leaving site(s) you must hand back all Company OT devices.
- Company OT devices are not to be used in any other environments or connected to the Internet.

Shared OT passwords for commissioned technology must be stored in the site password vault.

- Passwords must meet the complexity requirements defined by the Company and be unique for each system.
- Inform the Technology & Security Team if any new account is created, identified, or hardcoded into any OT system or service.

Stay up to date with all required OT security training.

- All employees and service providers accessing Company OT are required to complete the Company specific site induction and the OT acceptable use training module.
- You may be asked to complete additional OT cyber training modules to mitigate risks associated with the dynamic nature of cyber-attacks.

Support additional vetting and proof of competencies.

- With changing legislative requirements, and increased risk, the Company may at any time vet or require proof of competency for any employees or service providers working in Company OT environments.

Note

- While the IT Acceptable Use Policy remains applicable to OT environments, the OT Acceptable Use Policy will take precedence to accommodate OT's unique operational and security requirements.

Prohibited Use

No personal use is allowed on Company OT.

- Do not connect personal devices, such as laptops or tablets, to the Company OT networks.
- Ensure that all activities conducted on the Company OT systems are strictly related to operational activities and tasks.

No default manufacturer or third party credentials may be used on Company OT.

- No manufacturer or third party default credentials may be used for Company OT.
- Don't use the same passwords for IT, OT and/or personal accounts.

Don't make any changes to Company OT without following Management of Change (MoC) procedures.

- All changes on Company OT (including patching, account or configuration changes) must be logged, assessed and approved before being executed.

Industrial Internet of things (IIoT) and Internet of Things (IoT) devices cannot be directly connected to OT networks.

- Ensure that IIoT and IoT devices are on a separate network segment from the OT network to prevent direct connectivity.
- Use strict access control measures to regulate which devices can communicate with the OT network.

Exceptions

- The Company may allow or deny a particular prohibited use to any employee or service provider based on appropriate risk analysis, risk management and business justification, and they may revoke this right at any time.
- Requests to use Company OT devices in exemption from this Policy must be submitted to the site engineers or the Technology & Security Service Desk.

Compliance

- Any use of Company OT which breaches this Policy may be classified as misconduct or serious misconduct under the Code of Conduct, and may be subject to disciplinary action, up to and including dismissal.

*Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include Safety Instrumented Systems (SIS), process control systems etc.

Last Bit of Spice

1. Don’t compromise on your team or cybersecurity partners.
2. If things aren’t working, fail them, and fail them fast.
3. Spend more time on leveraging the 80% similarity than the 20% differentiation.

Questions