

B.Grimm Power – Overview Risk Management

"B.Grimm risk management process is anchored in the COSO 2017 framework, which forms the bedrock of our core principles for effective and comprehensive risk management."

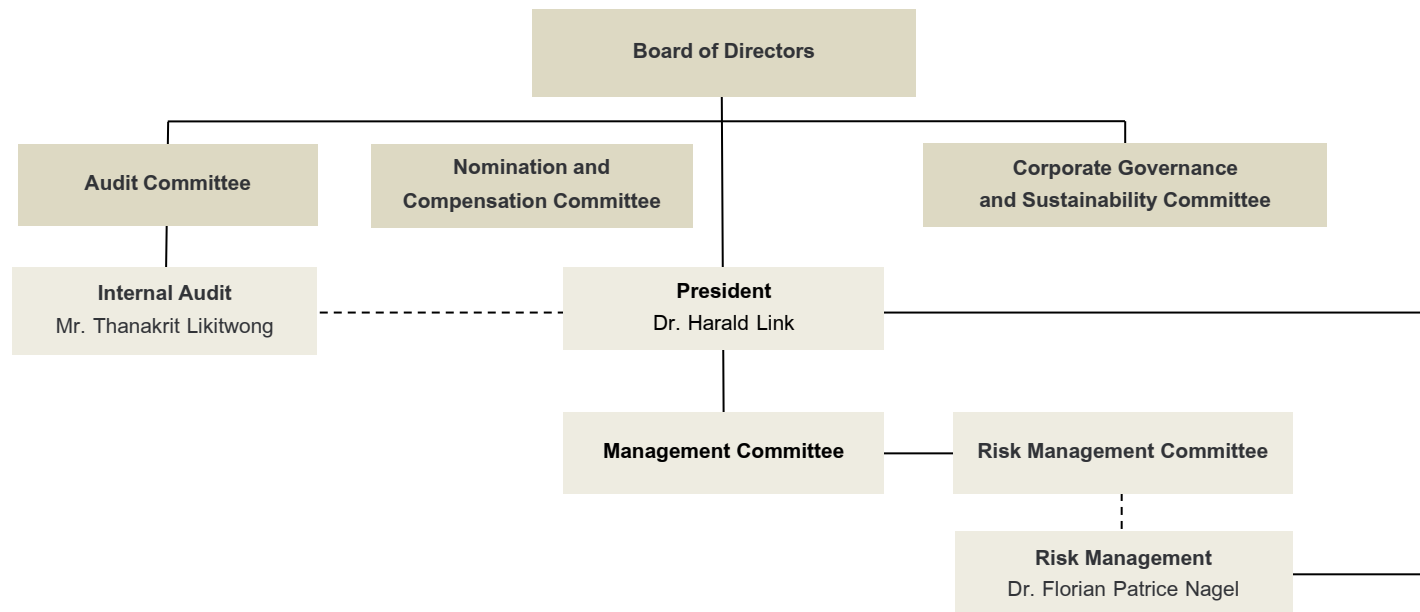
COSO ERM 2017 Enterprise Risk Management integrating with Strategy and Performance



Risk Governance

B.Grimm Power establish the Risk Management Committee (RMC) to establish and review the risk management policy, align strategies that reflect and cover operating risks, and continuously supervise risk management for ongoing efficiency and effectiveness. RMC reports to the Management Committee and the Board of Directors. We also have the Risk Management Unit is responsible in place, which is responsible for communicating risk policies and processes internally, assuring effective controls, analysing current risks and identifying potential risks affecting the company, ensuring business heads understand the risks that might affect their departments; ensuring risk awareness in each individual unit and operating divisions, as well as communicating the external risk posed by corporate governance to stakeholders. The Head of Risk Management Unit report directly to the President and administratively to the RMC.

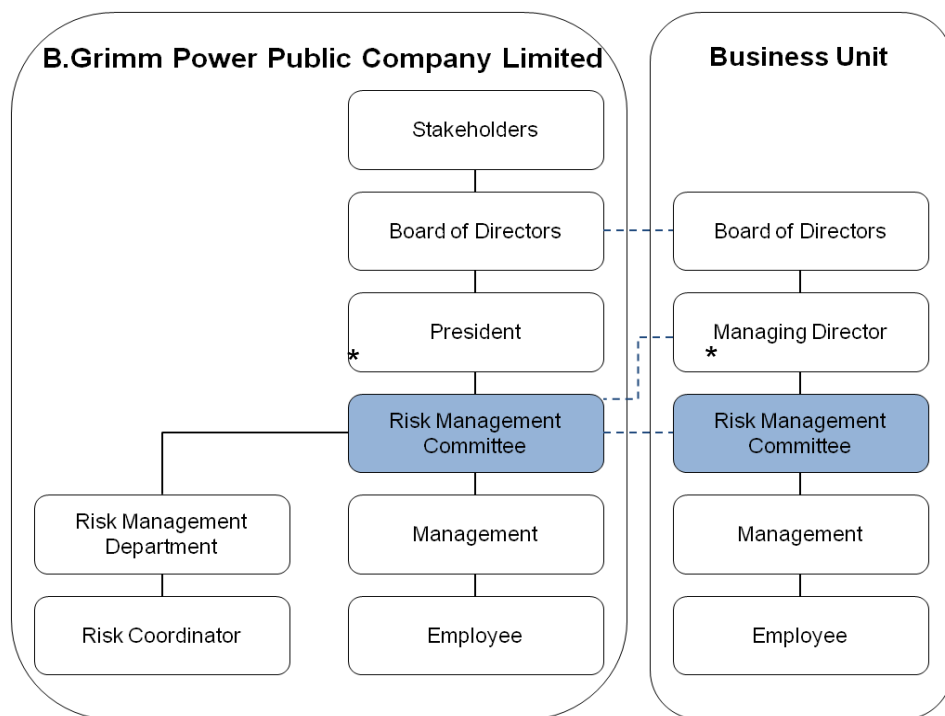
Also, B.Grimm Power has the Head of Internal Audit, who report directly to Audit Committee who oversees to ensure that Internal Audit Department performs internal auditing with independence, objectivity, integrity, and expertise, in adherence to the internal audit and internal control standards. The Audit then report to the Board of Directors. In addition, the Head of Internal Audit reports administratively to the President, who subsequently reports to the Board of Directors.



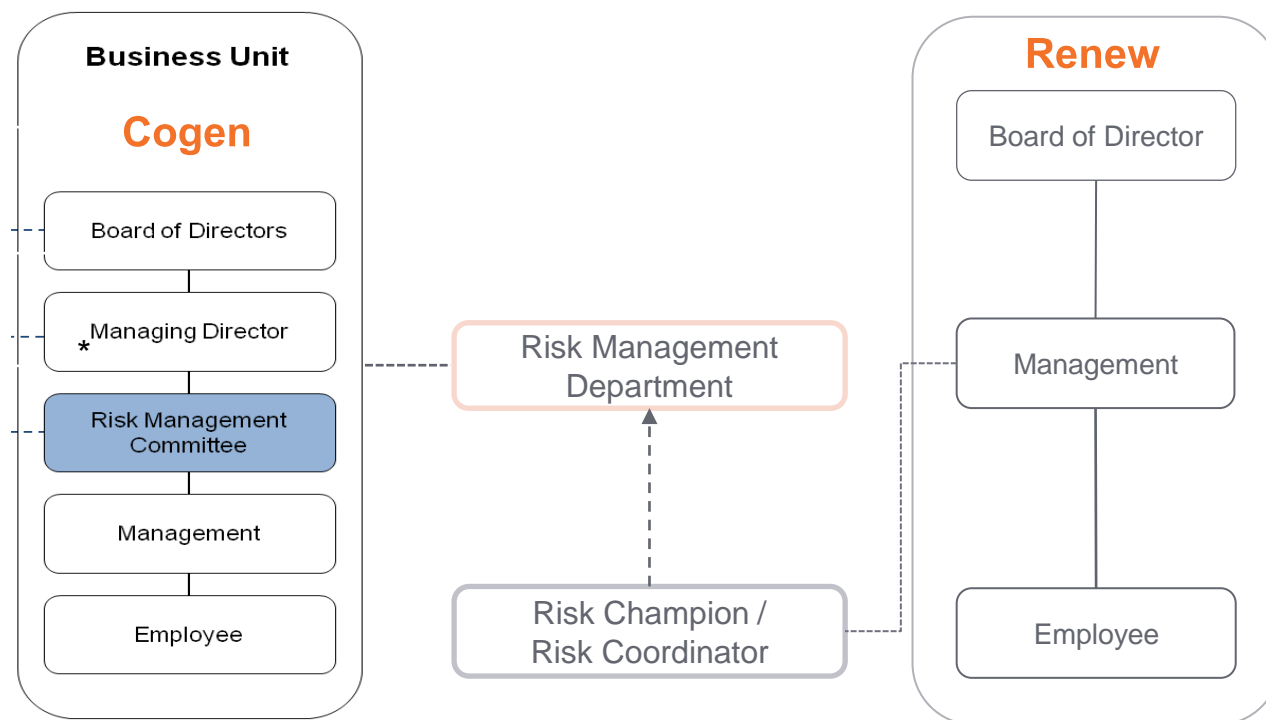
Risk Governance

Risk monitoring and review take place quarterly through the Risk Management Committee. Noteworthy endorsements and updates on mitigation are shared with the Board of Directors at least annually.

Corporate Level

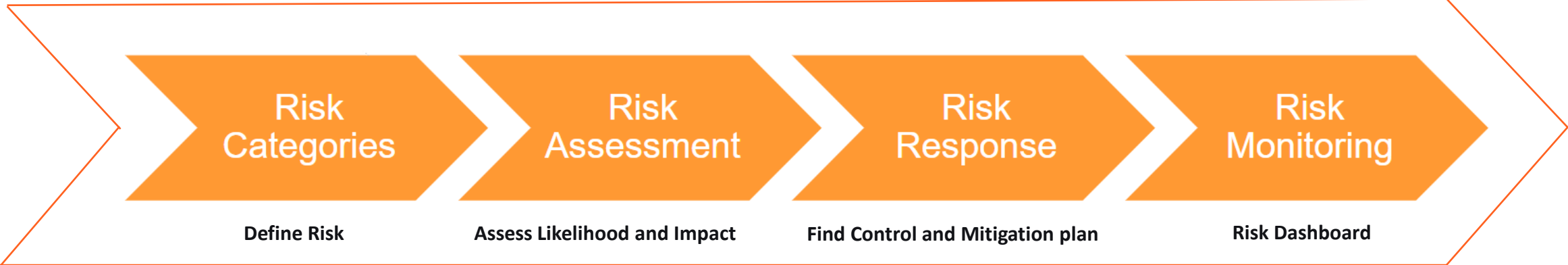


Business Units Level



* Risk Management Committee consists of Management Committee and Managing Directors









Risk Management Process – Overview



Risk Management Process – Step 1



“**Risk categorisation process** entails organising identified risks into distinct groups based on shared characteristics such as origin, impact type, or likelihood. This classification enhances our understanding of risks, streamlines prioritisation efforts, and enables the development of targeted mitigation strategies for each category.”

<p>1. Reputation Risk</p>  <ul style="list-style-type: none"> - Reputation/brand risk - Intellectual Property protection risk 	<p>2. Strategic Risk</p>  <ul style="list-style-type: none"> - General business environment risks (e.g. Political, macroeconomics) - Industry risks (e.g. consumer, competitor, technology) 	<p>3. Compliance Risk</p>  <ul style="list-style-type: none"> - Laws and regulations - Social commitment - Internal rules and regulations 	<p>4. Operation Risk</p>  <ul style="list-style-type: none"> - Partner - Plant operations - Sales & Marketing - Distribution - Raw materials - Labor
<p>5. Financial Risk</p>  <ul style="list-style-type: none"> - Financial market investment - Exchange rate - Interest rate - Liquidity - Credit 	<p>6. ESG Risk</p>  <ul style="list-style-type: none"> - Environmental damage - Natural disaster - Man-made disaster - Community - Safety and health risks - Governance risk 	<p>7. IT/Cyber Security</p>  <ul style="list-style-type: none"> - Cyber security - Data security 	<p>8. Emerging</p>  <ul style="list-style-type: none"> - Decentralization

Risk Management Process – Step 2



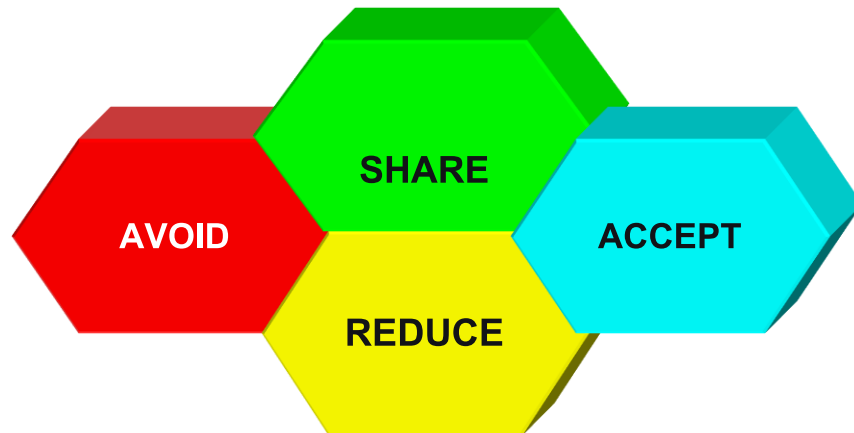
“**Risk assessment process** systematically involves identifying, analysing, and evaluating potential uncertainties that could affect our projects or objectives. The assessment criteria are based on a 1-5 rating scale for risk likelihood and impact. This process aims to comprehend the likelihood level and potential consequences of these risks, prioritise them, and empower us to make informed decisions and develop effective mitigation strategies.”



Risk Management Process – Step 3



"**Risk response process** involves developing and implementing strategies to address identified risks. It aims to mitigate potential negative impacts, capitalise on opportunities, and enhance project outcomes through proactive and effective actions."



1. **Accept** – Remaining risks that can be accepted
2. **Reduce** – Take actions to reduce likelihood or impact
3. **Avoid** – Action is taken to exit or avoid a risk activity
4. **Share** – Risk is reduced by sharing with a third party

Risk Management Process – Step 4



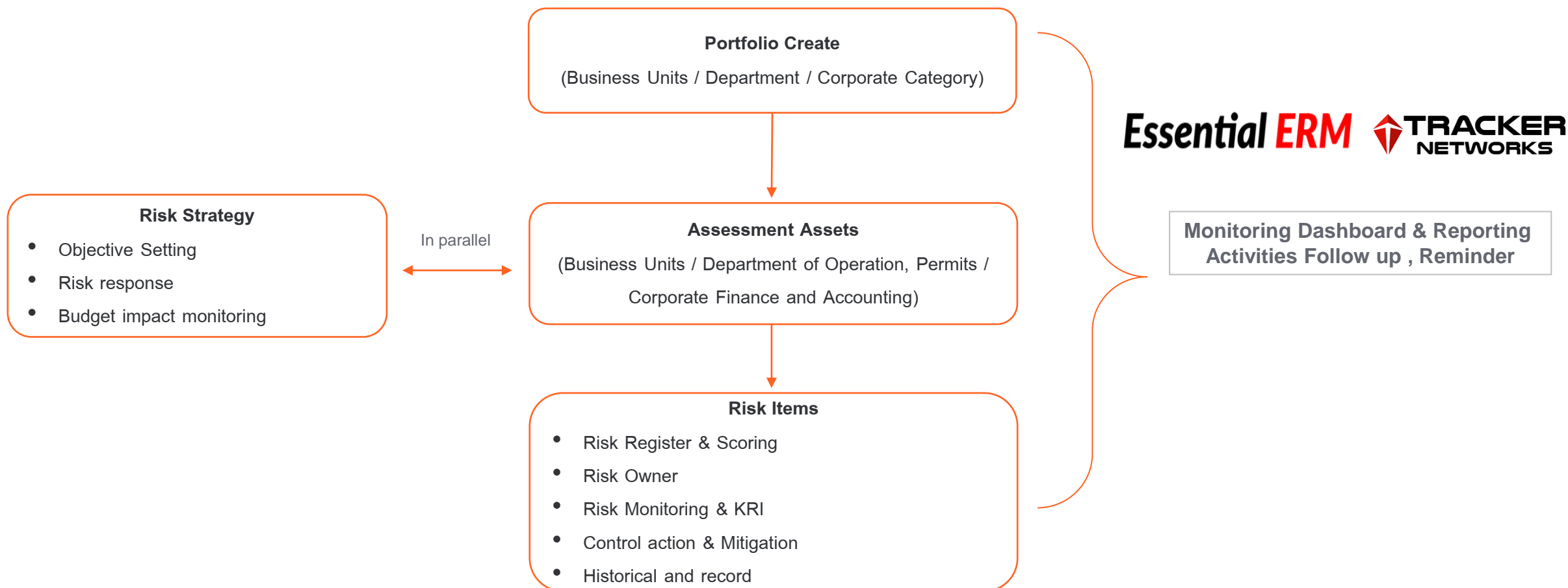
“**Risk monitoring process** By utilising the ERM dashboard as a vital tool, risk monitoring transforms into an ongoing process of tracking identified risks, ensuring prompt responses, and implementing adaptive strategies for the success of projects.”

B.GRIMM SINCE 1878 **Enterprise Risk Console**

Last Assessed	Portfolio	Risk Name	Category	Residual Likelihood	Residual Impact	Residual Risk	Inherent Likelihood	Inherent Impact	Inl
	HQ-Accounting	(Accounting).Failure in submission data from other dept / ...	Financial	3 - Possible	4 - Major	12	3 - Possible	4 - Major	
	HQ-Accounting	(Accounting).Related computer applications/ Network...	Operation	2 - Unlikely	4 - Major	8	2 - Unlikely	4 - Major	
	HQ-Accounting	(Accounting).A/C employee's Knowledge, qualification...	People	2 - Unlikely	3 - Moderate	6	2 - Unlikely	3 - Moderate	
	HQ-Accounting	(Accounting).Risk on tax with revenue dept	Financial	2 - Unlikely	4 - Major	8	2 - Unlikely	4 - Major	
	HQ-Accounting	(Accounting).Risk on BOI	Financial	2 - Unlikely	4 - Major	8	2 - Unlikely	4 - Major	

Enterprise Risk Management Platform

“Our enterprise risk management platform serves as a catalyst for proactive risk management activities”



Enterprise Risk Management Platform – Example Workflow

Our enterprise risk management platform facilitates real-time risk monitoring, reporting to management, and accurate tracking of risk exposure across the organisation.

Business Units / Department Level

Risk Coordinator
Risk Owner

Business
Portfolio

Risk
items

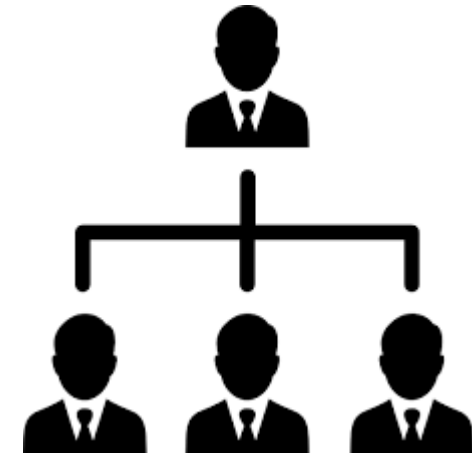
Risk Items Registration

Company Risk Data Portfolio

ERM
ESSENTIAL

Company Management
Risk Management Committee
Risk Management Team

- Risk Highlight
- Summary Report
- Support information
- Monitoring and Follow up



Enterprise Risk Management Platform – Use Case (Example)

Risk Details – Data Management

Essential ERM by Tracker Networks Inc.
JD Jason Doel Tracker Networks Inc.

Risk # TRNT-0983

Risk Details

Mike Jones owner
General Portfolio (unlocked)

Data Center Outage greater than 24 hours

Details

Category: Operational Risk

Sub Category: Availability & Resiliency

Risk Description: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris mauris fortor, tempor id congue et, malesuada ut nisi. Nullam at interdum dui. Nulla facilisi. Aenean aliquet mi quis nisi vulputate. ... nec feugiat tellus scelerisque. Nulla finibus diam vel en

Likelihood	Impact	Inherent Risk	Control Effectiveness	Residual Risk	Risk Thresholds
4 Likely	5 Extreme	20	Mostly Effective	6	
65%	\$10,000,000	\$6,500,000	After Mitigation Likelihood is 2 Unlikely 25% Impact is 3 Moderate \$2,500,000	\$625,000 override	
Velocity					
Very High					<input type="checkbox"/> suppress thresholds

Root Causes

- Cyberattack
- Flood (data center close to river)
- Internet Service Provider Outage
- Localized Power Disruption
- System Wide Power Failure (Large Grid Failure)
- Terrorist Attack

select or create new cause

Pre-Event Mitigations

- Onsite back up generators moved to roof of building for flood proofing
- Physical Security Hardening Measures
- Redundant ISPs with Automated Failover Capability
- SOC2 and ISO27000 Security Program (evidenced by continual certification)
- Wireless communication with ISP

select or create new control/mitigation

Risk Event

Data Centre Service Outage

This is considered an outage that prevents clients and users from gaining access to our production systems and/or to their data. A production outage that lasts more than 24 hours.

Post-Event Mitigations

- Data backups can be used to activate cold failover site in worst case scenario
- SLA claw backs with hosting provider

select or create new control/mitigation

Consequences

- Contract cancellations
- Damage to Reputation
- Exposure to litigation
- Regulatory fines & penalties
- Up to \$10,000,000 in customer SLA penalties

select or create new consequence

Business Areas

Objective 4 - Meet all Critical Annual Project Milestones | Legal | Internal Medicine | HR

Action Plans

Action Name	Owner	Due Date	Status
Business Continuity Test	Peter Ritchie	2019-3-29	In-Progress
Review 2019 SOC2 Report	Jason Doel	2019-5-31	Planned
Review and renegotiate SLA penalties on customer contracts	Jason Doel	2019-6-28	In-Progress
Complete Internal Audit Review of Security Program	Peter Ritchie	2019-6-30	In-Progress

11

Enterprise Risk Management Platform – Use Case (Example)

Corporate Risk Heat Maps

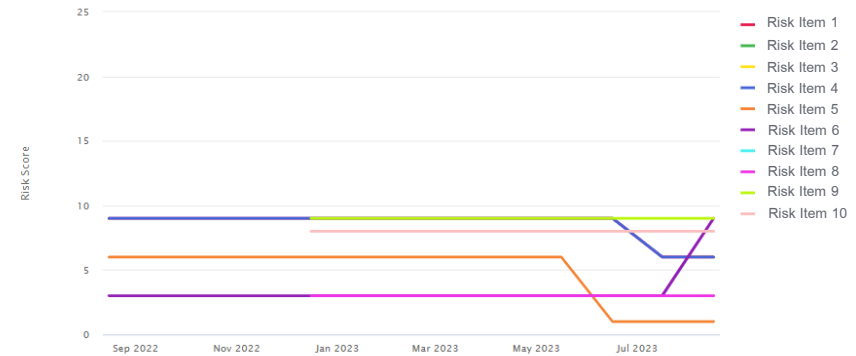
By Score (Top 10) - Residual Values

Report date Wed Aug 16 2023



Risk Trend Analytic

Risk Scores Over Time By Risk (Top 10) - Residual Values August 2022 through August 2023



Risk Details Report

Rank: 473
TRAC-4684

Strategic Objectives: Business Areas: [Power Plant A] - Issue

Portfolio: Power Plant Type - Power Plant A
Risk Owner:

Category: Operation
Sub-Category:

Description: Drainage Pump is broken that cannot pumping water out from drainage pit.

	Likelihood	Impact	Score	90 Day Trend	365 Day Trend
Inherent Risk	2	2	4	→	→
Residual Risk	2	2	4	→	→

Control Effectiveness: [Visual indicator]

Root causes:

- Pumping motor is short circuit.
- Control cabinet is broken.

Mitigations	Control Effectiveness	Owner	Last Update
Provide scheduled preventive maintenance (PM) for all machines.			Aug 09, 2023
Provide corrective maintenance			Aug 04, 2023
Permit to work			Aug 09, 2023
Operating Function test Test every 6 month.			Aug 09, 2023
Sparepart management			Aug 04, 2023
Spare part sharing with power plant in group			Aug 09, 2023

Materiality Assessment - Integration of Enterprise Risk Management

B.Grimm Power has incorporated the evaluation of Environmental, Social, and Governance (ESG) risks into our risk management framework. The outcomes of our materiality assessment have been woven into our Enterprise Risk Management (ERM) Process, enhancing our ability to identify and address corporate risks through risk assessment (risk identification) process. The summary of ESG related risks, the materiality topics from materiality assessment, and linkage to corporate risks are as follows:

EGS Risk	Material Topics	Impact level	Risk Category	Risk Items
Social	Corporate citizenship	● ● ●	ESG risk	Community and Social Engagement risk
Economic and Governance	Customer satisfaction	● ● ●	Operation risk	Customer Engagement risk
Economic & Governance and Environmental	Energy efficiency, availability, and reliability	● ● ●	Operation risk	<ul style="list-style-type: none"> › Heat rate and load optimisation risk › Plant availability risk
Economic & Governance and Environmental	Low-carbon portfolio development	● ● ●	Strategic risk	<ul style="list-style-type: none"> › Energy transition risk › Internal Carbon Pricing <u>Risk</u>
Environmental	Biodiversity	● ● ●	Strategic & Operation risk	Environmental impact risk
Economic & Governance	Growth and economic performance	● ●	Strategic risk	Business expansion risk
Social	Talent management and employee welfare	● ●	Operation risk	People risk
Economic & Governance	Governance	● ●	ESG risk	Corporate governance risk

EGS Risk	Material Topics	Impact level	Risk Category	Risk Items
Economic & Governance	Anti-corruption and transparency	● ●	ESG risk	Corporate governance risk
Economic & Governance	Innovation and digitalisation	● ●	Strategic risk	Decentralisation risk
Economic & Governance	Cybersecurity and data privacy	● ●	Operation risk	› Cybersecurity risk › Data security risk
Social	Diversity and equal opportunity	● ●	Operation risk	People risk
Environmental	Water and air management	● ●	Operation risk & Compliance risk	› Safety, Occupational Health and the Environment risk › Environmental compliance risk
Economic & Governance	Sustainable supply chain	● ●	Operation risk	Supply chain risk
Social	Disaster and emergency management	● ●	Operation risk	Natural disaster risk
Social	Occupational health and safety	● ●	Operation risk & Compliance risk	› People risk › Safety, Occupational Health and the Environment risk
Social	Vigilance against forced labour	●	ESG risk	› Governance risk › Employee Engagement risk › Supply chain risk
Environmental	Waste management and circularity	●	Operation risk	Safety, Occupational Health and the Environment risk

Appendix

B.Grimm Power – Significant Corporate Risk Factor

Analysing current risks and identifying potential risks affecting the company, we have identified significant corporate risk factors for the year 2022 as follows:

Risk Factors	Description
Decentralisation	Thailand's power sector is on the brink of decentralisation, as seen in ERC granting LNG supply and wholesale licenses to private firms in 2020. This enhances flexibility and backs decentralisation. However, if decentralisation progresses and local power generation becomes prevalent, demand for formal system power purchase might decrease. B.Grimm Power, mainly reliant on EGAT, readies for these shifts with comprehensive risk assessment and adaptive strategies.
Thailand's Electronic Vehicle (EV) Promotion	B.Grimm Power anticipates the auto industry's transformation from ICEs to EVs, closely monitoring the impact on its power supply to auto-parts manufacturers. With Thailand's support for EVs, the company proactively adapts by diversifying its customer base into sectors like data centers and EV components, ensuring growth, resilience, and contribution to integrated public utilities across industries.

For more detail: Form-56 One Report 2022 as link <https://bgrim.listedcompany.com/misc/one-report/20230324-bgrim-one-report-2022-en.pdf>

Risk Appetite Statement

“A concise declaration that outlines an organisation's willingness and capacity to handle various levels of risk in pursuit of its objectives and goals. It provides a framework for decision-making by indicating the boundaries and preferences regarding risk exposure.”

Risk Perspective	Risk Appetite Statement
Corporate	<ul style="list-style-type: none"> • Our company vision “empowering the world compassionately” together with our core values of positivity, partnership, professionalism and pioneering spirit are the fundamental of our corporate business and operations. • Our corporate pursuits are founded on an unwavering dedication to maintaining transparency, accountability, and steadfast adherence to ethical principles, all subject being assessable. • Central to our corporate approach is the meticulous adherence to regulations and professional standards, encompassing both local and global
Operations	<ul style="list-style-type: none"> • In pursuit of our company mission, B.Grimm Power strives to be a world-class energy producer and solution provider, we embrace controlled risks and steadfastly leverage technology, innovation, and operational optimisation to not only enhance energy efficiency but also achieve our strategic goals. • To engage in business while prioritising safety, health, and well-being, and ensuring prevention of environmental harm. • To manage cyber security and data security with pertinent international standards which mitigate risks that could impact business reputation and operations.

Risk Tolerance Levels

“Risk tolerance levels refers to an organisation's or individual's capacity to endure or accept the uncertainty and potential negative outcomes associated with a particular level of risk.”

Risk Perspective	Risk Tolerance Levels	
Corporate	Compliance	<p>No regulatory breaches will be tolerated.</p> <p>We will ensure full compliance with all relevant regulations and standards, both at local and global levels.</p>
	Fraud and Corruption	<p>Zero tolerance for any form of fraud or corruption .</p> <p>We are committed to maintaining the highest ethical standards across all business activities.</p>
Operations	Operations	<p>Zero tolerance for process safety incidents impacting stakeholders.</p> <p>Our operations are structured to ensure the safety and well-being of all stakeholders, and we strive to eliminate incidents that could compromise this commitment.</p>
	Cyber Security	<p>Cybersecurity incidents with potential to harm our reputation and assets are not tolerated.</p> <p>We are dedicated to maintaining robust security measures to safeguard against such risks.</p>

Risk Management Training for Non-executive Directors

Training & Seminar Program	Objectives	Lecturer	Category
Intro to Risk Management	The course aims to cultivate a comprehensive understanding of the value and significance of Risk Management. This will empower learners to initiate risk management practices within their organizations.	Dr. Awirut Chatmarathong	Business Function
Risks & Opportunities for ISO	The course is tailored to aid in managing risks and opportunities according to ISO 31000: Risk Management standards. It covers ISO standards such as 9001, 14001, and 45001, offering versatile techniques applicable in diverse organizational contexts upon completion.	The Industrial Thinker	Business Function
Digital Transformation Risk	To learn about the power of technology that could reshape the landscape of their future work, enabled them to adjust their perspectives and ways of thinking in the digital age and helped them learn essential digital skills through seven online workshops titled "Shift Your Digital Mindset".	B.Grimm People Partnership	B.Grimm Foundation
B.Grimm 101: Code of Conduct	To provide advice on relevant policies and guidelines in order to enhance directors, management and staff to perform their duties and responsibilities in compliance with corporate governance policy, anti-corruption policy, sustainability policy, risk management policy, digital technology policy, cyber security policy, and anti-corruption policy.	B.Grimm People Partnership	B.Grimm Foundation
Personal Data Risks	Mandatory training to understand of the roles and responsibilities, regarding privacy data protection laws and regulations. (PDPA basic, PDPA cases, and PDPA for executives)	KPMG Phoomchai Business Advisory Ltd./ Boston Network	Managerial/ Digital Literacy
Cyber Security Risks	IT security awareness training to keep employee up to date, raise their awareness of various cyber threats, and enable them to use our information infrastructure and network properly and in accordance with our policies and procedures include the information on pertinent laws and regulations.	B.Grimm People Partnership	B.Grimm Foundation
Climate Related-risks	To make informed decisions for enhancing business resilience, integrating climate considerations into strategic planning, meeting stakeholder expectations, ensuring regulatory compliance, understanding financial implications, identifying innovation opportunities, and maintaining a positive global reputation.	The Creagy	Business Function
Risk Prevention and Management	Promote the development of knowledge and understanding of Risk Management and Mitigation Plan. (Sharing on Townhall Day)	Mr. Anuwat Jongyindee	Business Function
Strategic Risk Management	To ensure executives comprehend the risk management process, how it supports the company goals, their role and responsibility in fortifying the effectiveness of the risk management process (Decision-making in Risk Management, COSOERM & ISO31000 International Risk Management Framework)	TRIS Academy	Business Function