NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

CyberSG R&D Programme Office (CRPO)

Grant Call Launch

December 12th, 2023

Programme

- 3:00 pm **Welcome**
- 3:10 pm **Overview on the CRPO Grant Call**
- 3:30 pm **Q&A**
- 4:00 pm **Networking and Light refreshments**
- 5:00 pm **End of Programme**

CyberSG R&D Programme Office (CRPO)

Overview

CyberSG Overview

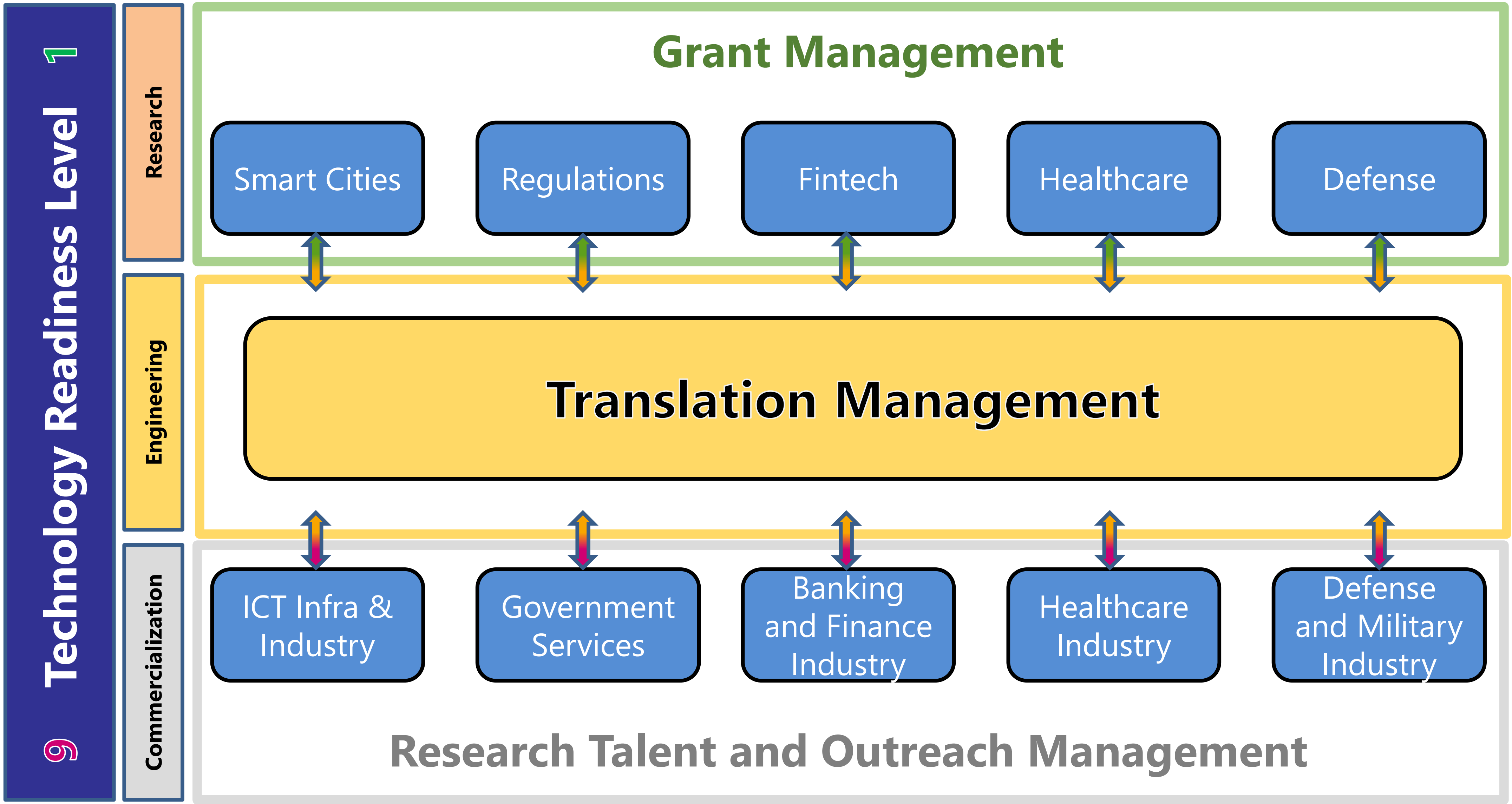
- CyberSG R&D Programme Office (CRPO)
  - spearheaded by CSA, NTU, and their affiliated organizations
  - forefront of cybersecurity development and implementation

- CRPO → acts as a research translation center
  - facilitating the translation of research outputs and,
  - establishing a governance framework for managing all translational activities

- CRPO → aims to create
  - an ecosystem supporting talent flow, development, and communication

- Covering the entire TRL spectrum
  - from TRL 1 to TRL 9 in cybersecurity

CyberSG Overview



CyberSG Overview

Frontier Research and Development

- Anchor fundamental research into next generation core cybersecurity capabilities
- To achieve technological and scientific excellence in cyber security
- Fund moon-shot and grand challenges for greater good of society

Translation and Industry Driven Technology Development

- Identify and translate high-potential IPs from fundamental research for commercial applications
- Establish a cybersecurity innovation platform and APIs for adoption by local public and private sector companies
- Drive the growth of the cybersecurity industry through translational grant management, including demos and field trials with governmental and private partners

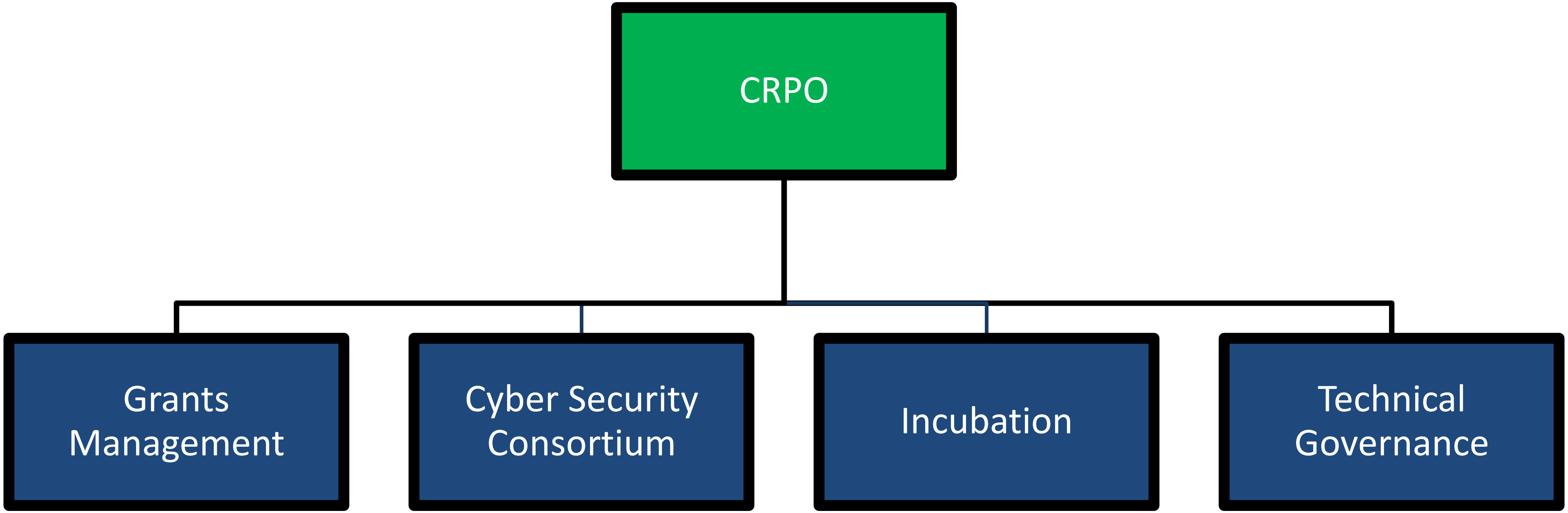
Ecosystem/Industry Development and Training

- Showcase cybersecurity capabilities with downloadable APIs and field trials for local SMEs
- Foster a robust cybersecurity startup ecosystem through incubators, training, certifications, and hackathons
- Develop and promote cybersecurity talent through industry training, awareness campaigns, and talent pool enhancement

CRPO Verticals

- **Open Sharing Platform**
- **Scientific and Technical Excellence**

- **Value Creation in Singapore**
- **Value Capture in Singapore**



CRPO

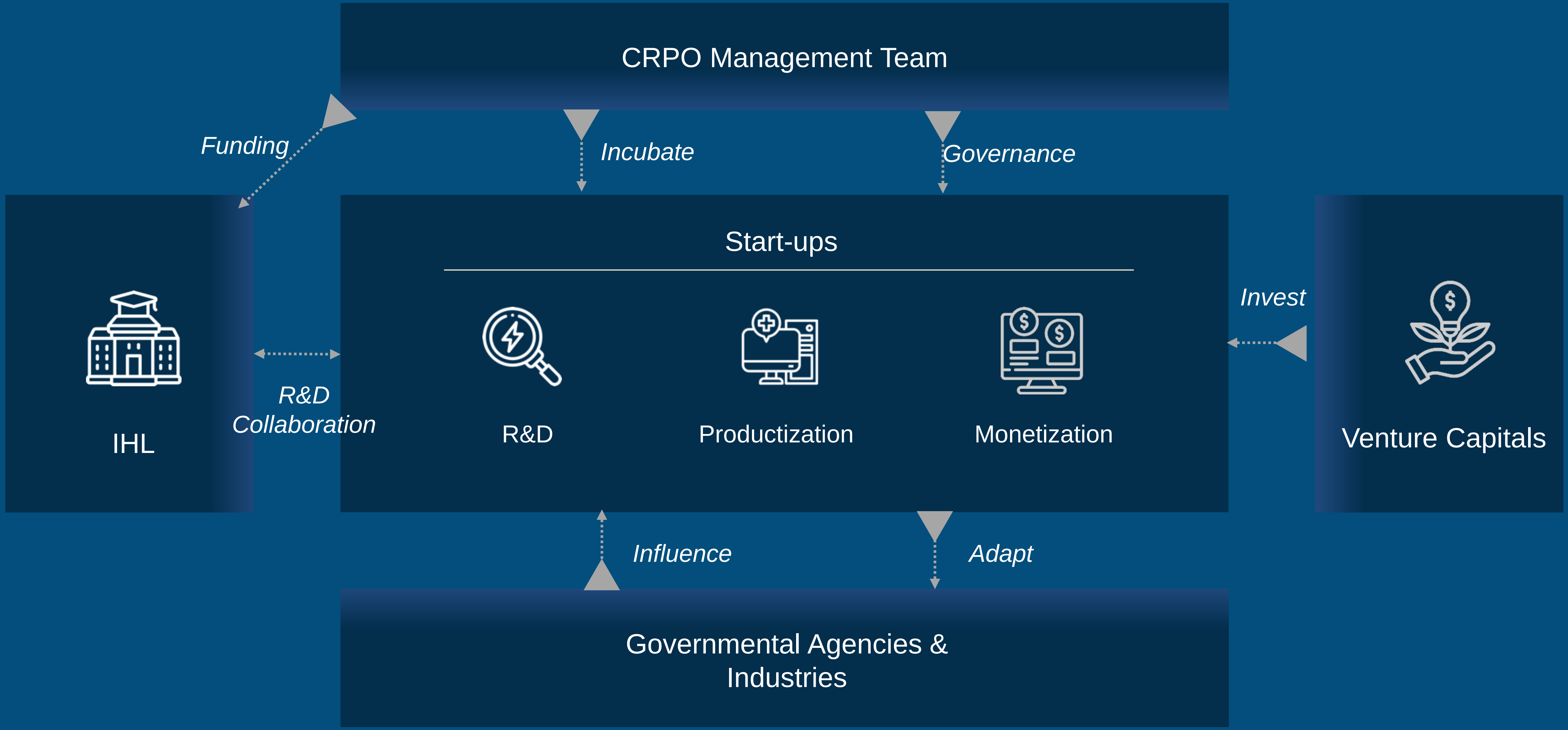
Grants Management

Cyber Security Consortium

Incubation

Technical Governance

CRPO will be the incubator of cybersecurity R&D and Translation in Singapore



CRPO Management Team

Funding

Incubate

Governance

IHL

R&D Collaboration

Start-ups

R&D

Productization

Monetization

Invest

Venture Capitals

Influence

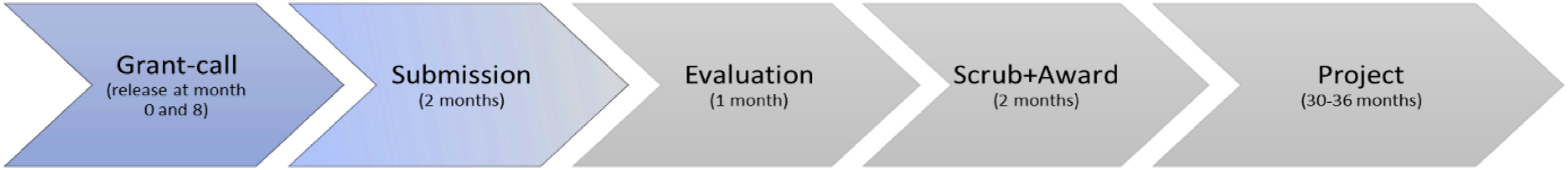
Adapt

Governmental Agencies & Industries

Grant Call Overview

Grand Challenges Grants (2 Teams)

- **Grand Challenges Grants (2 Teams)**
  - to address challenges with significant industrial and societal impact
  - current (if short-term) or future (if long-term) governmental challenges or initiatives
  - up to SGD$6,000,000 for one selected research team for a duration of 2.5-3 years



Grant-call (release at month 0 and 8)

Submission (2 months)

Evaluation (1 month)

Scrub+Award (2 months)

Project (30-36 months)

AI Security

- **Motivation**

  - ✓ AI models, including foundation models, have been applied in various real-world domains, such as autonomous vehicles, smart grids, industrial automation and smart healthcare

  - ✓ The proliferation of foundation models, such as GPT-4 and PaLM, has significantly transformed the landscape of Artificial Intelligence

  - ✓ The widespread deployment of foundation models has engendered a series of novel cyber-attack challenges that could have profound consequences for society, security, and privacy

AI Security

➢ Challenge Statements

- ✓ **Adversarial Manipulation:** Adversarial attacks exploit vulnerabilities in foundation models by introducing carefully crafted input perturbations, leading to incorrect or misleading outputs

- ✓ **Data Poisoning:** Malicious actors may attempt to manipulate the training data used to build foundation models, embedding biased or misleading information

- ✓ **Privacy Breaches:** Foundation models, often trained on large and diverse datasets, might inadvertently expose private or sensitive information contained within their learned representations

- ✓ **Transfer Learning Vulnerabilities:** Pre-trained foundation models are commonly fine-tuned for specific tasks, and such transfer learning can introduce vulnerabilities

- ✓ **AI Security in Real-World Complex Systems**: Real-world complex systems, such as autonomous driving systems, smart grids, intelligent manufacturing systems, and intelligent healthcare systems, are a fusion of AI models and conventional algorithms. The intricate interplay between these components presents unique challenges in the realm of AI security that distinguish it from traditional model-level security.

AI Security

- **Goal: Enhance the robustness of foundation models from different perceptive:**
  - ✓ Adaptive Adversarial Training
  - ✓ Robust Data Validation
  - ✓ Privacy-Preserving Architectures
  - ✓ Fine-Tuning Security
  - ✓ Robustness evaluation and improvement in real-world complex systems
  - ✓ Real-time attack detection and mitigation in real-world complex systems

Secure and Private Data Sharing

- **Motivation**

  - ✓ Break the data-silo and motivate wide collaborations to provide prominent benefits for versatile realms
  - ✓ Drive diverse AI applications, collaborative optimizations, foster large and accurate models
  - ✓ Support scalable operations, cost-efficient resources, and accessible collaboration for cloud computing
  - ✓ Ensure trust, integrity, ownership, and smart contract automation through decentralized transparency in Blockchain network

Secure and Private Data Sharing

➢ **Challenge Statements**

- ✓ **Security of Data Sharing for Intelligent Systems**: Rare existing approaches can guarantee the data confidentiality, integrity and availability (**CIA**) simultaneously to provide provable secure data sharing for AI driven intelligent systems

- ✓ **Privacy Concerns in Cloud Computing**: Numerous deployed applications tend to abuse user data, undermine privacy, and violate regulations (e.g., GDPR). Large-scale shared data introduce significant privacy concerns

- ✓ **Reliable Fairness Guarantees**: Reliable contribution evaluation and incentive mechanisms for large-scale data sharing frameworks like Blockchain and Intelligent Systems lacks sufficient efforts

- ✓ **Efficiency Boosting:** The co-design of algorithm and hard-ware acceleration is rarely touched in existing approaches. High efficiency is paramount for all the intelligent systems or novel computing paradigms such as Cloud and Blockchain

Secure and Private Data Sharing

- **Goal: Guarantee security, privacy and fairness for large-scale data sharing, including the efficient development of :**

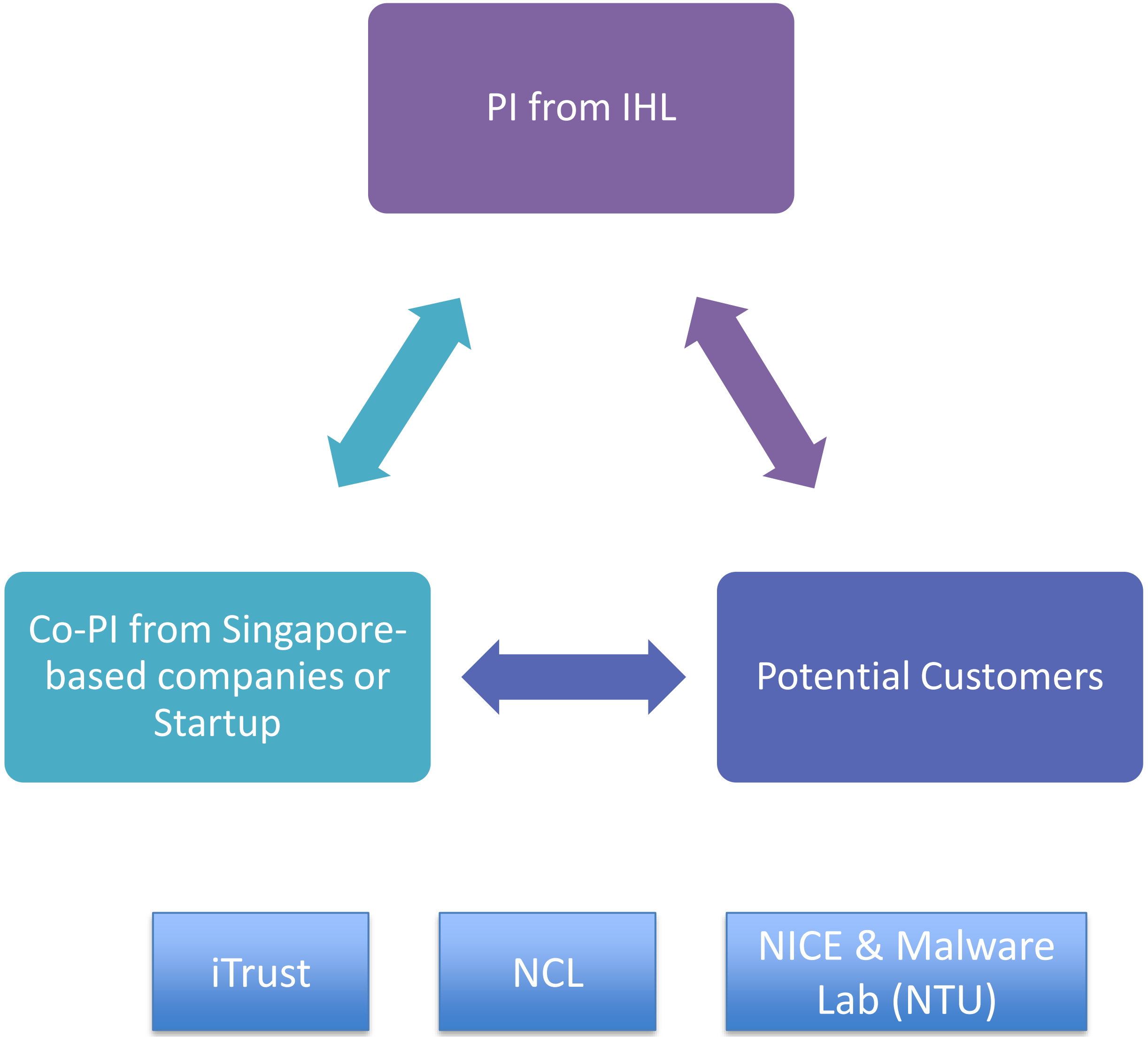
  - ✓ **Secure Data Sharing for Intelligent Systems**
    - Confidential computing framework for the sharing of large-scale training data
    - Formal integrity verification mechanisms for the diverse training and inference paradigms
    - Provable robustness enhancing methods for various data sharing functions with confidential and integrity guarantees

  - ✓ **Private Data Sharing in Cloud Computing**
    - Provable private preserving algorithms with rich data sharing functionalities
    - Fine-grained and dynamic access control that can restrict data sharing to selected individuals/groups
    - Private data sharing as a service enabling diverse cloud driven applications

  - ✓ **Fairness Guarantees for Data Sharing in Blockchain and Intelligent Systems**
    - Design of reliable contribution evaluation mechanisms
    - Deployable incentive mechanisms for large-scale Blockchain and Intelligent System
    - Provable security and privacy guarantees for fair data sharing

Team Structure Requirements

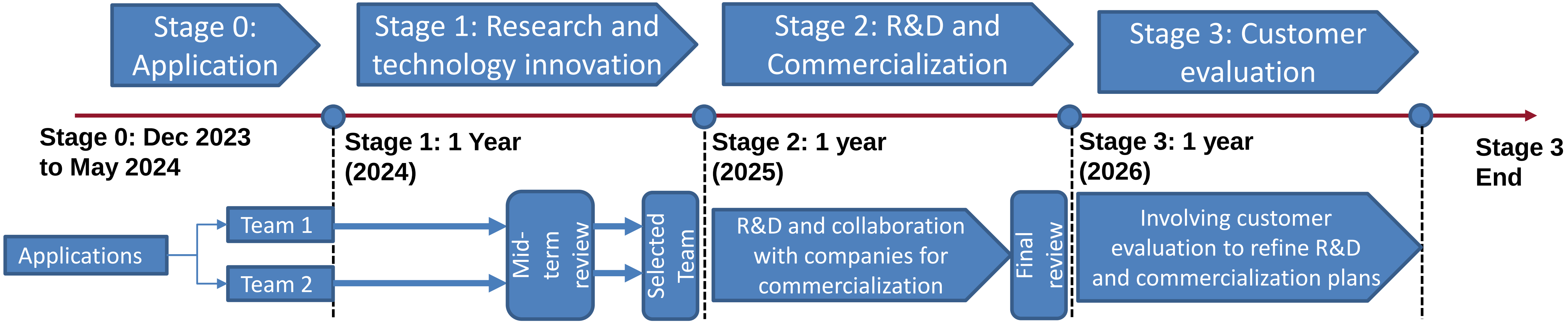
- One Lead-PI from Singapore-based Institutes of Higher Learning (IHLs) and Research Institutes (RIs) to conduct fundamental research
- One industry Co-PI from Singapore-based companies to identify and translate IPs with commercial potential
- Potential customer collaborators who are willing to adopt the developed security solutions and provide requirement feedbacks
- iTrust, NCL can be the partner to provide platform and data



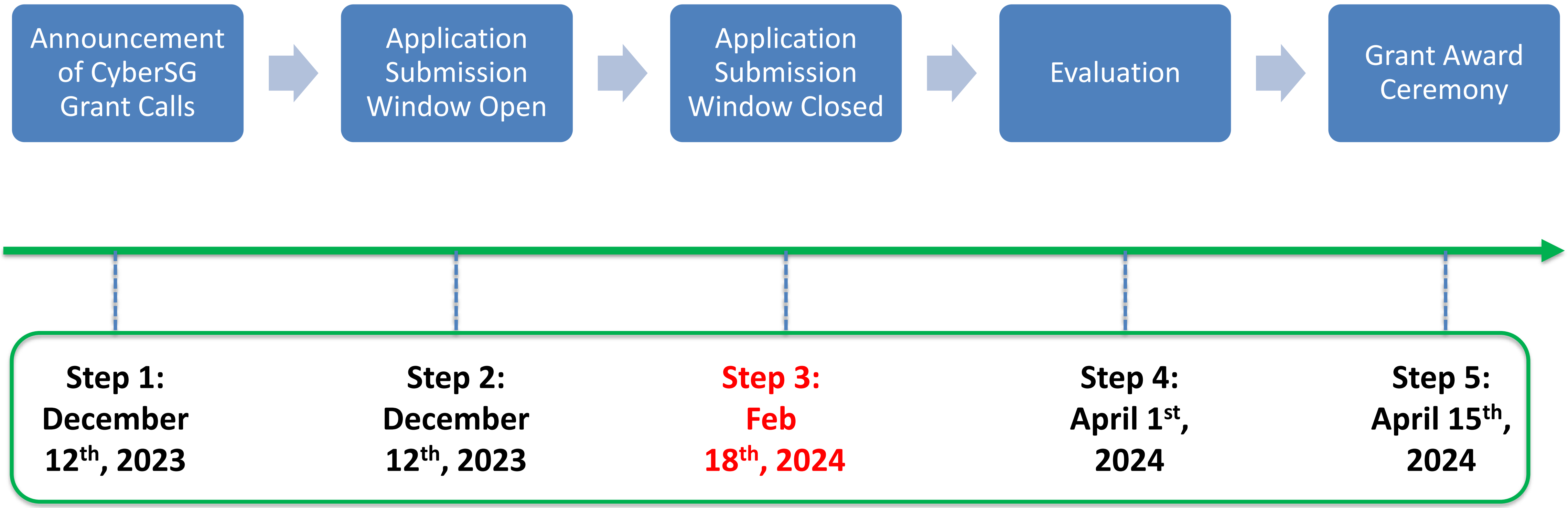
Programme Structure

- 2 successful teams will undergo a mid-term review on its project progress approx. 12 months into the challenge
  - Funding for Stage 2 will only be unlocked upon satisfactory progress
- Nearing the end of Stage 2, approx. 24 months into the commercialization, the team will undergo a final review
  - Eligibility for further support in Stage 3 will be assessed based on final review
- Nearing the end of Stage 3, approx. 36, the team is expected to provide mature products atop the R&D outputs
  - Receive benefits from marketplace and enter a virtuous cycle of R&D and commercialization

Grant Review Process


Stage 0: Application
Stage 1: Research and technology innovation
Stage 2: R&D and Commercialization
Stage 3: Customer evaluation
Stage 0: Dec 2023 to May 2024
Stage 1: 1 Year (2024)
Stage 2: 1 year (2025)
Stage 3: 1 year (2026)
Stage 3 End
Applications
Team 1
Team 2
Mid-term review
Selected Team
R&D and collaboration with companies for commercialization
Final review
Involving customer evaluation to refine R&D and commercialization plans

Grant Management Timeline



Announcement of CyberSG Grant Calls

Application Submission Window Open

Application Submission Window Closed

Evaluation

Grant Award Ceremony

Step 1: December 12th, 2023

Step 2: December 12th, 2023

Step 3: Feb 18th, 2024

Step 4: April 1st, 2024

Step 5: April 15th, 2024

Evaluation Criteria

Proposals Should Follow Strict Guidelines and Clear State the Following:

- Alignment of proposal to CRPO's objectives and direction
- Novelty of the research and the needle-moving research challenge that the proposal will solve
- Industry Partner to each proposal and Potential Industry Application or Impact
- Potential End Customer
- Translation Plan, Timeline and Know-how of deployment
- Relevance of the research to Singapore

Project Deliverables and Outcomes

Each project is expected to produce most, if not all, the following deliverables:

- **Translation, Technologies deployed, including licences.**
- Industry R&D jobs.
- Publications in top journals/conferences.
- PhDs & Masters trained.

Eligibility

- The grant call is open to researchers from all Singapore-based IHLs and RI
- PI and Co-PIs must hold full-time appointments in one of the above
- Singapore based companies and start-ups in Singapore are eligible to be industry partners
- Private sector, MNCs and start-ups, researchers from Medical Institutions, and other entities are eligible to apply as Collaborators
- Overseas collaborators and/or visiting experts may be invited to Singapore to assist with specific project tasks
- Only research conducted in Singapore may be funded
- Parallel submissions are not allowed

CRPO Intellectual Property Arrangements

- Solely Developed Solely Owned
- Joint Developed Joint Owned
- Public Sector IP Arrangement

→ CRPO: Non-Exclusive Commercialization Rights

Project Support

- CRPO is equipped with common research engineering capabilities to facilitate or support the community:

- Advice on opportunities for translational efforts
- Testbed support
- Industry contacts and matchmaking
- Fast prototyping
- Product Evaluation

For more information, please contact CRPO@ntu.edu.sg

Q&A?

Questions and Answers?

1. Can a company be collaborator of the grant call?
   - Yes

2. Is it mandatory to have industry partner for participating in grant call?
   - Yes

3. Is it mandatory to have potential end customer?
   - Yes

4. Are different RIs or IHLs encouraged to work together to jointly submit a proposal?
   - Yes, but not mandatory

5. Can a person only be involved in one project?
   - For research staff, a person can be involved in more than one project and staff costs should be charged based on time commitment to the research. In terms of NRF guidelines, there are no restrictions on PI/Co-PI being in involved in more than one project

Thank You