In short:

Like any such effort:
Build a strategic plan that stretches 36 months expecting changes and mods - structure this with specific goals, objectives, and intended outcomes

- Measure maturity over the 36 months
    - Do not strive for 5s since to do so is usually:
        - Achievable once but not maintainable
        - Comes at too high a cost
        - Expends too much energy on one area for a one time gain
            - Diminishing returns set in usually at about 3.5
            - You will burn people out
            - Other areas will suffer
            - So what

Organizationally place as supporting the whole business aligned with competitive and business intelligence not buried inside IT or Infosec

- Dotted line to CISO/CSO as required
- This lays the groundwork for building an internal 'community of interest' across corporate intelligence functions

Gain acceptance and funding
Define what intelligence is and is not
Define what intelligence can do an cannot
Define how your team will work with stakeholders
Define how your stakeholders need to work with your team
Ensure reporting includes briefs to leadership that are truly briefs
Clearly define your program based upon intelligence community standards

- Glossary, taxonomy, and common language required
- Communicate this with all stakeholders, internal partners, and communities of interest

Hire the right people

- Understanding the difference between all-source intel, DHS, CIA, NSA, DÍA, LEO and all intel groups
    - Do not hire all from one industry

        - All from gov for an example may bring a myopic view of intelligence
- Align the hiring to the intelligence lifecycle
    - Build a sustainable model for continued education, training and growth
    - Do not become top heavy

Determine and prioritize stakeholders

- Define PIRs and determine gaps

Assess for existing capabilities across all functions including technology

Build your intel model on 4 areas:

- Strategic
- Operational
- Tactical
- Technical

Define initial integration points with other groups that will provide information (RFIs)

Select initial technologies and perform a POC to prove the capabilities and features

Deploy and bleed the functionality out of any/all technologies

- If acquiring a TIP
    - Ensure ease of use, proper support, ability or it to grow into a product that supports as much of the intelligence cycle as possible
        - Understand the errors in STIX/TAXII with respect to data, confidence, etc., as it was not built by intel professionals
        - Utilize an integrated version of the Diamond Model and Kill Chain with IR and the SOC
            - Incorporate ATT&CK if not already incorporated within the TIP
        - Ensure the TIP can produce reports that follow the BLUF and AIMS models (SITREPs, TACREPs, SENSREP, Intelligence Advisories, etc.)
        - Ensure the TIP supports your ability to build workflows based upon your SOPs and subsequent process flow diagrams
        - Ensure the TIP is able to easily build communities for sharing data
        - Ensure the TIP has all the prerequisite capabilities to address IoCs (technical intel) while fully incorporating TTPs (tactical intel)

Author your SOPs with clear RACIs, process flow diagrams, examples

Define your products and product line mapping avoiding as much as possible serialized reporting

- Reports & briefs based upon PIRs and prioritized stakeholders
    - Start with intelligence advisories, situation reports, tactical reports, sensitive information reports
    - Collect information on past incidents
        - Look to establish patterns
            - Within the patterns determine if there are trends

Begin delivering reports accompanied with standard report feedback forms

- Strategic products to stakeholders based upon business need
- Operational and Technical to Crisis Management, Incident Response, Security Operations, Risk Management, Threat and Vulnerability Management, etc.

- Support each with intelligence products and services as defined in the SOPs and to the RACIs that should define OLAs and underpinning agreements
    - SOPs should follow the intelligence lifecycle
        - Collection planning
            - Priority intelligence requirements – Specific information requirements
            - Collection management, requirements management, mission management
            - Collection tools and methods
                - Internal data feeds
                - Threat intelligence platform data feeds
                - Open source collection
                - Dark net collection
            - Oversee collection activities to maintain relevancy while ensure data validity and credibility
        - Production management
            - Critical thinking
            - Cognitive bias
            - Methods of reasoning
        - Structured analytic techniques
            - Use when time allows and based upon need
        - Analytic methods
        - Analytic writing
            - Internal peer reviews
            - Analytic writing style guide
- Tactical to build adversary and campaign models
    - Align to technical needs
    - Integrate where applicable to competitive and business intel
    - If applicable, align with any physical security requirements
    - Determine tactics, techniques, and procedures of your adversaries
        - Extract tendencies and track
- When delivering reports, properly classify and insist on holding a corresponding briefing to explain report contents for clarity and understanding
- Continually assess your data, information, and intelligence preparing for periodic estimating intelligence reports delivered 1 month prior to budgeting season

Over communicate with all other teams

Consistently demand feedback on products and services

After action reviews should happen at any time:

- If something positive happens procedurally or process wise, stop and document it when it occurs – conversely, address issues when they occur not at the end of an effort

Understand it is okay to make mistakes, just do not make the same ones repeatedly

Do not deliver garbage – best to be late than known for poor work

Deliver actionable intelligence understanding that data feeds deduplicated, normalized, and enriched prior to determining internal sightings is not intelligence but cyber hygiene and a standard requirement, i.e., this is not your job but that of IR and/or the SOC

This is merely a shell outline but should start to answer your question.

T71