THREAT INTELLIGENCE PROGRAM CHECKLIST

1. Biannual process in place to derive, update and capture prioritized intelligence requirements (PIRs) that map to your organization's business risks.
2. Tracking of ad hoc requirements that meet and do not meet standing PIRs in order to identify emerging intelligence needs and requirements.
3. Documented intelligence production requirements.
4. Documented collection requirements.
5. Documented mapping of collection requirements to internal teams/capabilities or external (intelligence) providers/vendors (guidance).
6. Regular assessment and tracking of guidance versus output from internal capabilities and external (intelligence) providers/vendors (collection management).
7. Intelligence collection is easily consumable, i.e. in a threat intelligence platform (TIP).
8. Documented intelligence production style guide.
9. Documented intelligence review and editing process.
10. Formalized intelligence product style and templates.
11. Intelligence products include future predictions and doesn't just report on facts.
12. Sources used in intelligence products are linked to the relevant source and graded.
13. Knowledge gaps are identified in intelligence products and pushed back into the requirements part of the intelligence cycle.
14. Feedback is received from your intelligence consumer/customer and used to drive further intelligence collection and production if needed.
15. Key Performance Indicators (KPIs) are generated for the intelligence program.
16. KPIs are generated for each part of the intelligence cycle including for internal and external sources of finished intelligence products and intelligence collection.
17. Have an intelligence (collection) management function that tracks and prioritizes requirements and tasks them as assigned guidance.