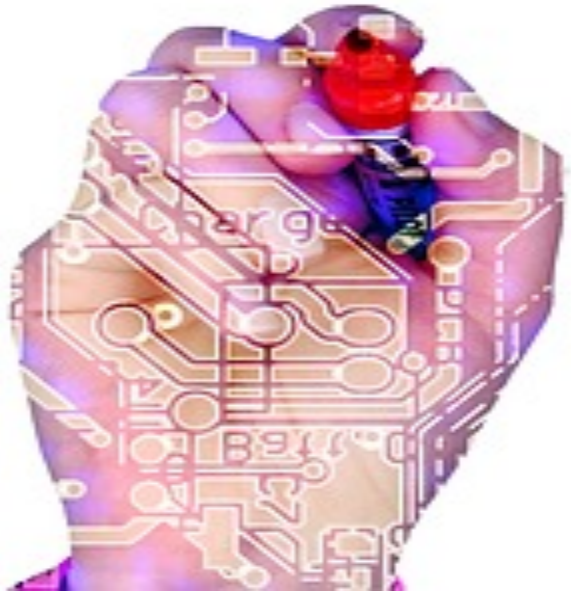
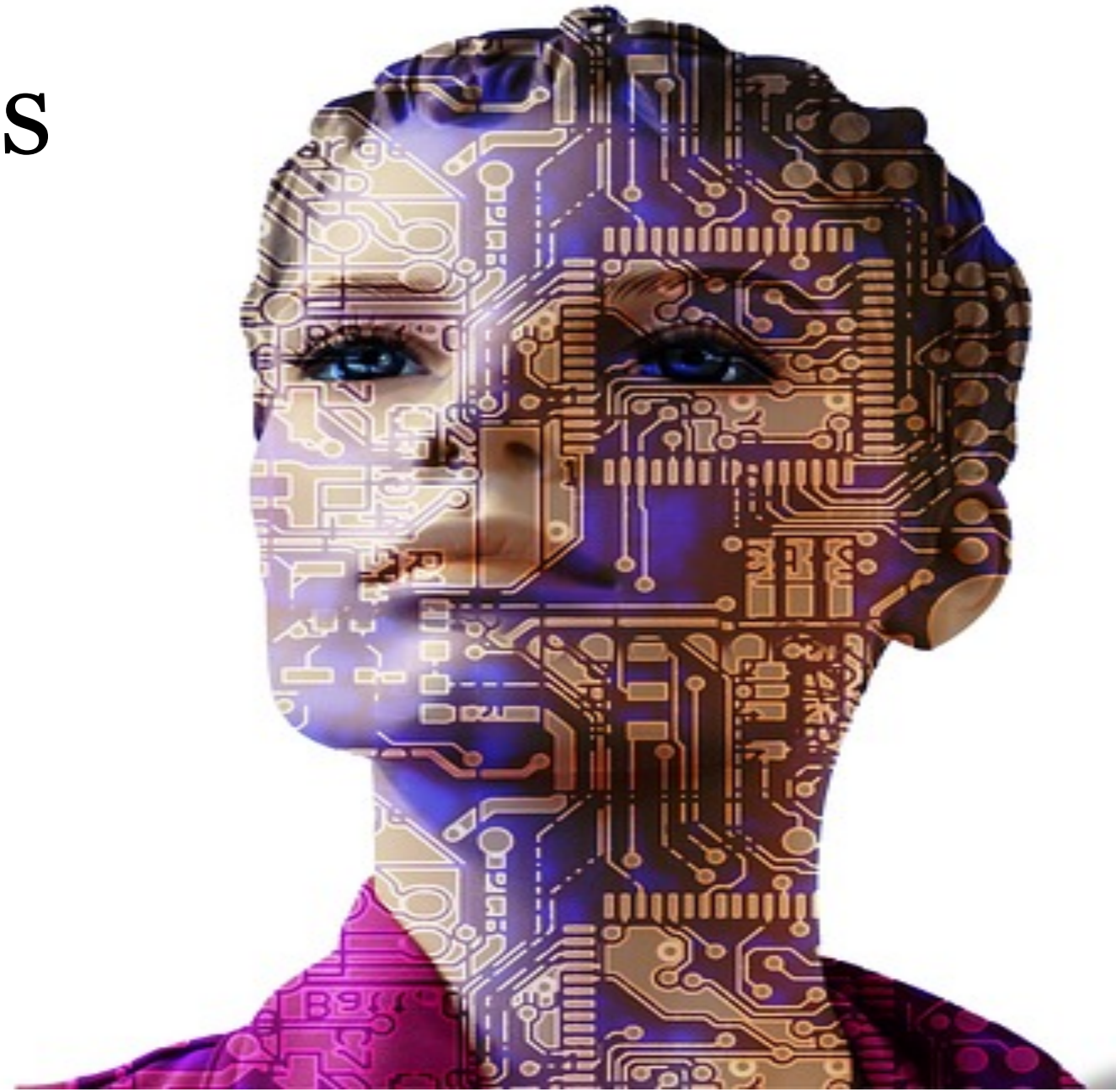
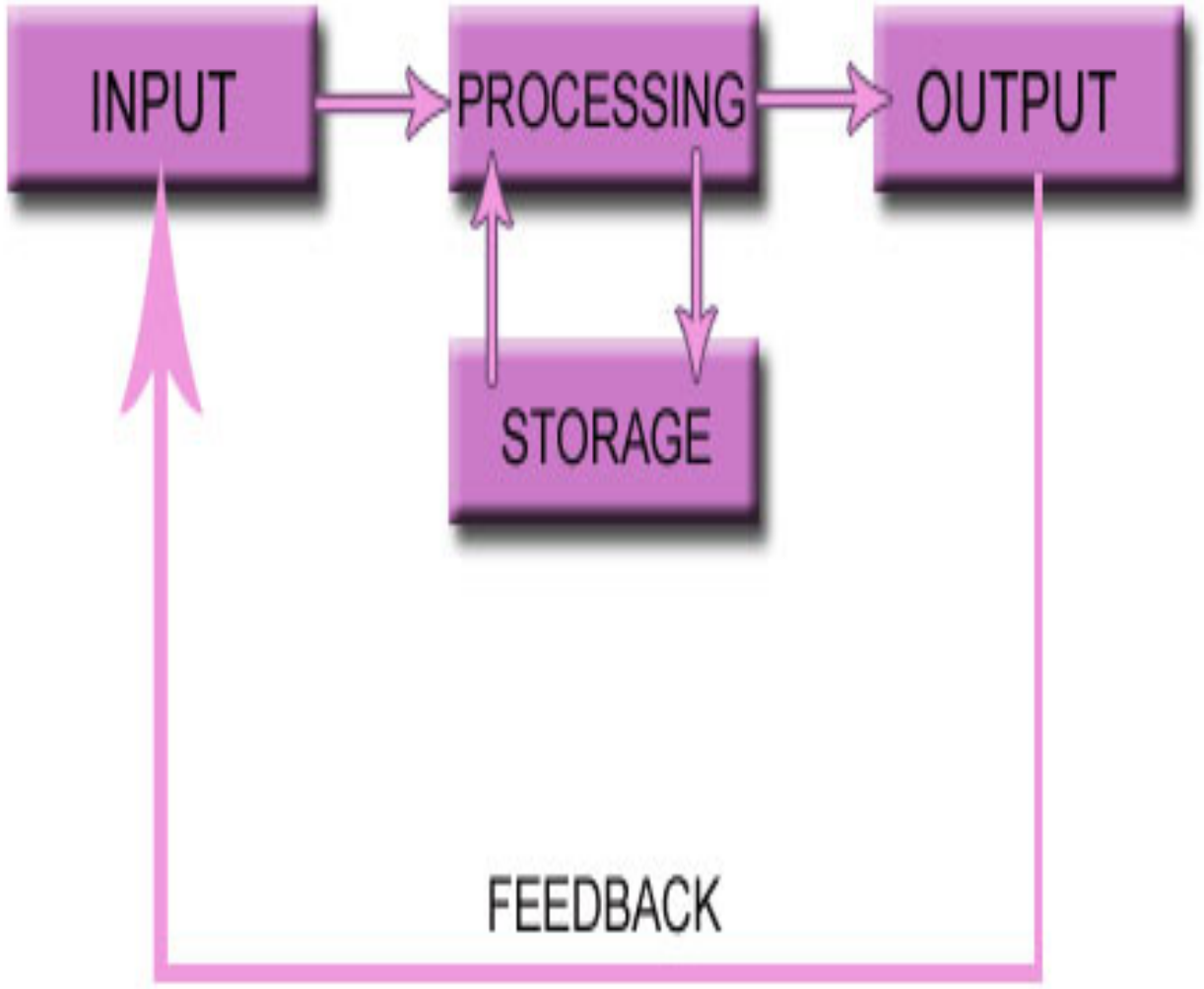
Training Humans To Be Machines





Dr. Stephanie Carter
CISM, CISSP, CISA

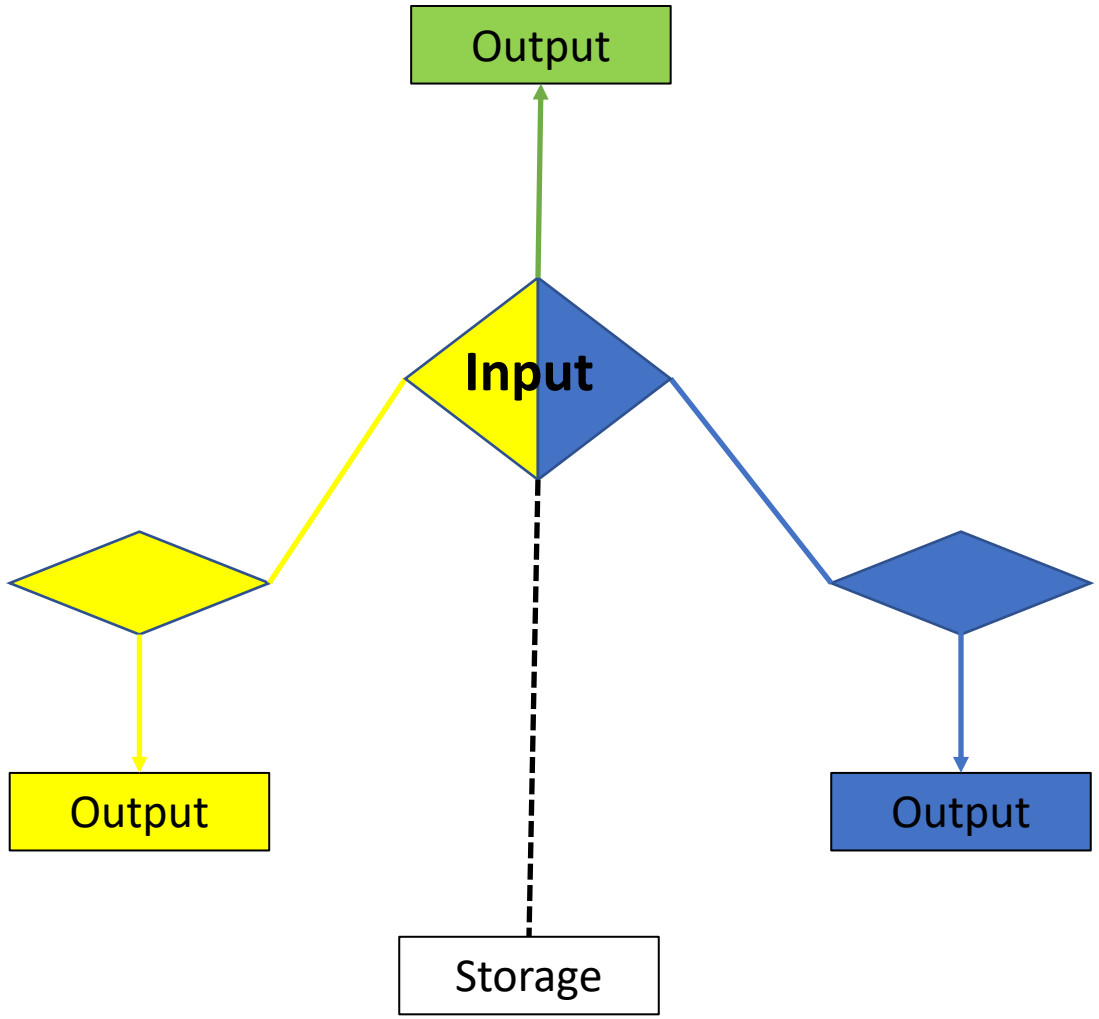
Machine Input/Output



- Input is based on the specific output
- Input is processed without choice
- Output demands stringent input
- Output determines if input stays the same or will change
- Output receives analysis or feedback
- Storage designed to make output more efficient
- Everything is stored
- Storage doesn't change until input changes

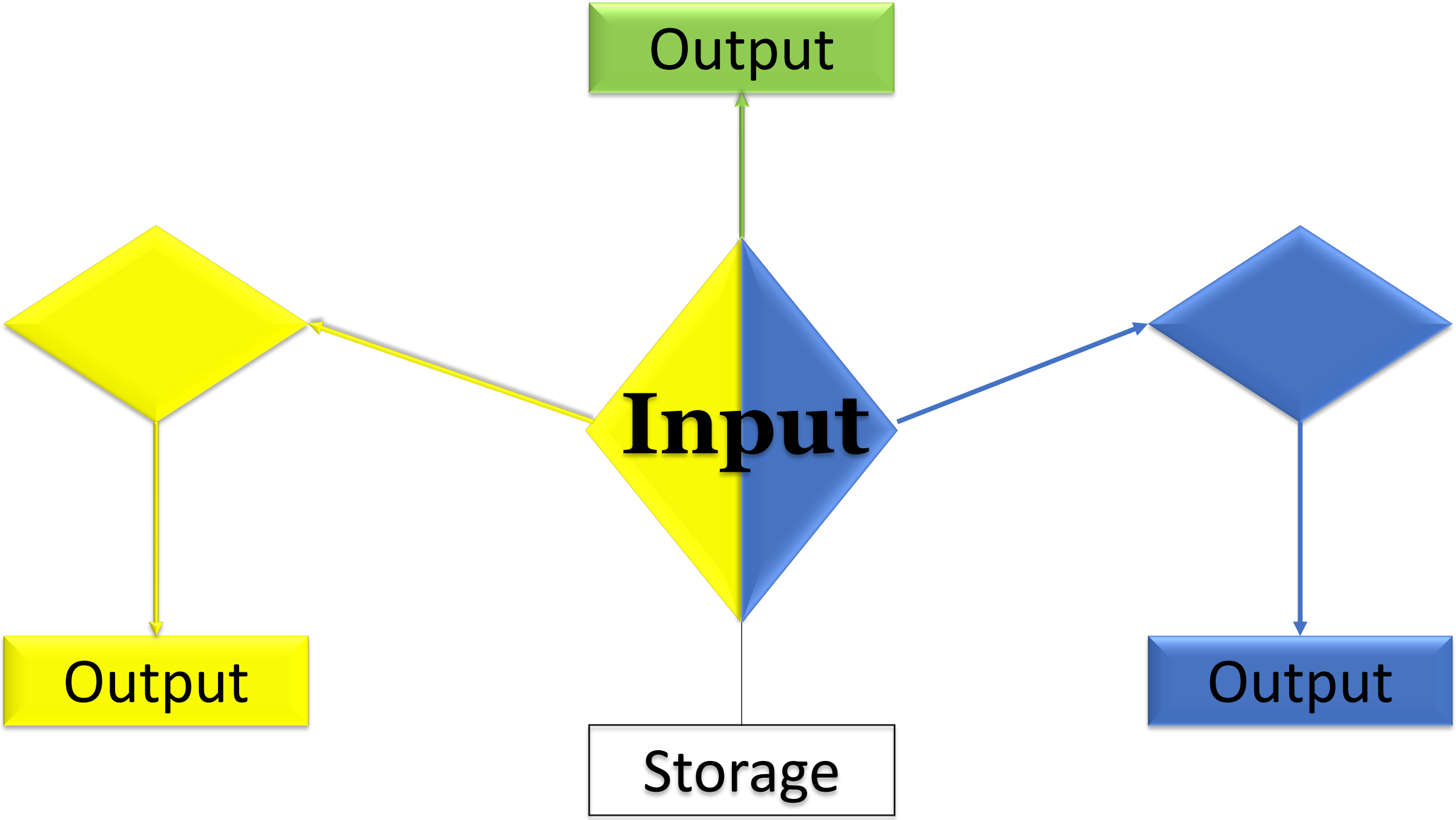
Human Input/Output

- Input has nothing to do with output; output has nothing to do with input
- Input is only processed if a decision is made to process it
- Output requires no specific input
- Output will determine if input will be required again
- Output is reacted to
- Storage only happens if input is pleasant
- Only what is pleasant is stored
- Storage can change if input never changes



Learning Styles

- Visual (seeing)
- Aural (hearing, listening)
- Verbal (talking, reading)
- Physical (touching, doing)
- Logical (thinking, figuring out)
- Social (focus groups)
- Solitary (self-learning)


Output
Input
Output
Output
Storage

Blame Culture

1. 1-hour computer-based training
2. 10 question test

Security Awareness & Training

1. Visual
2. Aural
3. Verbal
4. Physical
5. Logical
6. Social
7. Solitary

Security-focused CULTURE


Don't Do
Anything Stupid

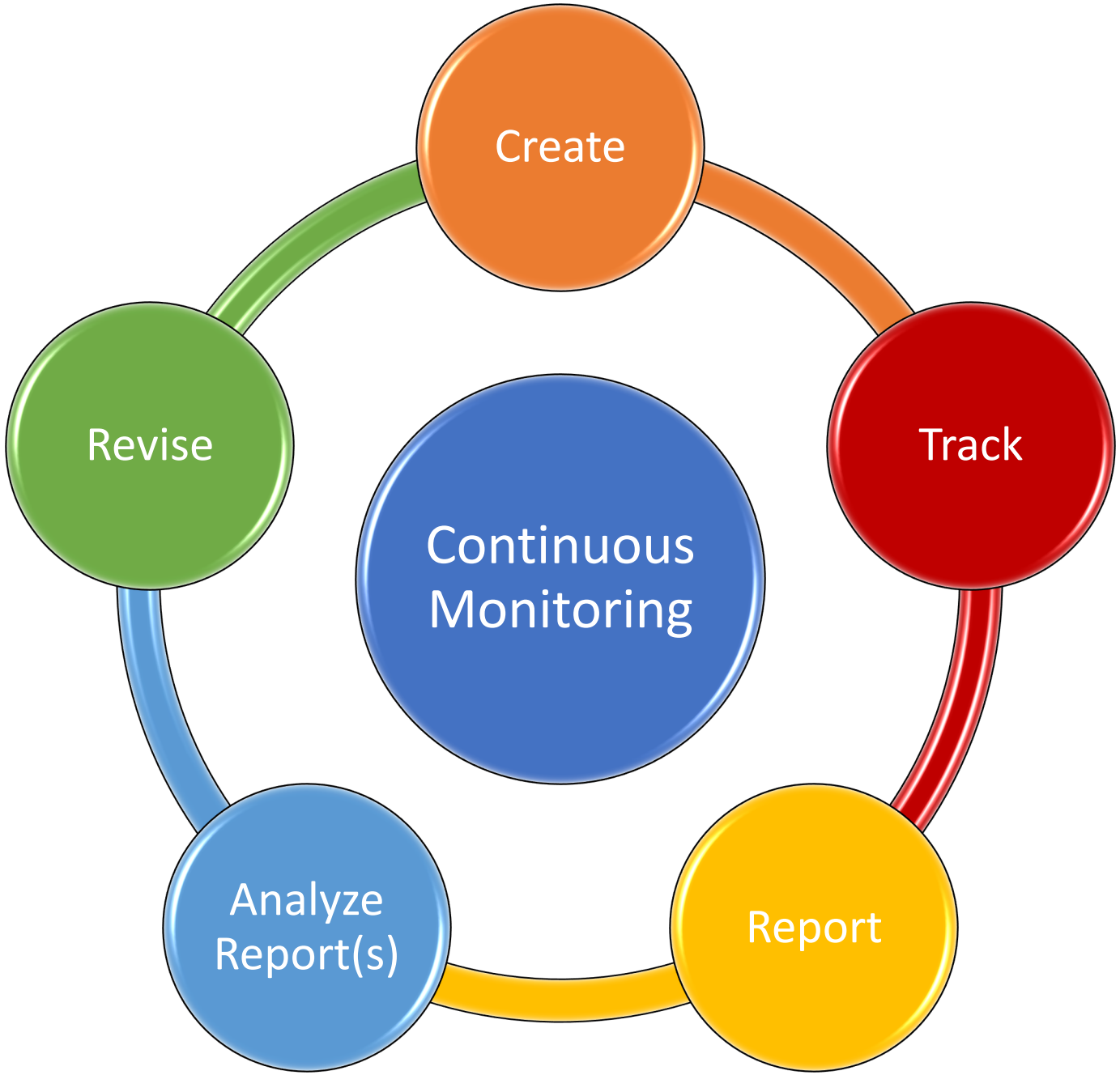
Creating Effective Training

Make your organization security aware

1. Create a Security Awareness & Training Policy
   - Define security awareness & training manager
   - Define minimum training requirements for all employees and special roles
   - Define minimum requirements for training
     - Automation
     - Require sign-in rosters
     - Require signatures at conclusion of training
   - Define reporting standards and timelines
   - Define key performance indicators
   - Define penalties for non-compliance
   - Define minimum training requirements for the organization
   - Require yearly read of policy with acknowledgement signature
     - Read policy in all training (or parts of it)
2. Communicate Reporting Metrics to Organization

Create a Security Awareness & Training Plan

1. Define your organization's security lifecycle
2. Define training objectives
3. Define types of training
   - Preferably based on learning styles
4. Define training period
5. Identify success metrics and critical success factors
   - What will make training effective?
   - What must training possess to be effective?
   - How must training be conducted to be effective?
6. Identify Key Performance Indicators
   - Developed by expected results of training as an organization
   - What does training do or expected to do for the organization?
   - What are the indicators that training is successful?
7. Identify Reporting Metrics
   - Identify who receives what reports
   - Define information to be included in each report


Create
Track
Report
Analyze Report(s)
Revise
Continuous Monitoring


COMPLIANT
NON-COMPLIANT
NON-COMPLIANT
NON-COMPLIANT
NON-COMPLIANT


RISK

QUESTIONS?