PUG
CHALLENGE
EXCHANGE
AMERICAS

# Disaster Planning and Incident Handling using Gaming Concepts

Michael Solomon, Ph.D.

June 2017

# Your speaker

- *Michael Solomon, Ph.D.*

  *CISSP PMP CISA*
- *Solomon Consulting Inc.*
  - *OpenEdge, Roundtable, Security architecture*
    - *Since 1988 (Progress Version 4)*
  - *CyberSecurity Simulation attack team leader*
    - *Penetration testing, attack detection and response*
- *Emory University*
  - *Assured Information Management and Sharing (AIMS)*
  - *Private location proximity detection research*
- *University of the Cumberlands*
  - *Associate Professor, Master of Science in Information Systems Security program*

SolomonConsulting
Securing your world

EMORY
UNIVERSITY

UNIVERSITY
of the
CUMBERLANDS

# Agenda

- Active learning – why bother?
- Can gaming really help with the boring stuff?
- What will it do for me?
- OK, “I want to go to there”

  - Liz Lemon

You've heard this before

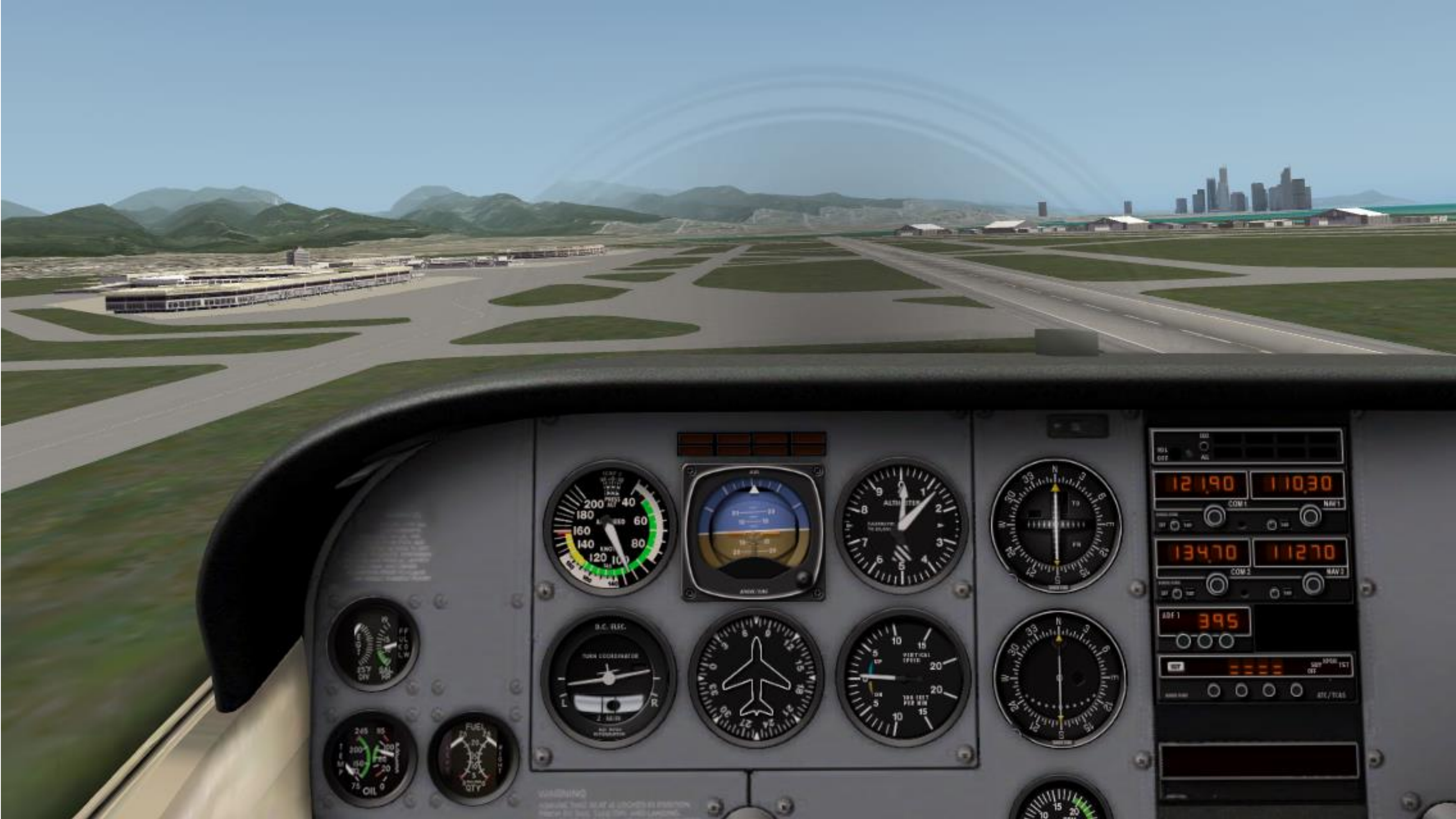
Two easy steps:

1) Make a plan

2) Follow the plan

# Question 1:
# Do you have a written BCP/IRP?

**Responding to incidents is all about minimizing surprise and confusion.**


121.90
110.30
COM 1
NAV 1
134.70
112.70
COM 2
NAV 2
ADF 1
395
AIRSPEED
KNOTS
ALTIMETER
D.C. ELEC.
TURN COORDINATOR
L
R
2 MIN
VERTICAL SPEED
100 FEET PER MIN
UP
DN
FUEL
QTY
OIL
ATC/TCAS
WARNING

### ENGINE FAILURE DURING TAKEOFF ROLL

| Challenge | Response |
|---|---|
| Throttle | IDLE |
| Brakes | APPLY |
| Wing Flaps | RETRACT |
| Mixture | IDLE CUT-OFF |
| Fuel Shutoff Valve | PULL OFF |
| Magneto Switch | OFF |
| Master Switch | OFF |

### ENGINE FAILURE IMMEDIATELY AFTER TAKEOFF

| Challenge | Response |
|---|---|
| Airspeed | (flaps up) 65 KIAS |
| Mixture | IDLE CUT-OFF |
| Fuel Shutoff Valve | PULL OFF |
| Magnetos | OFF |
| Wing Flaps | AS REQUIRED |
| Master Switch | OFF |

### ENGINE FAILURE IN FLIGHT

| Challenge | Response |
|---|---|
| Trim for Best Glide | 65 KIAS |
| Pick Suitable Landing Site | |
| Fly Toward Landing Site | |
| Fuel Selector | BOTH |
| Fuel Shutoff Valve | IN |
| Mixture | AS REQUIRED |
| Fuel Pump | ON |
| Magnetos | ON / BOTH |

IF NO RESTART OR AN OFF AIRPORT LANDING IS NECESSARY:

### ENGINE FIRE IN FLIGHT

| Challenge | Response |
|---|---|
| Mixture | IDLE CUT-OFF |
| Fuel Shutoff Valve | OFF / PULL OUT |
| Fuel Pump | OFF |
| Vents Heat / Air<br>(except wing root vents) | CLOSED |
| Airspeed | 100 KIAS |

(If fire is not extinguished, increase glide speed to find an airspeed which will provide an incombustible mixture.)

| Challenge | Response |
|---|---|
| Forced Landing | EXECUTE |

SEE ENGINE FAILURE IN FLIGHT: NO RESTART CHECKLIST

### ELECTRICAL FIRE IN FLIGHT

| Challenge | Response |
|---|---|
| Master Switch | OFF |
| All Other Switches Except Ignition | OFF |
| Vents Heat / Air | CLOSED |
| Fire Extinguisher | ACTIVATE |

WARNING: AFTER DISCHARGING FIRE EXTINGUISHER WITHIN CLOSED CABIN, VENTILATE CABIN

IF FIRE APPEARS OUT AND ELECTRICAL POWER IS NECESSARY FOR CONTINUANCE OF FLIGHT

| Challenge | Response |
|---|---|
| Master Switch | ON |
| Circuit Breakers | check for faulty circuit, do not reset |
| Radio / Electrical Switches | ON |

(One at a time, with delay after each until short circuit is localized.)

| Challenge | Response |
|---|---|
| Vents Heat / Air | OPEN |

(When it is ascertained that fire is completely extinguished.)

Response success **depends** on the **quality** of your plan and the **readiness** of your team.

# Let's plan

# Why am I in this meeting?

# Question 2:

# “Surprise incidents” list

# Question 3:

# "Surprise incidents" list

# Take 2

# Question 2: Functional areas

| | |
|---|---|
| 1 | Network |
| 2 | Data center |
| 3 | Physical plant |
| 4 | Customer facing web application |

# Let’s review our questions

## Question 1

- No engagement
- Raise your hands

## Question 2

- Limited engagement with competition

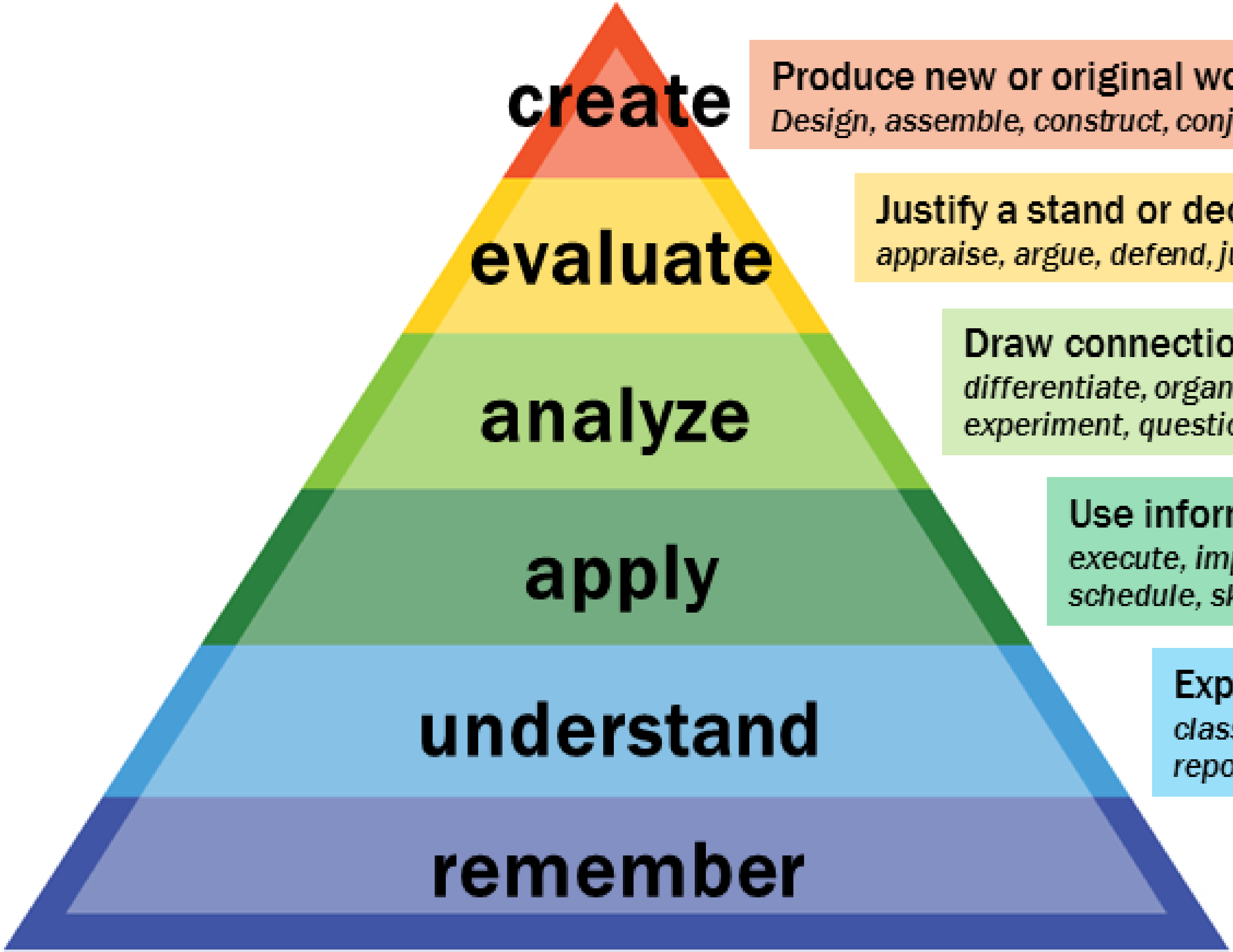
## Question 3

- Enhanced engagement
- Assigned roles
- Incentive (candy!!)

# Which one was most effective?

# It’s all a game.

# Bloom's Taxonomy



**create**

Produce new or original work

*Design, assemble, construct, conjecture, develop, formulate, author, investigate*

**evaluate**

Justify a stand or decision

*appraise, argue, defend, judge, select, support, value, critique, weigh*

**analyze**

Draw connections among ideas

*differentiate, organize, relate, compare, contrast, distinguish, examine, experiment, question, test*

**apply**

Use information in new situations

*execute, implement, solve, use, demonstrate, interpret, operate, schedule, sketch*

**understand**

Explain ideas or concepts

*classify, describe, discuss, explain, identify, locate, recognize, report, select, translate*

**remember**

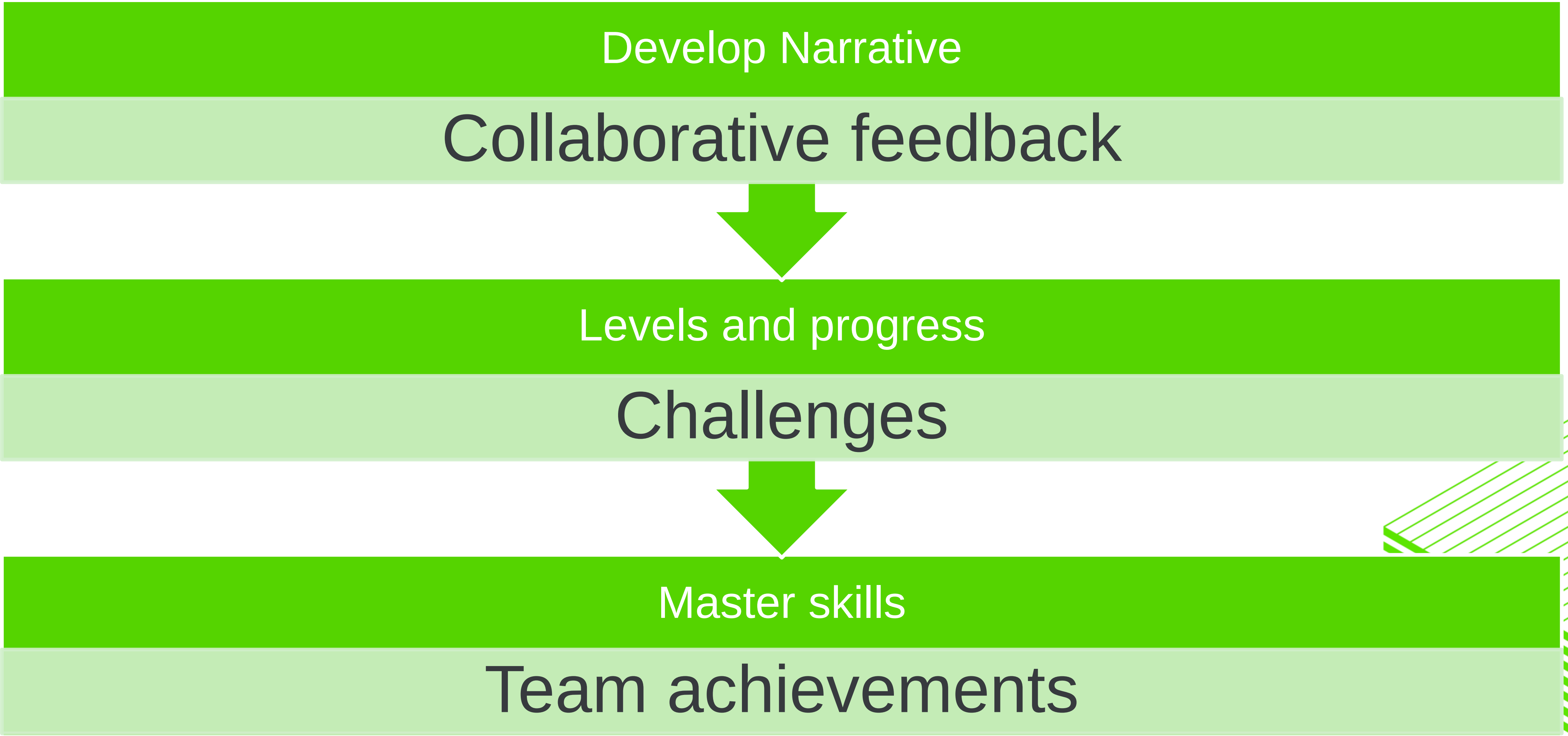
Recall facts and basic concepts

*define, duplicate, list, memorize, repeat, state*

Vanderbilt University Center for Teaching

**Active learning and engagement fosters critical thought and ownership**

# Game concepts



Develop Narrative

Collaborative feedback

Levels and progress

Challenges

Master skills

Team achievements

# Benefits of engagement – why gaming concepts work

Substantive input

Relevant plans

Crisis-ready personnel

# But where do we start?

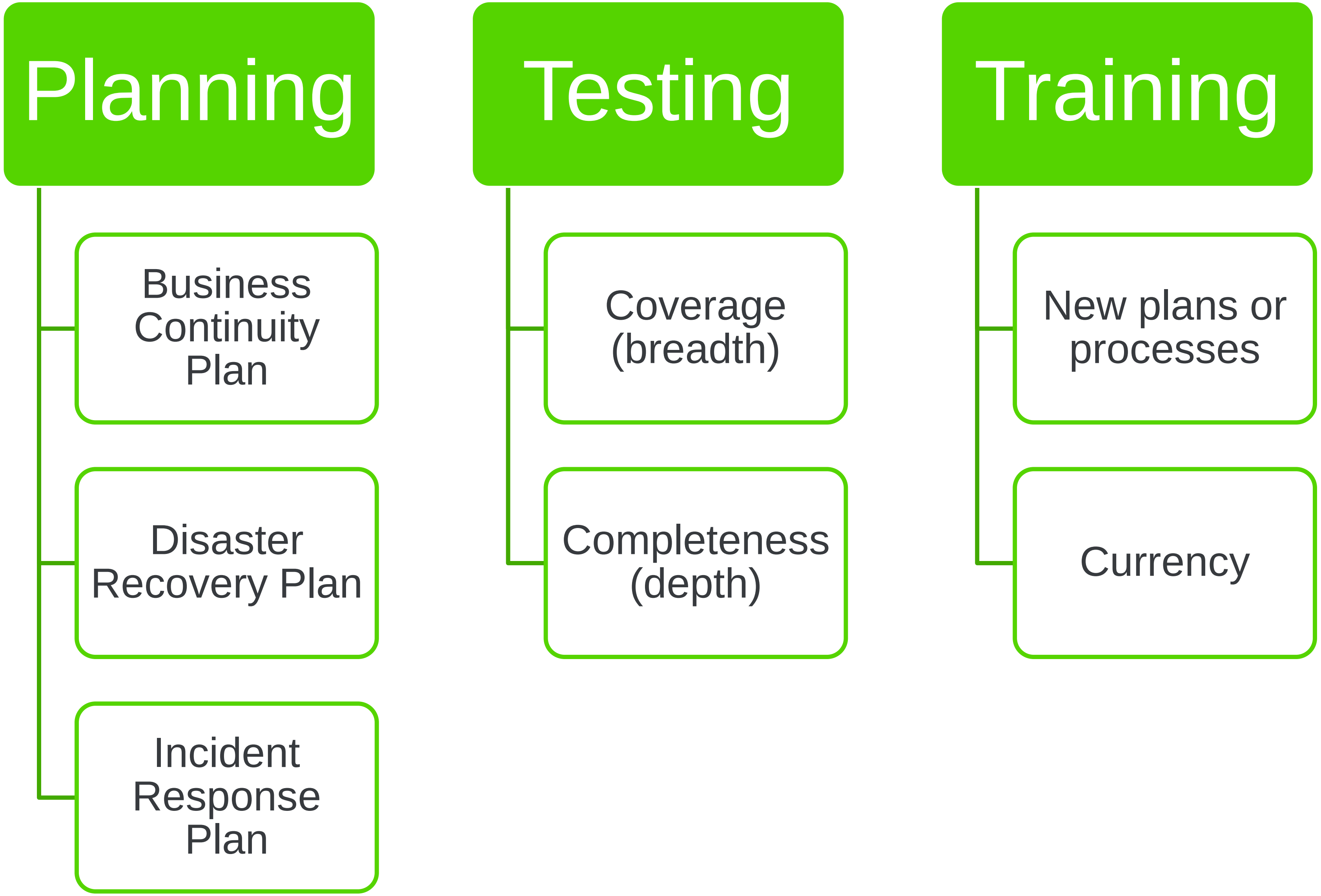
# SHALL WE PLAY A GAME?

Gamification

Role playing games

# Tabletop exercise (really just an RPG)

# Where do RPGs fit?



Planning

- Business Continuity Plan
- Disaster Recovery Plan
- Incident Response Plan

Testing

- Coverage (breadth)
- Completeness (depth)

Training

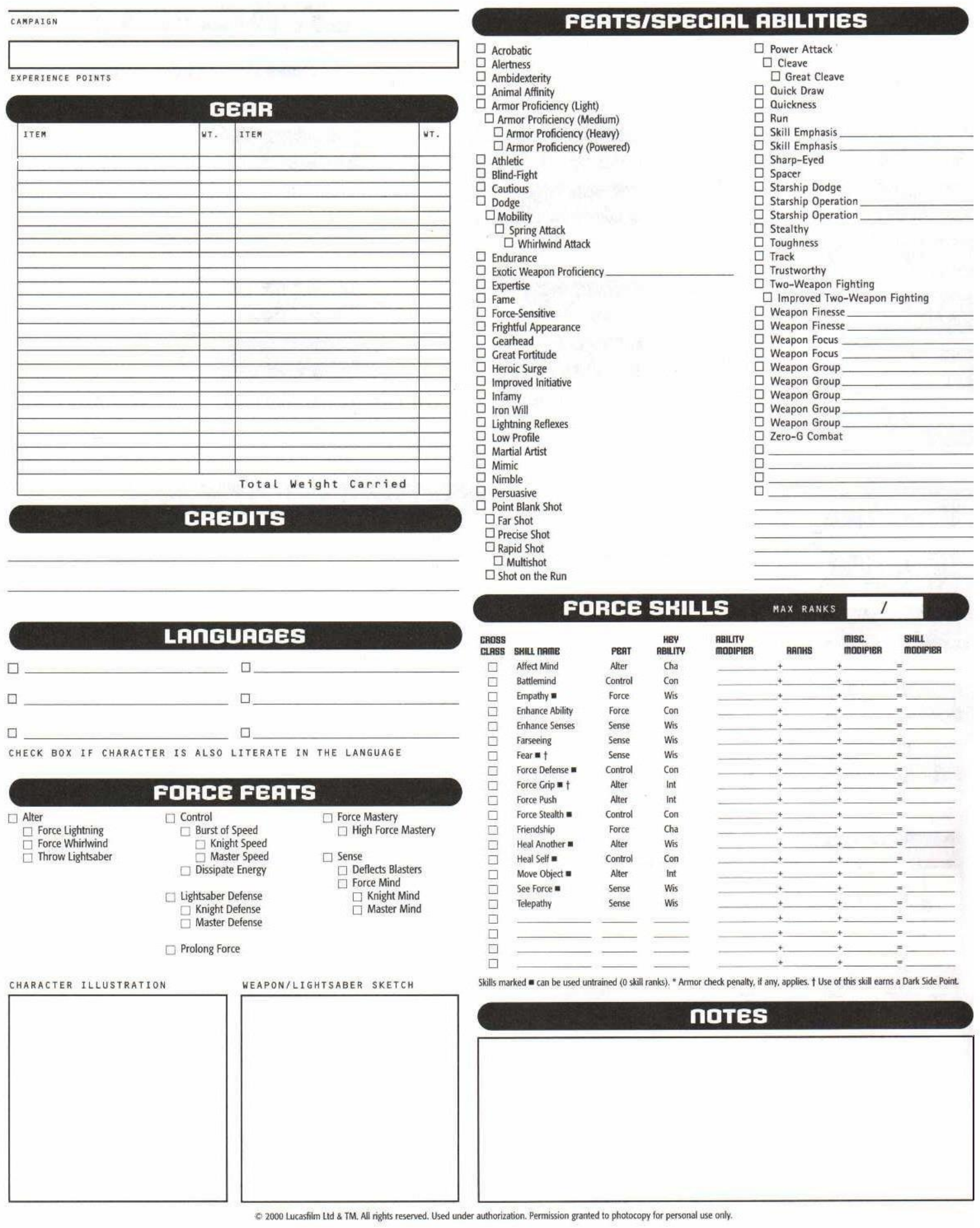
- New plans or processes
- Currency

# TESTING

I FIND YOUR LACK OF TESTS DISTURBING.

# Effective training

ADVANCED D&D
PLAYERS HANDBOOK
VAMPIRE
THE MASQUERADE
Advanced Dungeons & Dragons
Players Handbook
DUNGEONS & DRAGONS
PLAYER'S HANDBOOK
DUNGEONS & DRAGONS
PLAYER'S HANDBOOK
Arcane, Divine, and Martial Heroes
ROLEPLAYING GAME CORE RULES
STAR TREK
ROLEPLAYING GAME
MAGE
The Ascension
GURPS
Fourth Edition
THE PALLADIUM ROLE-PLAYING GAME
PATHFINDER
ROLEPLAYING GAME
STAR WARS
ROLEPLAYING GAME
KNIGHTS OF THE OLD REPUBLIC CAMPAIGN GUIDE



CAMPAIGN

EXPERIENCE POINTS

## GEAR

| ITEM | WT. | ITEM | WT. |
|---|---|---|---|
| | | | |
| | | Total Weight Carried | |

## CREDITS

## LANGUAGES

□ ____________ □ ____________

□ ____________ □ ____________

□ ____________ □ ____________

CHECK BOX IF CHARACTER IS ALSO LITERATE IN THE LANGUAGE

## FORCE FEATS

- □ Alter
  - □ Force Lightning
  - □ Force Whirlwind
  - □ Throw Lightsaber
- □ Control
  - □ Burst of Speed
    - □ Knight Speed
    - □ Master Speed
  - □ Dissipate Energy
- □ Lightsaber Defense
  - □ Knight Defense
  - □ Master Defense
- □ Prolong Force
- □ Force Mastery
  - □ High Force Mastery
- □ Sense
  - □ Deflects Blasters
  - □ Force Mind
    - □ Knight Mind
    - □ Master Mind

CHARACTER ILLUSTRATION

WEAPON/LIGHTSABER SKETCH

## FEATS/SPECIAL ABILITIES

- □ Acrobatic
- □ Alertness
- □ Ambidexterity
- □ Animal Affinity
- □ Armor Proficiency (Light)
  - □ Armor Proficiency (Medium)
    - □ Armor Proficiency (Heavy)
    - □ Armor Proficiency (Powered)
- □ Athletic
- □ Blind-Fight
- □ Cautious
- □ Dodge
  - □ Mobility
    - □ Spring Attack
      - □ Whirlwind Attack
- □ Endurance
- □ Exotic Weapon Proficiency ____________
- □ Expertise
- □ Fame
- □ Force-Sensitive
- □ Frightful Appearance
- □ Gearhead
- □ Great Fortitude
- □ Heroic Surge
- □ Improved Initiative
- □ Infamy
- □ Iron Will
- □ Lightning Reflexes
- □ Low Profile
- □ Martial Artist
- □ Mimic
- □ Nimble
- □ Persuasive
- □ Point Blank Shot
  - □ Far Shot
  - □ Precise Shot
  - □ Rapid Shot
    - □ Multishot
  - □ Shot on the Run
- □ Power Attack
  - □ Cleave
    - □ Great Cleave
- □ Quick Draw
- □ Quickness
- □ Run
- □ Skill Emphasis ____________
- □ Skill Emphasis ____________
- □ Sharp-Eyed
- □ Spacer
- □ Starship Dodge
- □ Starship Operation ____________
- □ Starship Operation ____________
- □ Stealthy
- □ Toughness
- □ Track
- □ Trustworthy
- □ Two-Weapon Fighting
  - □ Improved Two-Weapon Fighting
- □ Weapon Finesse ____________
- □ Weapon Finesse ____________
- □ Weapon Focus ____________
- □ Weapon Focus ____________
- □ Weapon Group ____________
- □ Weapon Group ____________
- □ Weapon Group ____________
- □ Weapon Group ____________
- □ Weapon Group ____________
- □ Zero-G Combat
- □ ____________
- □ ____________
- □ ____________
- □ ____________

## FORCE SKILLS

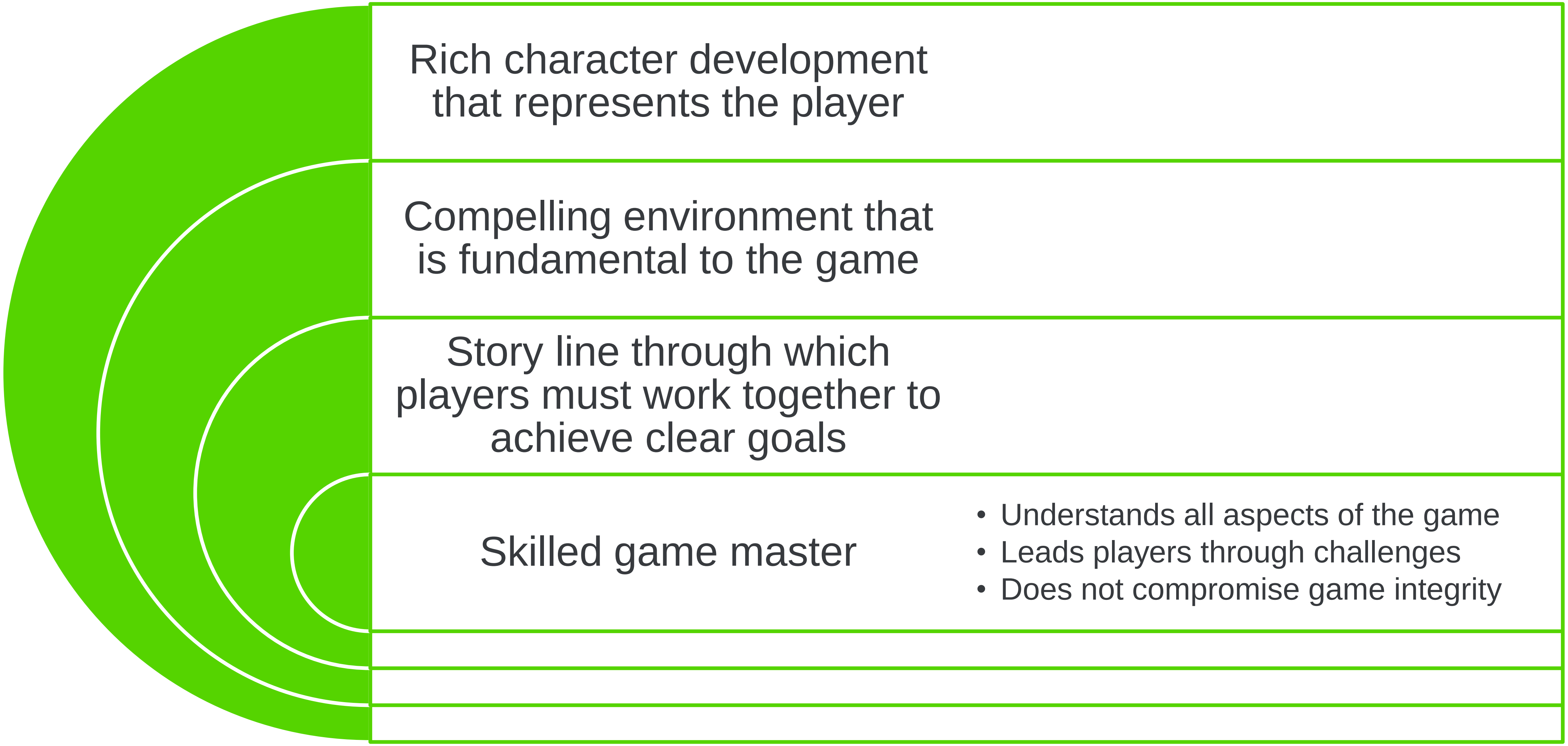
MAX RANKS /

| CROSS CLASS | SKILL NAME | FEAT | KEY ABILITY | ABILITY MODIFIER | | RANKS | | MISC. MODIFIER | | SKILL MODIFIER |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | Affect Mind | Alter | Cha | | + | | + | | = | |
| □ | Battlemind | Control | Con | | + | | + | | = | |
| □ | Empathy ■ | Force | Wis | | + | | + | | = | |
| □ | Enhance Ability | Force | Con | | + | | + | | = | |
| □ | Enhance Senses | Sense | Wis | | + | | + | | = | |
| □ | Farseeing | Sense | Wis | | + | | + | | = | |
| □ | Fear ■ † | Sense | Wis | | + | | + | | = | |
| □ | Force Defense ■ | Control | Con | | + | | + | | = | |
| □ | Force Grip ■ † | Alter | Int | | + | | + | | = | |
| □ | Force Push | Alter | Int | | + | | + | | = | |
| □ | Force Stealth ■ | Control | Con | | + | | + | | = | |
| □ | Friendship | Force | Cha | | + | | + | | = | |
| □ | Heal Another ■ | Alter | Wis | | + | | + | | = | |
| □ | Heal Self ■ | Control | Con | | + | | + | | = | |
| □ | Move Object ■ | Alter | Int | | + | | + | | = | |
| □ | See Force ■ | Sense | Wis | | + | | + | | = | |
| □ | Telepathy | Sense | Wis | | + | | + | | = | |
| □ | | | | | + | | + | | = | |
| □ | | | | | + | | + | | = | |
| □ | | | | | + | | + | | = | |
| □ | | | | | + | | + | | = | |

Skills marked ■ can be used untrained (0 skill ranks). * Armor check penalty, if any, applies. † Use of this skill earns a Dark Side Point.

## NOTES

# A “good” RPG



Rich character development that represents the player

Compelling environment that is fundamental to the game

Story line through which players must work together to achieve clear goals

Skilled game master

- Understands all aspects of the game
- Leads players through challenges
- Does not compromise game integrity

# RPGs and planning

## Assume a role (character)

- More than just “playing” a character
- Each player takes on the role of a character (i.e. “becomes”)

## Understand the rules

- Must have core rules (start with policy)
- Should cover all foreseeable situations

## Work with other characters to meet goals

- Encourage input
- Seek consensus

# RPG benefits

Engagement

Team goal pursuit

Outcome ownership

# Where to get guidance

Look internally

Explore on-line

Engage external resources

# Example IR planning scenario (phase 1)

- Split into groups
- Randomly assign each group a domain
  - Sample: https://www.sans.org/security-resources/policies
  - SANS example policy categories
    - General
    - Network Security
    - Server Security
    - Application Security
- Ask each group to create a list of incidents and response plans
- Have each group present a story based on findings
- Provide incentive for creative response

# Example challenge scenario (phase 1)

- Small fire just outside the data center, setting off the alarm system
- Sprinkler extinguishes the fire by the time the fire department arrives
- The building has been evacuated
- Personnel and the media are aware of what happened
- Then, as people begin to go back inside
  - The receptionist takes a call from someone who indicates that the fire is "only the beginning" because the company hasn't treated him right

Readiness depends on testing.
Want to play some more?

“It is better to be prepared than surprised”

- Dr. Michael Yousef

# SolomonConsulting

Ready

Set

Secure

# Resources

- Dr. Michael Solomon (michael@solomonconsulting.com)
- NIST SP 800-34 “Contingency Guide for Information Technology Systems”
- ISO 17799 / COBIT
- Disaster response sample scenarios
  - http://www.csoonline.com/article/2120836/disaster-recovery/pandemic-preparedness-tabletop-exercises-three-sample-scenarios.html?upd=1466709319099
- Business continuity tabletop exercises
  - http://www.csoonline.com/article/2132392/supply-chain-security/3-more-tabletop-exercises-for-business-continuity.html
- Gamemaster’s Guide to Incident Response
  - https://tisiphone.net/2015/07/13/gm-guide-to-ir/
- BCI online incident simulation game
  - http://www.thebci.org/index.php/resources/bc24-the-bci-s-online-incident-simulation-game