# Table of Contents

Right-click to update table of contents.

# Agent Persona Positioning and Hierarchy

## Executive Summary

**YES, positioning matters significantly.** The order of content in agent persona YAML files affects how LLMs interpret and prioritize information through positional bias, emphasis patterns, and cognitive load management.

# Part 1: Understanding Positional Bias

## Core Principle: Positional Bias in LLM Processing

### Primacy Effect

**What appears FIRST has outsized influence**

**Mechanism**:  
  
- LLMs pay strong attention to early content in prompts  
  
- First impressions establish context and framing  
  
- Early rules create "mental model" for subsequent interpretation  
  
- First-mentioned constraints often override later ones in conflict situations

**Application**:  
  
- Critical constraints should appear early  
  
- Mission/role statements benefit from top placement  
  
- Non-negotiable rules belong near the beginning

### Recency Effect

**What appears LAST also has strong influence**

**Mechanism**:  
  
- Final instructions are "fresh" when LLM begins reasoning  
  
- Last-stated rules often win in ambiguous situations  
  
- Concluding statements reinforce earlier content  
  
- "Remember:" statements at end have high impact

**Application**:  
  
- Repeat critical constraints at the end  
  
- Final reminders of most important rules  
  
- Closing emphasis on mission-critical behaviors

### Middle Dilution

**Middle content can be less influential**

**Mechanism**:  
  
- Detailed procedures in middle can blur together  
  
- Long sections reduce attention per item  
  
- Context switching between topics reduces retention  
  
- Procedural details compete for attention

**Mitigation**:  
  
- Use clear section headers for middle content  
  
- Bold/capitalize critical items even in middle  
  
- Break long middle sections into digestible chunks  
  
- Repeat critical rules if appearing in middle

## Evidence from BOKF Agents

### Example: Gatekeeper Orchestrator Structure

**Positioning Analysis**:

# Position 1: CRITICAL INTERACTION GUIDELINES (TOP)  
## CRITICAL INTERACTION GUIDELINES  
- \*\*STOP IMMEDIATELY if workspaces/paths don't exist\*\*  
 # ↑ HIGHEST PRIORITY rule - positioned FIRST  
 # This ensures it's seen before any other instructions  
  
# Position 2: SHAWN WALLACE TECHNICAL AUTHORITY (EARLY)  
## SHAWN WALLACE TECHNICAL AUTHORITY  
\*\*MANDATORY SIGNOFF PROTOCOL\*\*: ...  
 # ↑ Critical authority relationship - positioned SECOND  
 # Establishes non-negotiable approval hierarchy upfront  
  
# Position 3: MANDATORY SCOPE CONSTRAINTS (EARLY-MIDDLE)  
## 🚨 MANDATORY SCOPE CONSTRAINTS - NON-NEGOTIABLE  
 # ↑ Critical operational boundaries  
 # Positioned early to establish what agent CAN'T do  
 # Uses emoji 🚨 for visual emphasis even in middle position  
  
# Middle sections: Mission, team coordination, workflows  
 # Detailed procedures and context  
 # Less critical positionally but well-structured  
  
# Final Position: Success metrics and REMINDER  
Remember: Your role is to orchestrate a team that transforms...  
 # ↑ Recency effect - final reminder of core mission  
 # Reinforces primary objective as last thing before execution

**Pattern Observed**:  
  
1. **Absolute constraints FIRST** (stop rules, critical guidelines)  
  
2. **Authority relationships SECOND** (who has power, signoff requirements)  
  
3. **Scope boundaries THIRD** (what's permitted/prohibited)  
  
4. **Mission and procedures MIDDLE** (how to do the work)  
  
5. **Reminders and success metrics LAST** (reinforce mission)

# Part 2: Best Practices and Patterns

## Positioning Best Practices

### Tier 1: Top Position (Highest Priority)

**What Goes Here**:  
  
- Critical stop rules ("STOP if X")  
  
- Absolute constraints that override everything  
  
- Emergency protocols  
  
- Highest-priority behavioral rules

**Example**:

persona: |  
 ## CRITICAL: STOP RULES  
 - \*\*STOP IMMEDIATELY if workspaces/paths don't exist\*\*  
 - \*\*STOP if requirements contradict established patterns\*\*  
 - \*\*STOP if clone tasks exceed 30 minutes\*\*

**Why This Works**:  
  
- LLM sees constraints before being tempted by other instructions  
  
- Establishes "safety rails" before complex procedures  
  
- Creates strong initial framing for all subsequent behavior

### Tier 2: Early Position (High Priority)

**What Goes Here**:  
  
- Role and mission statement  
  
- Authority relationships and signoff requirements  
  
- Non-negotiable scope boundaries  
  
- Critical coordination protocols

**Example**:

You are Douglas, the Gatekeeper System Modernization Orchestrator...  
  
 ## SHAWN WALLACE TECHNICAL AUTHORITY  
 \*\*MANDATORY SIGNOFF PROTOCOL\*\*: ...  
  
 ## 🚨 MANDATORY SCOPE CONSTRAINTS - NON-NEGOTIABLE  
 ✅ PERMITTED: ...  
 ❌ PROHIBITED: ...

**Why This Works**:  
  
- Establishes identity and mission context early  
  
- Authority relationships clear before delegation instructions  
  
- Scope boundaries prevent invalid work planning

### Tier 3: Middle Position (Standard Priority)

**What Goes Here**:  
  
- Detailed workflows and procedures  
  
- Team coordination specifics  
  
- Tool usage instructions  
  
- Context management strategies  
  
- Clone delegation details

**Important**: Use strong formatting to prevent middle dilution

### 🔥 Clone Delegation Framework - MANDATORY DISCIPLINE  
 - \*\*15-30 Minute Financial Task Rule\*\* - NEVER create clone tasks longer than 30 minutes

**Emphasis Techniques for Middle Content**:  
  
- Emoji for visual differentiation (🔥, 🚨, ✅, ❌)  
  
- Bold for critical terms (**MANDATORY**, **NEVER**)  
  
- ALL CAPS for emphasis (STOP, ONE, CRITICAL)  
  
- Section headers with clear hierarchy (##, ###)  
  
- Numbered/bulleted lists for clarity

### Tier 4: Late Position (Reinforcement)

**What Goes Here**:  
  
- Success metrics  
  
- Quality standards  
  
- Final mission reminders  
  
- Key principle repetition

**Example**:

## Success Metrics  
 - Requirements Coverage: 100%  
 - Code Quality: Superior maintainability  
  
 Remember: Your role is to orchestrate a team that transforms  
 comprehensive financial requirements into superior C# solutions  
 under Shawn Wallace's technical authority. Systematic, requirements-driven  
 development produces better results than experience-based assumptions.

**Why This Works**:  
  
- Recency effect reinforces mission as LLM begins work  
  
- Success metrics provide clear targets for evaluation  
  
- Final reminder creates strong closing framing

## Hierarchy Patterns

### Pattern 1: Constraint Sandwich

**Structure**:

[Critical constraints and stops - TOP]  
[Mission and role]  
[Detailed procedures - MIDDLE]  
[Reinforced constraints and mission - BOTTOM]

**Usage**: When absolute rules must never be violated  
  
**Example**: Gatekeeper agent (scope constraints repeated/reinforced)

### Pattern 2: Mission-First

**Structure**:

[Mission and role identity - TOP]  
[Critical constraints - EARLY]  
[Detailed workflows - MIDDLE]  
[Success criteria - BOTTOM]

**Usage**: When agent identity and purpose drive behavior  
  
**Example**: Standard orchestrator agents

### Pattern 3: Authority-Driven

**Structure**:

[Stop rules - TOP]  
[Authority relationships - EARLY]  
[Coordination protocols - MIDDLE]  
[Authority reminders - BOTTOM]

**Usage**: When signoff/approval workflows are critical  
  
**Example**: Gatekeeper with Shawn Wallace authority

### Pattern 4: Sequential Workflow

**Structure**:

[Role definition - TOP]  
[Sequential phase definitions - EARLY TO MIDDLE]  
[Phase transition rules - MIDDLE]  
[Workflow reminders - BOTTOM]

**Usage**: When agent follows strict sequential process  
  
**Example**: Dominic domain analysis (one domain at a time)

## Emphasis Techniques

### Visual Emphasis (Emoji)

🚨 CRITICAL: ... # Emergency/danger  
🔥 MANDATORY: ... # Non-negotiable requirement  
✅ PERMITTED: ... # Allowed actions  
❌ PROHIBITED: ... # Forbidden actions  
⚠️ WARNING: ... # Caution/risk  
💡 TIP: ... # Helpful guidance

**Effect**: Breaks up text walls, creates visual hierarchy even in middle sections

### Textual Emphasis

\*\*BOLD\*\*: Critical terms  
\*Italic\*: Emphasis  
ALL CAPS: Strong emphasis (use sparingly)  
"Quotes": Specific values/terms

**Effect**: Draws eye to critical information in dense text

### Structural Emphasis

## Major Section  
### Subsection  
#### Detail Level  
  
- Top-level bullet  
 - Nested detail  
 - Further nesting

**Effect**: Creates clear information hierarchy

### Repetition for Emphasis

# Early in persona:  
\*\*15-30 Minute Task Rule\*\* - NEVER create clone tasks longer than 30 minutes  
  
# Middle reminder:  
- Clone tasks: 15-30 minutes maximum  
  
# Final reminder:  
Remember: All clone tasks must be 15-30 minutes for optimal execution

**Effect**: Critical rules reinforced through strategic repetition

# Part 3: What to Avoid

## Common Anti-Patterns

### Anti-Pattern 1: Buried Critical Constraints

**Problem**:

persona: |  
 You are an orchestrator who coordinates teams...  
  
 [3 pages of detailed workflows]  
  
 NEVER exceed 30-minute clone tasks.

**Why It Fails**: Critical constraint appears too late, after agent has internalized complex workflows

**Solution**: Move constraint to top or early position

### Anti-Pattern 2: Wall of Text (No Hierarchy)

**Problem**:

persona: |  
 You coordinate teams and ensure quality and manage context and  
 delegate clones and validate requirements and track progress and  
 compress context and handle failures and escalate issues...

**Why It Fails**: No visual breaks, everything equal priority, cognitive overload

**Solution**: Use headers, bullets, emphasis to create hierarchy

### Anti-Pattern 3: Contradictory Positioning

**Problem**:

persona: |  
 ## CRITICAL: Work on multiple domains in parallel for efficiency  
  
 [10 sections later]  
  
 Sequential processing: ONE domain at a time (never parallel)

**Why It Fails**: Primacy effect means early instruction wins, conflicts with later rule

**Solution**: Ensure critical rules don't contradict, position critical rule first

### Anti-Pattern 4: Weak Final Position

**Problem**:

persona: |  
 [Excellent persona content]  
  
 Workspace structure: $workspace\_tree

**Why It Fails**: Wastes recency effect on structural information instead of mission reminder

**Solution**: End with mission reminder or critical constraint repetition

### Anti-Pattern 5: Critical Rules Only in Middle

**Problem**:

persona: |  
 You are an orchestrator...  
  
 [Section 5 of 10]  
 NEVER modify source code in read-only workspace  
  
 [Continues with more sections]

**Why It Fails**: Critical safety rule buried in middle dilution zone

**Solution**: Move to top AND repeat at bottom

# Part 4: Application Guide

## Positioning Strategy by Agent Type

### Orchestrator Agents

**Priority Order**:  
  
1. Stop rules and critical constraints (TOP)  
  
2. Mission and team composition (EARLY)  
  
3. Authority relationships (EARLY)  
  
4. Sequential workflow phases (MIDDLE)  
  
5. Quality gates and coordination (MIDDLE)  
  
6. Success metrics (LATE)  
  
7. Mission reminder (BOTTOM)

**Rationale**: Orchestrators need constraints first, then team coordination structure

### Specialist Agents

**Priority Order**:  
  
1. Role definition and focus (TOP)  
  
2. Critical constraints (EARLY)  
  
3. Deliverable requirements (EARLY)  
  
4. Detailed procedures (MIDDLE)  
  
5. Quality standards (MIDDLE)  
  
6. Success criteria (LATE)  
  
7. Role reminder (BOTTOM)

**Rationale**: Specialists need clear focus area, then detailed execution guidance

### Validator/Reviewer Agents

**Priority Order**:  
  
1. Independence requirement (TOP) - "Do not rely on X"  
  
2. Validation criteria (EARLY)  
  
3. Critical accuracy thresholds (EARLY)  
  
4. Validation procedures (MIDDLE)  
  
5. Escalation protocols (MIDDLE)  
  
6. Approval standards (LATE)  
  
7. Quality reminder (BOTTOM)

**Rationale**: Validators must establish independence first, then criteria

### Domain/Sequential Processing Agents

**Priority Order**:  
  
1. ONE at a time rule (TOP)  
  
2. Sequential discipline (EARLY)  
  
3. Assignment protocol (EARLY)  
  
4. Per-unit workflow (MIDDLE)  
  
5. Cross-unit tracking (MIDDLE)  
  
6. Completion signaling (LATE)  
  
7. Sequential reminder (BOTTOM)

**Rationale**: Sequential discipline is paramount, must be established immediately

## Practical Checklist

### Persona Design Review

**Top Section (Lines 1-50)**:  
  
- [ ] Critical stop rules present?  
  
- [ ] Absolute constraints clearly stated?  
  
- [ ] Strong opening framing of mission/role?  
  
- [ ] Authority relationships established if needed?

**Early Section (Lines 51-200)**:  
  
- [ ] Mission and objectives clear?  
  
- [ ] Non-negotiable scope boundaries defined?  
  
- [ ] Team composition/coordination pattern stated?  
  
- [ ] Critical behavioral rules emphasized?

**Middle Section (Lines 201-1000)**:  
  
- [ ] Clear section headers breaking up content?  
  
- [ ] Emoji or bold used for emphasis?  
  
- [ ] Detailed procedures logically organized?  
  
- [ ] Critical rules repeated or reinforced?

**Late Section (Last 100 lines)**:  
  
- [ ] Success metrics defined?  
  
- [ ] Quality standards clear?  
  
- [ ] Mission reminder present?  
  
- [ ] Critical constraints reinforced?

**Overall**:  
  
- [ ] No contradictions between sections?  
  
- [ ] Critical rules appear early AND late?  
  
- [ ] Visual hierarchy clear (headers, bullets, emphasis)?  
  
- [ ] Most important rules not buried in middle?

## Conclusion

**Positioning is a critical design element, not an afterthought.**

**Key Principles**:  
  
1. **Primacy**: Put critical constraints and stops FIRST  
  
2. **Recency**: Reinforce mission and critical rules LAST  
  
3. **Emphasis**: Use formatting to prevent middle dilution  
  
4. **Repetition**: Repeat critical rules strategically  
  
5. **Hierarchy**: Clear structure prevents cognitive overload

**Test Your Design**:  
  
- What does the agent see in first 30 seconds of reading? (Should be critical constraints)  
  
- What's the last thing before execution? (Should be mission reminder)  
  
- Can you skim middle sections and still find critical rules? (Should have visual emphasis)  
  
- Are absolute constraints repeated? (Should appear top AND bottom if critical)

**Remember**: LLMs are influenced by position, emphasis, and structure just like humans reading documentation - design personas accordingly.